# Decision Notice 169/2021

## CCTV footage

**Applicant: The Applicant**

**Public authority: Scottish Prison Service**

**Case Ref: 202100354**

Scottish Information Commissioner

## Summary

The SPS was asked for CCTV footage recorded in HMP Edinburgh on a specific date. The SPS refused to disclose the information as it considered it to be third party personal data, exempt from disclosure. Following an investigation, the Commissioner agreed that the footage was exempt from disclosure.

## Relevant statutory provisions

Freedom of Information (Scotland) Act 2002 (FOISA) sections 1(1) and (6) (General entitlement); 2(1)(a) and (2)(e)(ii) (Effect of exemptions); 38(1)(b), (2A), (5) (definitions of "data protection principles", "data subject", "personal data", "processing" and "the UK GDPR") and (5A) (Personal information)

United Kingdom General Data Protection Regulation (the UK GDPR) articles 5(1)(a) (Principles relating to processing of personal data); 6(1)(f) (Lawfulness of processing)

Data Protection Act 2018 (the DPA 2018) sections 3(2), (3), (4)(d), (5), (10) and (14)(a), (c) and (d) (Terms relating to the processing of personal data)

The full text of each of the statutory provisions cited above is reproduced in Appendix 1 to this decision. The Appendix forms part of this decision.

## Background

1. On 19 June 2020, the Applicant made a request for information to the Scottish Prison Service (SPS). The information requested was:

   *All and any information, not being my own personal data, contained within CCTV footage recorded within Ingliston House Level 3 South and within CCTV footage recorded via cameras in the IL3 Desk area, directed towards Ingliston 3 South, such footage having been recorded between 20:20 and 20:45 on Thursday 12 March 2020.*

2. The SPS responded on 15 July 2020. In its response, the SPS refused to provide the information requested and applied the exemption in section 38(1)(b) of FOISA, as it considered the requested information to be third party personal data, disclosure of which would contravene the data protection principles in the General Data Protection Regulation (GDPR) (which still applied in the United Kingdom at that time).

3. On 15 August 2020, the Applicant wrote to the SPS requesting a review of its decision. He did not believe the SPS had shown why disclosure of third party personal data in response to the request would infringe the rights of the data subjects. The Applicant referred to instances where CCTV footage had been disclosed despite privacy issues being raised on behalf of the data subjects.

4. The SPS notified the Applicant of the outcome of its review on 22 September 2020. The SPS upheld its original response, satisfied that the requested information related to identifiable individuals and therefore constituted personal data. The SPS went on to explain, in detail, why it considered disclosure of this information, in response to this request, would be a breach of the first data protection principle.

5. On 12 March 2021, the Applicant wrote to the Commissioner, applying for a decision in terms of section 47(1) of FOISA. The Applicant stated he was dissatisfied with the outcome of the

SPS's review, because he did not agree that it was entitled to rely on the exemption in section 38(1)(b) of FOISA to withhold information from him.

## Investigation

6. The application was accepted as valid. The Commissioner confirmed that the Applicant made a request for information to a Scottish public authority and asked the authority to review its response to that request before applying to him for a decision.

7. On 29 March 2021, the SPS was notified in writing that the Applicant had made a valid application. The case was allocated to an investigating officer.

8. Section 49(3)(a) of FOISA requires the Commissioner to give public authorities an opportunity to provide comments on an application. The SPS was asked to provide the Commissioner with the CCTV footage withheld from the Applicant and also invited to comment on this application and answer specific questions. These related to why it considered the requested information to be third party personal data, disclosure of which would breach any of the data protection principles. Comments were also sought from the SPS on the Applicant's view that CCTV footage of this type should not be withheld under this exemption as it has been published with judicial approval in a previous case.

9. During the investigation, further submissions were received from the Applicant, particularly on his legitimate interests.

## Commissioner's analysis and findings

10. In coming to a decision on this matter, the Commissioner considered all of the withheld information and the relevant submissions, or parts of submissions, made to him by both the Applicant and the SPS. He is satisfied that no matter of relevance has been overlooked.

### Section 38(1)(b) – Personal information

11. When responding to the Applicant's request and requirement for review, the SPS relied on the exemption in section 38(1)(b) for withholding the content of the CCTV footage recorded on 12 March 2020.

12. The SPS explained that a number of prisoners and staff could clearly be identified in the CCTV footage, and disclosure of this would breach the first data protection principle in Article 5(1) of the UK GDPR ("lawfulness, fairness and transparency") as well as Article 10 of the UK GDPR ("Processing of personal data relating to criminal convictions and offences").

13. Section 38(1)(b) of FOISA, read in conjunction with section 38(2A), exempts information from disclosure if it is "personal data" (as defined in section 3(2) of the DPA 2018) and its disclosure would contravene one or more of the data protection principles set out in Article 5(1) of the UK GDPR or (where relevant) in the DPA 2018.

14. The exemption in section 38(1)(b) of FOISA, applied on the basis set out in the preceding paragraph, is an absolute exemption. This means that it is not subject to the public interest test contained in section 2(1)(b) of FOISA.

*Is the withheld information personal data?*

15. The first question the Commissioner must address is whether the CCTV footage comprises personal data for the purposes of section 3(2) of the DPA 2018.

16. "Personal data" is defined in section 3(2) of the DPA 2018 as "any information relating to an identified or identifiable living individual". Section 3(3) of the DPA 2018 defines "identifiable living individual" as a living individual who can be identified, directly or indirectly, in particular by reference to –

    (i) an identifier such as a name, an identification number, location data, or an online identifier, or

    (ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

17. The SPS submitted, as mentioned above, that a number of prisoners and staff could clearly be identified in the footage and it was the personal data of these individuals that was being withheld. In the SPS's view, disclosure of this footage would have the effect of disclosing the identities of those in custody, effectively identifying them as having been convicted of criminal activity. The SPS noted that the Applicant was also visible in the CCTV footage: the Applicant clearly excluded his own personal data from the information request (so any personal data of his cannot be considered for potential disclosure).

18. In the case of *Breyer v Bundesrepublik Deutschland*[1], the Court of Justice of the European Union looked at the question of identification. The Court took the view that the correct test to consider is whether there is a realistic prospect of someone being identified. When making that determination, account can be taken of the information in the hands of a third party. However, there must be a realistic casual chain – if the risk of identification is insignificant, the information will not be personal data.

19. Although this decision was made before the UK GDPR and the DPA 2018 came into force, the Commissioner considers the same rules apply now in this regard.

20. The two main elements in the definition of personal data are that the information must "relate to" a living person, and that person must be identified – or identifiable – from the data, or from the data and other information (using means reasonably likely to be used).

21. Information will "relate to" a person if it is about them, is linked to them, has biographical significance for them, is used to inform decisions affecting them, or has them as its main focus.

22. An individual is "identified" or "identifiable" if it is possible to distinguish them from other individuals.

23. The Commissioner has considered the SPS's submissions, together with the withheld information. The Commissioner is satisfied that the CCTV footage would reveal the identities of a number of prisoners resident in HMP Edinburgh and some members of staff working there. He is satisfied that this comprises information sufficiently biographical in relation to these individuals that it can be said to relate to them.

24. The Commissioner is therefore satisfied that the CCTV footage requested by the Applicant is the personal data, as defined in section 3(2) of the DPA, of more than one data subject.

25. In his submissions, the Applicant referred to media publication of CCTV images showing the actions of SPS officers and others in relation to the death of a prisoner. He explained that the publication of these images was challenged because it would breach the privacy of those

[1] http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

involved. However, he understood that, having attempted to interdict publication, the SPS was obliged to accept that pixilation of these images rendered the individuals concerned no longer identifiable. The Applicant submitted that it was open to the SPS to provide pixelated images in response to his request.

26. Anonymous information will not be personal data. Recital [26] of the GDPR describes information as anonymous where it does not relate to an identified or identifiable natural person, or is personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

27. The Commissioner acknowledges that the footage *could* be pixelated, meaning that the individuals in it would no longer be immediately identifiable. However, he is not satisfied that this would render the individuals no longer identifiable to a reasonable number of people within the prison community, unless the pixilation were taken to an extent which rendered the footage unintelligible. With that in mind, he also has to question whether any level of pixilation would be compatible with the legitimate interests the Applicant has identified (see below). In all the circumstances, the Commissioner is not satisfied as to pixilation or any similar process as a practicable means of rendering the requested data anonymous and still fulfilling the request.

*Would disclosure contravene one of the data protection principles?*

28. The SPS argued that the first data protection principle would be breached by disclosure of the information.

29. The definition of "processing" is wide and includes (section 3(4)(d) of the DPA 2018), "disclosure by transmission, dissemination or otherwise making available". In the case of FOISA, personal data are processed when disclosed in response to a request. This means that the personal data could only be disclosed if disclosure would be both lawful (i.e. it would meet one of the conditions of lawful processing listed in Article 6(1) of the GDPR) and fair.

*Lawful processing: Article 6(1)(f) of the UK GDPR*

30. In considering lawfulness, the Commissioner must consider whether any of the conditions in Article 6(1) of the UK GDPR would allow personal data to be disclosed.

31. It appears to the Commissioner that the only lawful basis in Article 6(1) of the UK GDPR which could allow disclosure of the information would be condition (f). This states that processing shall be lawful if it is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

32. Although Article 6(1) states that this condition cannot apply to processing carried out by a public authority in performance of its tasks, section 38(5A) of FOISA (see Appendix 1) makes it clear that public authorities can rely on Article 6(1)(f) when responding to requests under FOISA.

33. The tests which must be met before Article 6(1)(f) can be met are as follows:

    (i) Would the Applicant have a legitimate interest in obtaining the personal data?

    (ii) If so, would the disclosure of the personal data be necessary to achieve that legitimate interest?

(iii) Even if disclosure is necessary, is that overridden by the interests or fundamental rights and freedoms of the data subject(s)?

Would the Applicant have a legitimate interest in obtaining the personal data?

34. The Applicant stated that he had a direct and legitimate interest in the information contained in the CCTV footage. He asserted that there was an ongoing dispute about the nature of the striking of a named prisoner by a named prison officer and this, in turn, had a bearing on what the prison officer subsequently said to the Applicant.

35. The Applicant has set out, in detail, why he believes he has a legitimate interest in accessing the CCTV footage. He has referred to two court cases which led to criticisms of the SPS in relation to systems of working in place, training given and the way in which procedures were followed when managing prisoners. The Applicant has stated that it is in this context, taken with his own intention to pursue certain aspects of the investigation into his complaint carried out by Police Scotland, that he believes the requested information can contribute to the learning process required if lethal use of force (UOF) incidents at HMP Edinburgh are to be avoided in future.

36. The Applicant considers Police Scotland were not fully aware of all of the information available, or all the circumstances surrounding the handling of a particular complaint relating to the matter captured by the CCTV footage. Nor, in his view, were they aware of particular circumstances relating to the health of the named prisoner when reaching a decision on the Applicant's complaint.

37. It is the Applicant's view that access to the CCTV footage would permit him to demonstrate (to the Police Investigations and Review Commissioner (PIRC)) that his complaint to Police Scotland was wholly justified.

38. The Applicant has also referred to the content of a document which refers to a prison disciplinary finding against him which was subsequently overturned, a change which is not reflected in that document (which he has submitted will be used to inform decisions affecting his future). The Applicant believes this underlines the need for him to be in possession of the CCTV footage, to demonstrate the lengths that prison staff are prepared to take to discredit him as a witness to an assault.

39. In further comments, the Applicant referred to another document which he submitted would be used to inform decisions about his future. He believed an entry in this document, relating to matters connected to the incident captured by the CCTV footage, to have been made maliciously. He submitted that he needed the footage to demonstrate the false nature of the statements and vindicate his own position.

40. In addition, the Applicant considers himself to be at a disadvantage in not having access to the CCTV footage, on a "without prejudice" basis, in connection with a related complaint of gross misconduct against a member of prison staff.

41. Whilst the SPS acknowledged that the Applicant was concerned that prison staff captured by the CCTV footage were guilty of assaulting a named prisoner, it did not accept that the Applicant had a legitimate interest in obtaining the personal data contained in the footage.

42. The SPS commented that an investigation into this allegation was carried out by Police Scotland and it was found that no crime had been committed and there was no case to answer. The SPS submitted that the Applicant was not involved in the matter captured by

the CCTV footage, other than as a bystander, and so it concluded that he had no legitimate interest in obtaining the information.

43. The Commissioner accepts that the Applicant, with the wider public, has a legitimate interest in obtaining the CCTV footage. Having read the reports into the two cases referred to by the Applicant, the Commissioner acknowledges that concerns may exist over whether SPS staff are following appropriate procedures and protocols when managing prisoners to ensure that prisoners' welfare is protected, and disclosure of the CCTV footage in this case might help address concerns in this area. The Commissioner also accepts that there is a more general legitimate interest in the public knowing that relevant policies and procedures are being followed appropriately.

44. The Commissioner also acknowledges that the Applicant has demonstrated a legitimate interest in pursuing the more personal matters referred to in his submissions (although it is not clear whether the misconduct complaint was actually in contemplation at the time of the request or requirement for review). He would reiterate, however, that any legitimate interest would be an interest in obtaining the footage in its full (unpixellated) form – he cannot see what practical or evidential value the footage would have, for any of these purposes, if pixelated to the extent that rendered the individuals in it anonymous.

Would disclosure of the personal data be necessary?

45. Having accepted that the Applicant has a legitimate interest in the personal data, the Commissioner must consider whether disclosure of this personal data would be necessary to meet the Applicant's legitimate interests.

46. "Necessary" means "reasonably" rather than "absolutely" or "strictly" necessary. When considering whether disclosure would be necessary, public authorities should consider whether the disclosure is proportionate as a means and fairly balanced as to the aims to be achieved, or whether the requester's legitimate interests can be met by means which interfere less with the privacy of the data subjects.

47. Having considered the submissions from both the Applicant and the SPS, the Commissioner does not accept that the disclosure of the CCTV footage is necessary to fulfil the legitimate interests of the Applicant in this case.

48. Firstly, from the footage, it is not apparent why risk to life should have been considered likely in this case. The Commissioner acknowledges that the Applicant was present at the incident and may have a greater understanding of aspects that were not apparent to the cameras, but it is not clear to the Commissioner what lessons on the lethal use of force might possibly be learned from the footage that is available. He also notes, as the Applicant has been assured by Police Scotland, that the footage has been reviewed and taken into account by the SPS for staff training purposes.

49. As Police Scotland have also advised the Applicant, there are avenues for pursuing concerns about whether the SPS is complying properly with the required procedures in any given area via the Scottish Public Services Ombudsman (the SPSO) once internal complaints processes are exhausted. The Commissioner sees no reason why pursuing concerns via this route should require the public disclosure of the footage in question. Neither can he see why raising and pursuing a complaint with PIRC should require such disclosure. Either regulator should be able to see the footage, if it finds it necessary to do so, without it being made available to the world at large: to date, both Police Scotland and the Commissioner have had the opportunity to inspect it in private, apparently without difficulty. Viewing the footage

again, incidentally, would not make Police Scotland any more aware of the underlying circumstances than they were the first time they viewed it.

50. The Commissioner notes the Applicant's concerns about his own disciplinary situation and related complaints, which are clearly matters of considerable interest to him. It is not apparent, however, why anyone should need the withheld footage either to investigate the Applicant's complaint against a prison officer or to understand that the disciplinary finding was subsequently overturned. There should be (and indeed are) other – almost certainly more reliable – means of evidencing the latter point and, if the footage is of any relevance to the investigation of the conduct complaint, again it is not apparent why those carrying out any investigation cannot view it in private, without it being made available to the whole world.

51. The same, in the Commissioner's view, can be said of anyone making future decisions about the Applicant. If they needed access to the CCTV footage to understand the Applicant's position in relation to the incident and related circumstances (and it is not immediately apparent that they should), the Commissioner is not satisfied that they would have any difficulty viewing it privately, without the need for it to be disclosed into the public domain.

52. In terms of the wider public's legitimate interest in ensuring that SPS staff follow relevant procedures and practices when managing prisoners, the Commissioner is satisfied that there are mechanisms in place to allow relevant behaviours and practices to be challenged and investigated. As discussed above, however, it is not apparent that the relevant regulatory processes should require the disclosure of personal data to the world at large.

53. Overall, the Commissioner does not accept that disclosure of the CCTV footage is necessary to fulfil the Applicant's legitimate interests, or those of the wider public.

54. As the Commissioner has concluded that the disclosure of the personal data in this case is not necessary to fulfil the Applicant's legitimate interests, he finds that condition (f) in Article 6(1) of the UK GDPR cannot be satisfied. Accordingly, he accepts that disclosure of the personal data would be unlawful.

55. Given that the Commissioner has found that the processing would be unlawful, he is not required to go on to consider separately whether the data subject's interests or fundamental rights and freedoms would be prejudiced by disclosure (or to balance them against any legitimate interest in making the information available).

56. In all the circumstances of the case, in the absence of a condition in Article 6(1) of the UK GDPR being met, the Commissioner must conclude that disclosure of the personal data would breach the data protection principle in Article 5(1)(a) of the UK GDPR. Consequently, he is satisfied that the SPS was entitled to withhold the information under section 38(1)(b) of FOISA.

57. As mentioned previously, the SPS also argued that disclosure of the CCTV footage would be contrary to Article 10 of the UK GDPR, in relation to the processing of personal data relating to criminal convictions and offences. Because the Commissioner has found that disclosure of the withheld information would be unlawful in terms of the data protection principle in Article 5(1)(a) of the UK GDPR, he need not (and will not) go on to consider whether disclosure would also breach Article 10.

## Decision

The Commissioner finds that the Scottish Prison Service complied with Part 1 of the Freedom of Information (Scotland) Act 2002 in responding to the information request made by the Applicant.

## Appeal

Should either the Applicant or the SPS wish to appeal against this decision, they have the right to appeal to the Court of Session on a point of law only. Any such appeal must be made within 42 days after the date of intimation of this decision.

**Margaret Keyse**
**Head of Enforcement**

**26 October 2021**

## Appendix 1: Relevant statutory provisions

# Freedom of Information (Scotland) Act 2002

### 1 General entitlement

(1) A person who requests information from a Scottish public authority which holds it is entitled to be given it by the authority.

…

(6) This section is subject to sections 2, 9, 12 and 14.

### 2 Effect of exemptions

(1) To information which is exempt information by virtue of any provision of Part 2, section 1 applies only to the extent that –

(a) the provision does not confer absolute exemption; and

…

(2) For the purposes of paragraph (a) of subsection 1, the following provisions of Part 2 (and no others) are to be regarded as conferring absolute exemption –

(e) in subsection (1) of section 38 –

…

(ii) paragraph (b) where the first condition referred to in that paragraph is satisfied.

### 38 Personal information

(1) Information is exempt information if it constitutes-

…

(b) personal data and the first, second or third condition is satisfied (see subsections (2A) to (3A);

…

(2A) The first condition is that the disclosure of the information to a member of the public otherwise than under this Act -

(a) would contravene any of the data protection principles, or

(b) would do so if the exemptions in section 24(1) of the Data Protection Act 2018 (manual unstructured data held by public authorities) were disregarded.

…

(5) In this section-

"the data protection principles" means the principles set out in –

(a) Article 5(1) of the UK GDPR, and

(b) section 34(1) of the Data Protection Act 2018;

"data subject" has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);

…

"personal data" and "processing" have the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2), (4) and (14) of that Act);

"the UK GDPR" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(10) and (14) of that Act).

(5A) In determining for the purposes of this section whether the lawfulness principle in Article 5(1)(a) of the UK GDPR would be contravened by the disclosure of information, Article 6(1) of the UK GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted.

## UK General Data Protection Regulation

### Article 5 Principles relating to processing of personal data

1 Personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency")

…

### Article 6 Lawfulness of processing

1 Processing shall be lawful only if and to the extent that at least one of the following applies:

…

f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

## Data Protection Act 2018

### 3 Terms relating to the processing of personal data

…

(2) "Personal data" means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)).

(3) "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to –

(a) an identifier such as a name, an identification number, location data or an online identifier, or

(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

(4) "Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as –

…

(d) disclosure by transmission, dissemination or otherwise making available,

…

(5) "Data subject" means the identified or identifiable living individual to whom personal data relates.

(10) "The UK GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and see section 205(4)).

…

(14) In Parts 5 to 7, except where otherwise provided –

(a) references to the UK GDPR are to the UK GDPR read with Part 2;

…

(c) references to personal data, and the processing of personal data, are to personal data and processing to which Part 2, Part 3 or Part 4 applies;

(d) references to a controller or processor are to a controller or processor in relation to the processing of personal data to which Part 2, Part 3 or Part 4 applies.

**Scottish Information Commissioner**
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t 01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

**www.itspublicknowledge.info**