

Decision Notice 111/2021

Employee misconduct investigation

Applicant: The Applicant

Public authority: University of Edinburgh

Case Ref: 202001288



Scottish Information
Commissioner

Summary

The University was asked for information relating to a misconduct investigation against a named individual.

The University refused to confirm or deny whether it held the information. The Commissioner investigated and found that the University was entitled to refuse to confirm or deny whether it held the information.

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); 18(1) (Further provision as respects responses to request); 38(1)(b), (2A)(a), (5) (definitions of “the data protection principles”, “data subject”, “personal data” and “processing”, and “the UK GDPR”) and (5A) (Personal information)

United Kingdom General Data Protection Regulation (the UK GDPR) Article 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) and (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 10 July 2020, the Applicant made a request for information to the University of Edinburgh (the University). The information requested concerned a misconduct investigation in 2018/2019 about a named individual working within the University. The Applicant specifically requested:
 - a) Details (names of attendees, date and time) of all meetings which had taken place with regard to the investigation and their full transcripts.
 - b) The details (dates and contents) of all correspondences with a named research council.
 - c) Full name of the full list of individuals (excluding HR persons) involved with the investigation, to include anyone who contributed to the investigation by providing witness accounts, evidence and other. The details of HR persons could be omitted.
 - d) The full list of correspondence (e-mails, calls and texts) involving five named individuals and the defendant.
 - e) The complete list of evidence (e-mail and others) produced by the defendant to the investigation.
2. In the request, the Applicant stated that it was not necessary to disclose full names if sufficient enough part names could be provided to identify individuals uniquely. The Applicant also commented that if, and only if, the materials (e-mails, letters, calls or texts requested in parts a) to e)) also had or included non-relevant materials to the investigation

and/or personal information of anybody at the University, only those parts of the material could be redacted.

3. The University responded on 6 August 2020. It explained that, if it were to answer the Applicant's request, it would be disclosing whether or not the named individual had been the subject of an investigation under the Research and Misconduct Policy. The University commented that this would lead to the disclosure of personal information about that individual and others and would breach the data protection principles under data protection law. The University explained that this meant it could not tell the Applicant whether or not it held the requested information and stated that the requirement to provide this information was exempt under sections 18 and 38(1)(b) (Personal information) of FOISA.
4. The University set out why it considered it would be contrary to the public interest to reveal whether the information existed or was held.
5. On 27 August 2020, the Applicant wrote to the University, requesting a review of its decision.
6. The University notified the Applicant of the outcome of its review on 14 September 2020. The University upheld the decision and reasoning given in its response to the Applicant's request and concluded that it had been correct to state, with reference to section 18(1) of FOISA, that it could not confirm or deny whether it held any of the requested information, or whether that information existed. The University concluded that it was appropriate to apply section 18(1) of FOISA, in conjunction with section 38(1)(b).
7. On 26 October 2020, the Applicant wrote to the Commissioner, applying for a decision in terms of section 47(1) of FOISA.

Investigation

8. 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.
9. On 25 November 2020, the University was notified in writing that the Applicant had made a valid application. The case was allocated to an investigating officer.
10. Section 49(3)(a) of FOISA requires the Commissioner to give public authorities an opportunity to provide comments on an application. The University was invited to comment on this application and to answer specific questions. These related to its reasons for neither confirming nor denying whether it held the information, or whether it existed.

Commissioner's analysis and findings

11. In coming to a decision on this matter, the Commissioner considered all of the relevant submissions, or parts of submissions, made to him by both the Applicant and the University. He is satisfied that no matter of relevance has been overlooked.
12. During the investigation, the University confirmed that it still wished to rely on section 18 of FOISA, read in conjunction with section 38(1)(b), as outlined in the correspondence to the Applicant.

Section 18(1) – “neither confirm nor deny”

13. Section 18(1) of FOISA allows public authorities to refuse to confirm or deny whether they hold information in the following limited circumstances:
 - a request has been made to the authority for information which may or may not be held by it; and
 - if the information existed and was held by the authority (and it need not be), it could give a refusal notice under section 16(1) of FOISA, on the basis that the information was exempt information by virtue of any of the exemptions in sections 28 to 35, 38, 39(1) or 41 of FOISA; and
 - the authority considers that to reveal whether the information exists or is held by it would be contrary to the public interest.
14. Where a public authority has chosen to rely on section 18(1), the Commissioner must establish whether the authority is justified in stating that to reveal whether the information exists or is held would be contrary to the public interest. He must also establish whether, if the information existed and were held by the public authority, the authority would be justified in refusing to disclose the information by virtue of any of the exemptions listed in section 18(1) and cited by the authority.
15. Where section 18(1) is under consideration, the Commissioner must ensure that his decision notice does not confirm one way or the other whether the information requested actually exists or is held by the authority. This means he is unable to comment in any detail on the University’s reliance on any of the exemptions referred to, or on other matters which could have the effect of indicating whether the information existed or was held by the University.
16. Also, this decision notice summarises the arguments put forward by the Applicant. He believes the University holds information falling within scope of his request, and his submissions reflect that position. It should not be taken from his submissions that he is necessarily correct in that view.

Section 38(1)(b) – Personal information

17. Section 38(1)(b), read in conjunction with section 38(2A)(a) (or (b)), 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 GDPR.

Would the information be personal data?

18. “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 with 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.”
19. The Applicant has named the individual he considers to have been subject to a misconduct complaint and investigation, together with others he considered to be involved in meetings and the investigation.

20. In his information request, the Applicant also asked for the names of those who attended meetings and those involved in the investigation.
21. The University considered that the information, if held, would be “personal data”, given that it would concern attendees of investigation meetings and the wider investigation, correspondence and witness accounts. Disclosure of such information, if held, would (in the University’s view) disclose information “relating to” and “obviously about” the named member of staff as well as witnesses.
22. The Commissioner notes that each part of the information request is framed with reference to the named University employee and a complaint of misconduct made against them. Given that the Applicant has named specific individuals, and the subject matter of the request is the conduct and behaviour of the named member of University staff, the Commissioner is satisfied that, if this information did exist and were held by the University, any information captured by the request would clearly relate to one or more named individuals. The Commissioner therefore accepts that, if it existed and were held, the information would be personal data as defined in section 3(2) of the DPA 2018.

Would disclosure contravene one of the data protection principles?

23. The University argued that disclosing the personal data, if it existed and were held, would breach the first data protection principle. This requires personal data to be processed “lawfully, fairly and in a transparent manner in relation to the data subject” (Article 5(1)(a) of the GDPR).
24. 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. if it would meet one of the conditions of lawful processing listed in Article 6(1) of the GDPR) and fair.

Lawful processing: Articles 6(1)(f) of the GDPR

25. In considering lawfulness, the Commissioner must consider whether any of the conditions in Article 6(1) of the UK GDPR would allow the personal data to be disclosed.
26. The University considered the only lawful basis in Article 6(1) of the UK GDPR which could allow disclosure of the information, if it existed and were held, would be condition (f).
27. The Commissioner agrees that condition (f) is the only one which could potentially apply, assuming the personal data existed and were held. 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.”
28. 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.
29. 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 personal data, if held?

- (ii) If so, would the disclosure of the personal data be necessary to achieve that legitimate interest?
- (iii) Even if the processing would be necessary to achieve that legitimate interest, would that be overridden by the interests or fundamental rights and freedoms of the data subjects?

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

- 30. The University acknowledged that, if the information existed and were held, the Applicant would be undoubtedly pursuing a legitimate interest in seeking this information.
- 31. In the circumstances, the Commissioner is satisfied that these would be matters of legitimate interest to the Applicant. The Commissioner is also satisfied that this legitimate interest would extend to the wider public interest, in being satisfied that the University investigates such matters thoroughly. The Commissioner is therefore satisfied that, if it existed and were held, the Applicant would have a legitimate interest in obtaining the personal data.

Would disclosure be necessary?

- 32. The next question is whether the disclosure of personal data (if held) would be necessary to achieve that legitimate interest. "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 Applicant's legitimate interests could reasonably be met by means which interfered less with the privacy of the data subject.
- 33. The Commissioner has considered the scope of the Applicant's request and he accepts that, given the subject matter of his request, disclosure of the personal data, if in existence and held, would be necessary to achieve the Applicant's legitimate interest.
- 34. In the Commissioner's view, the only way the Applicant's legitimate interest could be met would be by viewing the information he has requested (assuming it exists and is held). Only then would he be able to understand who was directly involved in the decision making and what factors and circumstances were taken into account by the University. The Commissioner notes that no policy or procedure has been brought to his attention by either the University or the Applicant that might offer another way for the Applicant to be able to scrutinise and understand the actions and decisions of the University. The Commissioner therefore accepts that disclosure of any information held would be necessary for the Applicant's legitimate interests.

The data subject's interests or fundamental rights and freedoms (and balancing exercise)

- 35. The Commissioner has concluded that the disclosure of the information (if existing and held) would be necessary to achieve the Applicant's legitimate interests. However, this must be balanced against the fundamental rights and freedoms of the data subjects (the individuals named by the Applicant as being subject to allegations or otherwise captured by the request). Only if the legitimate interests of the Applicant outweighed those of the data subjects could personal data be disclosed without breaching the first data protection principle.
- 36. The Commissioner has considered the submissions from both parties carefully, in the light of the decision by the Supreme Court in *South Lanarkshire Council v Scottish Information*

Commissioner [2013] UKSC 555¹. He is unable to set out, in detail, the arguments put forward by the University.

37. The Commissioner's guidance² on section 38 of FOISA notes that, in carrying out the balancing exercise, much will depend on the reasonable expectations of the data subjects. Factors which will be relevant in determining reasonable expectations include:
- (i) whether the information relates to the individual's public life (i.e. their work as a public official or employee) or their private life (i.e. their home, family, social life or finances)
 - (ii) the potential harm or distress that may be caused by disclosure
 - (iii) whether the individual objected to the disclosure.
38. The Commissioner agrees with the University that the information (if it existed and were held) would be information a person would generally expect to be kept confidential and only shared amongst limited individuals for specific purposes.
39. The Commissioner has also considered the potential harm or distress that could be caused by disclosure of the information (if it existed and were held). Disclosure under FOISA is a public disclosure. At the most general level, disclosing or alleging some work place impropriety has taken place is likely to cause some reputational damage to the named employee.
40. Furthermore, such disclosure would also publicly link other individuals to having a role in contributing to, or undertaking, an investigation into this complaint when they would have a reasonable expectation that this information would remain confidential and would not be shared publicly.
41. After carefully balancing the legitimate interests of the Applicant against the interests or fundamental rights or freedoms of the data subjects, the Commissioner finds that the legitimate interests served by disclosure of any information held would be outweighed by the unwarranted prejudice that would result to the rights and freedoms or legitimate interests of the individuals in question in this case.
42. In all the circumstances of this particular case, the Commissioner concludes that condition (f) in Article 6(1) of the UK GDPR could not be met in relation to the withheld personal data (if it exists and is held).

Fairness and transparency

43. Given that the Commissioner has concluded that the processing of the personal data, if existing and held, would be unlawful, he is not required to go on to consider whether disclosure of such personal data would otherwise be fair and transparent in relation to the data subjects.

Conclusion on the data protection principles

44. For the reasons set out above, the Commissioner is satisfied that disclosure of any personal data, if it existed and were held, would breach the data protection principle in Article 5(1)(a) of the UK GDPR. Consequently, he is satisfied that such personal data would be exempt from disclosure under section 38(1)(b) of FOISA and that the University could give a refusal

¹ <https://www.supremecourt.uk/cases/docs/uksc-2012-0126-judgment.pdf>

² <http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/section38/Section38.aspx>

notice under section 16(1) of FOISA, on the basis that the information would be exempt by virtue of section 38(1)(b).

Section 18(1) – The public interest

45. The Commissioner must now consider whether the University was entitled to conclude that it would be contrary to the public interest to reveal whether the information existed or was held.
46. The University submitted that disclosing information (if in existence and held) to the Applicant would mean disclosure to the general public, which would breach a data protection principle.
47. The University acknowledged the clear public interest in the transparent operation of public authorities and in identifying instances of research misconduct. This, the University submitted, was why it took all allegations of research misconduct seriously and dealt with them in accordance with its Research Misconduct Policy.
48. The University asserted that there was a strong public interest in ensuring such cases were handled in accordance with these policies and guidance, to ensure issues were thoroughly considered and all parties treated fairly. The University commented that this meant ensuring confidentiality of any allegations and any subsequent actions. If staff members were aware that any confidential witness statement they might give in a misconduct investigation was to be publicised, the University believed they would hesitate and think twice before providing evidence. This would, the University claimed, result in less and less investigations being carried out in a satisfactory way with appropriate results. The University therefore concluded that the public interest in withholding whether or not it held the information sought by the Applicant outweighed the public interest in releasing it.
49. The Applicant considered there to be a public interest in the University confirming whether it held information covered by his request and disclosing this to him. The Applicant stated that there was an unprecedented level of public interest in the transparent and impartial operations of public authorities in the UK higher education sector.
50. In the Applicant's view, where the University had stated it considered the public interest to favour withholding whether or not it held this information, it had not been able to articulate whose interests it was trying to serve by maintaining the exemption.
51. The Applicant stated he had concluded that, within the University alone, over 40% of academic staff and about 53% of students had more than one reason to know how the University, as an elite public organisation, handled complaints with serious allegations. The Applicant submitted that, in combination with interested parties within the University and in the rest of the UK, the public interest in disclosure of the information easily outweighed the public interest in maintaining the exemption.
52. The test the Commissioner must consider is whether (having already concluded that the information, if it existed and were held, would be exempt from disclosure) it would be contrary to the public interest to reveal whether the information existed or was held.
53. The Commissioner has fully considered the submissions from the Applicant and appreciates that, where a complaint of misconduct has been made against a member of staff, there would be a public interest in ensuring that adequate consideration had been given to all facts of the case and a full and robust investigation is carried out.
54. However, the Commissioner is aware that the action of confirming or denying whether the information existed or was held would have the effect of revealing whether the named employee was subject to a misconduct investigation and who else was involved in providing

submissions to any such investigation and carrying it out. This would, of itself, lead to the University breaching its duties as a data controller under data protection legislation. In the circumstances, the Commissioner must find that it would be contrary to the public interest for the University to reveal whether it held the requested information, or whether the information existed.

55. Consequently, the Commissioner is satisfied that the University was entitled to refuse to confirm or deny, whether the information requested by the Applicant existed or was held, in accordance with section 18(1) of FOISA.

Decision

The Commissioner finds that the University of Edinburgh 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 University 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

12 July 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.

18 Further provision as respects responses to request

- (1) Where, if information existed and was held by a Scottish public authority, the authority could give a refusal notice under section 16(1) on the basis that the information was exempt information by virtue of any of sections 28 to 35, 38, 39(1) or 41 but the authority considers that to reveal whether the information exists or is so held would be contrary to the public interest, it may (whether or not the information does exist and is held by it) give the applicant a refusal notice by virtue of this section.

...

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

...

(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