Section 18 FOISA — a case of interest

Fiona Killen, Partner with Burness Paull LLP, considers a recent decision of the Scottish Information Commissioner involving the application of the provisions of section 18 FOISA by a Scottish University to neither confirm nor deny the existence of information, in relation to a request for information about an investigation into employee misconduct under a Research Misconduct Policy

Section 1 of the Freedom of Information (Scotland) Act 2002 ('FOISA') provides that a person who requests information from a Scottish public authority holding it in a recorded form is entitled to be given it by that authority. Unlike section 1 of the Freedom of Information Act 2000 ('FOIA'), the right in section 1 FOISA is not broken down into (a) a right for a requester to be informed as to whether a public authority holds requested information and (b) to have it communicated to the requester.

Section 18 FOISA provides public authorities with a general power to respond to an information request by issuing a notice under that section, neither confirming nor denying whether information exists or is held, in certain specified circumstances. This is in contrast to FOIA, where specific exemptions in different sections contain a formulation of the power to neither confirm nor deny, adapted to reflect the interests intended to be protected by each exemption.

There are two gatekeeping provisions within section 18 FOISA which must be considered before that power can be used.

The first is the requirement that section 18 can only be applied if the authority would be entitled to issue a refusal notice under section 16 FOISA, if the information did exist and was held, but was exempt under one or more of the following sections: 28 to 35, 38, 39(1) or 41 FOISA. The second is the requirement that a section 18 response can only be given in circumstances where the authority considers that to provide confirmation of whether or not information exists or is held would be contrary to the public interest.

Section 18 requires the application of a public interest test even where the specified exemption being relied upon is an 'absolute' exemption in terms of section 2 FOISA, i.e. where there is otherwise no requirement under FOISA to apply a public interest test in order to claim the exemption. An example of such an absolute exemption is the exemption in section 38(1)(b) FOISA which applies to third party personal data falling within the scope of a request.

Section 38(1)(b) provides that information is exempt from disclosure in response to a FOISA request if one of three conditions set out in section 38(2A) FOISA applies. One of these conditions is that disclosure of 'personal data', as defined in section 3(2) of the Data Protection Act 2018 ('DPA'), would contravene one or more of the data protection principles contained in Article 5(1) GDPR.

It is possible to envisage circumstances where an information request is made in such terms that an authority issuing a refusal notice under section 16 FOISA by applying the section 38(1)(b) exemption could in itself reveal personal data of individuals, and therefore breach one or more of the data protection principles. One example would be a request for information about a disciplinary process relating to an individual named in the request.

University of Edinburgh and a request regarding an employee misconduct investigation

Decision Notice 111/2021 (Case Ref: 202001288) (www.pdpjournals.com/docs/888178) concerned an information request that was wide-ranging in its scope, yet quite specific in its terms in relation to individuals. The request sought information about a misconduct investigation concerning a named individual at the University of Edinburgh.

It asked for details of all meetings held in relation to the matter, including date, time, name of attendees and full transcripts; details of all correspondence with a named Research Council; the names of all individuals involved in the matter including those providing witness accounts and evidence, but excluding members of the University's HR team; a list of all correspondence involving five named individuals and an individual described as a 'defendant'; and a complete list of evidence produced by the 'defendant'.

The University's response to the information request was given under section 18 of FOISA (read with sec-

tion 38(1)(b)) that, to respond other than under section 18 would involve disclosing third party personal data and, in so doing, would breach one or more of the data protection principles set out in Article 5(1) of the GDPR.

SIC's decision

In considering whether the University complied with its duties under FOISA, the Scottish Information Commissioner ('SIC') had to consider first the applicability of the exemption for third party personal data in section 38(1)(b) FOISA and then the public interest test.

As a first step, if section 38(1)(b) did not apply to the case (and no other specified exemption in section 8 applied), then the University could not rely on section 18.

The SIC decided that, if this information did exist and was held by the University, because the applicant named an individual and other third parties in the context of a misconduct complaint and investigation, any information captured by the request would relate to one or more named individuals and would be personal data as defined in section 3(2) DPA.

In terms of whether disclosure of such personal data under FOISA, i.e. disclosure into the public domain as a form of 'processing' (using the language of data protection law), would breach one or more of the data protection principles, the Decision Notice starts and ends its consideration of the data protection principles by reference to the first data protection principle, which requires personal data to be processed lawfully, fairly and transparently. Before commencing his analysis, the SIC noted that personal data could be disclosed if it would be both fair and lawful, including meeting one of the conditions of lawful processing listed in Article 6(1) GDPR. However, it is important to note that the exemption in section 38(1)(b) would apply if any of the requirements in the first data protection principle would be breached by disclosure of the requested information, e.g. the fairness, transparency or lawfulness requirements.

> ***"In circumstances where an authority is determining whether a disclosure under FOISA is lawful under the first data protection principle in Article 5(1), the GDPR's restrictions on the use of Article 6(1)(f) by public authorities in the performance of their tasks are to be omitted."***

The SIC thought that disclosure of the requested personal data, if it existed or was held, could only look to Article 6(1)(f) GDPR as a possible lawful basis for disclosure. This lawful basis is where disclosure 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.'

The restrictions placed on the use of Article 6(1)(f) by public authorities in the performance of their tasks by the GDPR are to be read as if those restrictions had been omitted from the GDPR, in circumstances where an authority is determining whether a disclosure under FOISA is lawful under the first data protection principle in Article 5(1). That qualification was added to FOISA in the form of new section 38(5A) FOISA, in a change made by the DPA 2018.

The Decision Notice lays out the approach taken by the SIC in considering whether Article 6(1)(f) could be met in this case, if the information existed or was held:

- would the Applicant have a legitimate interest in obtaining personal data, if held?
- if so, would the disclosure of the personal data be necessary to achieve that legitimate interest?
- 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?

This is a challenging exercise given that the application of Article 6(1)(f) is being tested not just in relation to the disclosure of information to the Applicant, but also the disclosure of information into the public domain. In the context of section 18, it is also challenging given that the interests, rights and freedoms of the data subjects can only be explained by reference to hypothetical circumstances, as to go any further could disclose the existence of requested information including personal data.

The SIC concluded that there was a legitimate interest in the information sought in the request, if it existed or was held, both for the applicant and the wider public. In terms of whether disclosure would be necessary to meet that interest, the SIC considered what was reasonably necessary, rather than absolutely or strictly necessary, i.e. proportionate as a means and fairly balanced as to the aims to be achieved. No alternative mechanism had been brought to the SIC's attention that offered the applicant (or the public) another way to understand the actions or decisions of the University in relation to the matters covered by the request.

In the balancing exercise between the legitimate interests in disclosure on the one hand, and the interests, rights and freedoms of those individuals identified or identifiable in the information request on the other, the SIC placed particular emphasis on the reasonable expectations that individuals would have in relation to any disclosure, including whether such information would relate to their public or private life, the potential for disclosure of their personal data to cause harm or dis-

(Continued on page 6)

(Continued from page 5)

tress and whether they would object to the disclosure. He concluded that the general expectation of the named individual and other third parties would be one of confidentiality or limited data sharing in the context of involvement in a process to consider alleged misconduct. Disclosure of such information into the public domain would be likely to result in reputational damage.

The SIC concluded that, if the information existed, the unwarranted prejudice to the rights and freedoms or legitimate interests of the identified or identifiable individuals would outweigh the legitimate interests in disclosing such information under FOISA. Disclosure would therefore be a breach of the first data protection principle in terms of the requirement for lawfulness, and such information would be exempt from disclosure under section 1(1) of FOISA by virtue of the exemption in section 38 (1)(b).

Having established that section 38(1)(b) could be claimed in this case, the SIC had to apply the test in section 18 to decide whether it would be contrary to the public interest for the University to reveal whether the information existed or was held.

Given that the public interest test under section 2(2) FOISA does not apply to the exemption relied upon in section 38(1)(b) in this case, and that confirming or denying the existence of the requested information would result in disclosure of personal data in breach of the data protection principles, it is difficult to see how the public interest in confirming or denying information could override the requirement to comply with data protection principles. If such a strong public interest existed, it would surely be recognised in the application of the condition in Article 6(1)(f) in relation to a FOISA disclosure, and tip the balance in favour of such a disclosure, therefore providing a lawful basis for disclosure.

In applying the public interest test in section 18 as was required, the SIC might simply be going through the motions in considering whether there was a public interest in revealing whether information existed and was held.

Whilst mention was made in the decision of certain public interest factors in favour of confirming or denying the existence of the requested information, it is difficult to see how the SIC could ever order disclosure of information where, by his own admission, it would breach a data protection principle.

The SIC's decision in this case was to uphold the application of section 18 FOISA, as to do otherwise would result in a breach of data protection principles and, for that reason if no other, would be contrary to the public interest.

Comment

This case does seem to support the view that the requirement to consider the public interest test under section 18 appears to be a somewhat redundant exercise where the exemption in section 38(1)(b) must be claimed because confirming or denying the existence of information would give rise to a breach of data protection principles.

In contrast to the level of detail required in a section 16 refusal notice, FOISA does not require authorities to say very much in a section 18 notice issued to applicants, for obvious reasons. Authorities seeking to rely on section 18 should nonetheless ensure that they keep an internal record of their decision-making that is sufficiently adequate to explain their approach, if required to do so by the SIC. This should include a clear articulation of the public interest factors they have considered in reaching their decision.

Fiona Killen
Burness Paull LLP
Fiona.Killen@burnesspaull.com