Decision Notice 012/2023

Cyber-attack on SEPA

Authority: Scottish Environmental Protection Agency
Case Ref: 202100872

Summary

The Applicant asked the Authority about the cyber-attack which occurred in 2020. The Authority provided some information to the Applicant, but withheld other information, and refused to confirm or deny whether certain information covered by the Applicant's request was held by it.

The Commissioner investigated and found that the Authority was entitled to withhold most of the information from the Applicant. The Commissioner also found that the Authority had not been entitled to argue that certain information was otherwise accessible to the Applicant or to refuse to confirm or deny whether specific information exists and is held by it.

The Authority changed its approach during the investigation, so the Commissioner did not require it to take any action.

Relevant statutory provisions

Freedom of Information (Scotland) Act 2002 (FOISA) sections 1(1), (2) and (6) (General entitlement); 17 (Notice that information is not held); 18(1) (Further provisions as respects responses to request); 25 (Information otherwise accessible); 30(c) (Prejudice to the effective conduct of public affairs); 35(1)(a) and (c) (Law enforcement); 47(1) and (2) (Application for decision by Commissioner)

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

Background

1. On 27 March 2021, the Applicant made a request for information to the Authority. He asked:

   a) for details of all statutory/regulatory datasets that the Authority was responsible for maintaining that remain inaccessible as a result of the attack. For each dataset affected, he asked the Authority to confirm the scope of the data that is inaccessible – this should include a description of the data, the volume of data that is inaccessible and the proportion of the dataset that is affected. (For example, if SEPA holds a 50 year dataset of pollution for a particular site, how much of it was affected by the attack, what proportion of it remains inaccessible, or how many years of it remain inaccessible?)

   b) for details of all statutory/regulatory datasets that are deemed by the organisation to be permanently lost as a result of the cyber-attack, including a description of the dataset, the proportion of the whole dataset lost, and the volume of missing data.

   c) for details of all statutory/regulatory datasets that were affected by the attack but have since been recovered and are fully accessible by staff and service users following the cyber-attack, including a description of the dataset, the proportion of each dataset affected by the attack that is now recovered and is accessible.

   d) for details of the costs incurred in mitigating the attack to date, including an itemised breakdown of external consultants/contractors that have been commissioned to work on the recovery process to date, a short summary of their role, and the amount each has been paid.

   e) the Authority to confirm whether, prior to the attack, it kept copies of statutory/regulatory datasets in secure, offsite, "cold" backups (i.e. backups that are not routinely connected to the same network) and, if so, whether these were also affected by the cyber-attack.

   f) for details of independent certifications in cyber-security, if any, that applied to the Authority at the time of the attack and, if they were held, for the documentation that outlines the standards the Authority was required to meet in order to comply with the certification standards and the documentation confirming compliance.

   g) the Authority to confirm whether any internal staff disciplinary action has been taken as a result of the security breach, or whether any external contractor will incur any penalty as a consequence of the cyber-attack.

2. The Authority did not respond to the Applicant's request for information.

3. On 28 April 2021, the Applicant wrote to the Authority requesting a review of its failure to respond to his information request.

4. An email, acknowledging the Applicant's request for review, was sent to him on 3 May 2021.

5. The Authority notified the Applicant of the outcome of its review on 7 July 2021. It:

   - acknowledged it had failed to provide a response to the Applicant's request within 20 working days

   - provided links to the Applicant to enable him to access publicly available information, on both its own, and the Scottish Parliament's website, which it considered may be of interest in relation to parts a) to c) and e) of his request

- withheld information which would fulfil parts a) to c) and e) of the Applicant's request as it considered it to be exempt under section 30(c) of FOISA
- with relation to part d) of the request, while the Authority withheld information under section 30(c) which would fulfil part of part d) of the request, it also relied on section 25 for information it stated was publicly available via links it provided
- the Authority also explained that it held a Cyber Essentials and Cyber Essentials Plus accreditation, but relied on section 25 of FOISA for refusing to provide copies of these, as it stated that these were otherwise accessible. Again, it gave the Applicant a link to a website where this information could be viewed.
- In response to part g) of the Applicant's request, the Authority refused to confirm or deny whether the information requested exists or is held by it (section 18(1) of FOISA).

6. On 20 July 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 Authority's review for the following reasons:
   - the handling of his request by the Authority was poor
   - the Authority's application of the exemptions to the requested information is erroneous
   - he did not believe that the parts of his request that the Authority had relied on section 25 for had been answered sufficiently by the publicly available information
   - there is a very strong public interest in understanding the impact of the cyber-attack on the Authority, and the Authority has been "less than transparent".

Investigation

7. The Commissioner determined that the application complied with section 47(2) of FOISA and that he had the power to carry out an investigation.

8. On 18 August 2021, the Authority was notified in writing that the Applicant had made a valid application. The Authority was asked to send the Commissioner the information withheld from the Applicant. The Authority provided the information and the case was allocated to an investigating officer.

9. Section 49(3)(a) of FOISA requires the Commissioner to give public authorities an opportunity to provide comments on an application. The Authority was invited to comment on this application and to answer specific questions. These related to the reasons why the Authority considered that disclosure of certain information would prejudice its ability to conduct its business effectively. Questions were also asked as to why the Authority was of the view that information in the public domain would assist in fulfilling some parts of the Applicant's request. Submissions were also sought around the Authority's decision to neither confirm nor deny whether certain information existed and was held by it.

10. During the course of the investigation, the Authority disclosed some information to the Applicant for which it had previously relied on the exemption in section 30(c) of FOISA. It also withdrew its decision to neither confirm nor deny whether particular information existed and was held which would fulfil part g) of the Applicant's request, and it released relevant

information to him. However, it explained that it was now relying on section 17 (information not held) in relation to information which would fulfil part of part f) of the request.

11. The Authority decided to disclose this information due to the passage of time and because of the progress it had made in its recovery from the cyber-attack.

12. The Applicant acknowledged receipt of this information, but explained that he still wanted a Decision from the Commissioner.

13. Further submissions were sought and received from the Authority. These led to the disclosure of some further information to the Applicant.

Commissioner's analysis and findings

14. The Commissioner has considered all of the submissions made to him by the Applicant and the Authority.

15. Although the Authority has now disclosed information to the Applicant, the Commissioner's decision focuses (as it is required to do) on the circumstances at the time the Authority responded to the Applicant's requirement for review.

Background

16. It has been well publicised that, on 24 December 2020, the Authority was subject to a cyber-attack which significantly impacted its organisation and affected its internal systems, processing and communications.

17. Since the attack, the Authority has worked with the Scottish Government, Police Scotland, the National Cyber Security Centre and the Scottish Business Resilience Centre to a clear recovery strategy.

18. This request is seeking information about the practical affect the cyber-attack has had on the Authority's ability to recover its data assets, the cost to it in doing so, what security it had in place at the time of the attack and whether any employees have faced disciplinary proceedings as a consequence of the attack.

Information out with scope of request

19. In its submissions, the Authority argued that certain of the information it had previously withheld from the Applicant did not fall within scope of the request.

20. Having considered this information, the Commissioner agrees with the Authority's conclusion. Therefore, certain information in document 1 and all of the information in document 2 will not be considered any further in this decision.

Section 17 – Notice that information is not held

21. In its submissions, the Authority explained that it is continuing to rely on section 25 of FOISA for information which confirms its compliance with cyber security standards (part f) of the request). However, in terms of the actual certificates themselves, it is seeking to rely on section 17 of FOISA as it states that it does not hold copies of these.

22. Under section 1(4) of FOISA, the information to be provided in response to a request under section 1(1) is that falling within the scope of the request and held by the authority at the time the request is received.

23. Under section 17(1) of FOISA, where an authority receives a request for information it does not hold, it must (unless it believes it has grounds to neither confirm nor deny whether the information is held, under section 18 of FOISA), give the applicant notice in writing to that effect.

Authority's submissions about section 17

24. The Authority explained that any information falling within scope of the request was held by a few specific people, and it detailed which individuals were asked to carry out searches for any information held which fell within scope of the request.

25. Searches were also carried out by external bodies who work with the Authority to determine if they held any copies of the certificates which evidence compliance with the requisite cyber security standards.

26. None of these searches led to the location of the certificates, with the external bodies confirming that they do not hold copies.

The Commissioner's view about section 17

27. The standard of proof to determine whether a Scottish public authority holds information is the civil standard of the balance of probabilities. In determining where the balance of probabilities lies, the Commissioner considers the scope, quality, thoroughness and results of the searches carried out by the public authority. He also considers, where appropriate, any reason offered by the public authority to explain why it does not hold the information.

28. Having considered all of the relevant submissions and the terms of part f) of the Applicant's request, the Commissioner accepts that the searches undertaken by the Authority were thorough and would have been likely to have led to the identification of the certificates if they had been held.

29. As a consequence, the Commissioner is satisfied that the Authority was entitled to notify the Applicant, in line with section 17 of FOISA that it did not hold some of the information (the certificates) requested in part f) of his request.

Section 25 – Information otherwise accessible

30. Under section 25(1) of FOISA, information which an applicant can reasonable obtain other than by requesting it under section 1(1) of FOISA is exempt information. The exemption in section 25(1) is absolute, in that it is not subject to the public interest test set out in section 2(1)(b) of FOISA.

31. In response to the Applicant's request, the Authority relied on section 25(1) of FOISA for information it considered would be of interest in response to the first part of part d) and all of part f) of the Applicant's request.

32. In the first part of part d) of his request, the Applicant asked for details of the costs incurred in mitigating the attack to date.

33. The Authority provided the Applicant with a link to a parliamentary question and answer, which was available on the Scottish Parliament website, which it stated was still accurate.

34. In part f) of his request, the Applicant asked for details of any independent certifications in cyber-security, if any, that applied to SEPA at the time of the attack. He also asked that, if they were held, for the documentation that outlines the standards SEPA were required to

meet in order to comply with the certification standards and the documentation confirming compliance.

35. The Authority explained that it holds a Cyber Essentials and Cyber Essentials Plus accreditation, and provided a link to enable the Applicant to access information about these via the National Cyber Security Centre (NCSC) website.

Applicant's submissions

36. In his submissions, the Applicant argued that the first part of part d) and part f) of his request had not been answered sufficiently by the publicly available information.

Authority's submissions about section 25

37. With regard to the information contained in the parliamentary question and answer that the Authority had provided the Applicant with a link to, in response to the first part of part d) of his request, the Authority submitted that this was the most relevant information that was available on this matter at the time, and it was already in the public domain.

38. As regards the information which would fulfil part of part f) of the Applicant's request, the Authority commented that, due to it updating its cyber security certification, evidence of this was no longer accessible via the NCSC website.

39. The Authority was satisfied, however, that the certification it held at the time of the cyber-attack was publicly available, via the link it had provided to the Applicant, when it responded to his request for review.

40. Although evidence of its compliance with cyber security requirements was no longer publicly accessible via the NCSC website, the Authority submitted that, in an updated response it made to the Applicant on 15 February 2022, it had provided links to an internal audit report, as well as to a report from the Scottish Business Resilience Centre, both of which referred to the certification being held by the Authority prior to the cyber-attack. Links were also provided to enable the Applicant to understand the standards that required to be met to attain certification.

The Commissioner's view on section 25

41. Having considered the scope of the first part of part d) and part f) of the Applicant's request, together with the information which is (and was) available via the links provided by the Authority, the Commissioner accepts that (at the time the Authority responded to the Applicant's request for review) the links given to the Applicant to enable him to access the NCSC website would have enabled him to see what accreditation it held. However, the Commissioner does not accept that this would have shown the standards that the Authority would have had to achieve to attain that accreditation, nor would it have allowed the Applicant to view the certificates.

42. That said, the revised response, issued to the Applicant on 15 February 2022, does confirm the level of cyber security certification that the Authority had in place prior to the cyber-attack, and also allows him to see the standards that had to be met to achieve that certification. The matter of the actual certificates has been addressed earlier in this decision.

43. The Commissioner is therefore not satisfied that, at the time of its response to the Applicant's request for review, information which would fulfil all of part f) of his request was otherwise accessible. However, the Commissioner does accept that the revised response issued to the Applicant did provide him with links to information which was otherwise accessible which

would go someway to fulfilling this part of his request. As a consequence, the Commissioner is not satisfied that the Authority was entitled to rely on the exemption in section 25(1) of FOISA for information which would fulfil part f) of the request.

44. With regard to information which would fulfil the first part of part d) of the Applicant's request, the Commissioner accepts the information contained in the parliamentary question and answer would go someway to fulfilling this part of the Applicant's request. He is therefore satisfied that the Authority was entitled to rely on section 25(1) of FOISA for this information.

45. The Authority relied on the exemption in section 30(c) of FOISA for information which would fulfil the rest of part d) of the Applicant's request as well as information which would fulfil parts a) to c) and e) of the request. The Commissioner will go on to consider this now.

Section 30(c) – Effective conduct of public affairs

46. Under section 30(c) of FOISA, information is exempt information if its disclosure would "otherwise" prejudice substantially, or be likely to prejudice substantially, the effective conduct of public affairs. This exemption is subject to the public interest test in section 2(1)(b) of FOISA. The word "otherwise" distinguishes the harm required from that envisaged by the exemptions in sections 30(a) and (b).

47. Section 30(c) is a broad exemption and the Commissioner expects any public authority applying it to show what specific harm would (or would be likely to) be caused to the conduct of public affairs by disclosure of the information, and how that harm would be expected to follow from disclosure.

48. There is no definition of "substantial prejudice" in FOISA, but the Commissioner considers the harm in question would require to be of real and demonstrable significance. The authority must also be able to satisfy the Commissioner that the harm would, or would be likely to, occur. Therefore, the authority needs to establish a real risk or likelihood of actual harm occurring as a consequence of disclosure at some time in the near (certainly foreseeable) future, not simply that the harm is a remote possibility.

49. As noted above, the Authority relied on the exemption in section 30(c) for withholding information which would fulfil parts a) to c), part of part d) and part e) of the Applicant's request. The Authority withheld all information in five documents and partial information in one document.

Authority's submissions on section 30(c)

50. The Authority submitted that, at the time of the Applicant's request, it was still acting under its Emergency Management Team arrangements and was very much in emergency response mode. It also stated that it was still at the early stages of the wider criminal investigation being undertaken by Police Scotland as well as a (UK) Information Commissioner's investigation into the impact of the cyber-attack on personal data.

51. The Authority argued that disclosing the information could have caused substantial prejudice to its ability to deliver its statutory purpose including in relation to its current or future cyber security arrangements. It is the Authority's contention that disclosure of the withheld information at the time when it was vulnerable and building back in emergency mode could have left it open to further attack by cyber criminals who it knew were keeping a close eye on everything it was doing publicly. The Authority was also concerned that any perceived vulnerability would be taken advantage of by criminals in the waste sector that it regulates.

52. Disclosure would also, the Authority argued, potentially reveal operational vulnerabilities which could encourage regulatory criminal behaviour. This could have a significantly detrimental effect on its ability to deliver its statutory purpose and cause harm to the environment.

53. With regard to the information withheld in document 5 at the time of its response to the Applicant's requirement for review, the Authority relied on the same arguments set out above. In addition, it also argued that detailing the substantial cost of mitigating the cyber-attack to date potentially incentivises cyber criminals and activist groups to target it, and other public bodies, for further cyber-attacks to cause financial and severe disruption to public services.

54. It also noted that, due to operational spending not being collated centrally, it was unable to provide a working estimate of spending to mitigate the impact of the cyber-attack as at 21 June 2021. Therefore, the Authority contended that having unverified, potentially inaccurate information publicly available would cause confusion and undue alarm, which could impact its ability to deliver its statutory purpose.

55. The Authority stated that, as a public body, it was accountable to both the Scottish Government for its budget and the Scottish Parliament to ensure the propriety and regularity of its finances. The Authority also asserted that staff would have to be diverted away from the emergency response priority to rebuild its finance, procurement and payroll system so that full and accurate costs of the cyber-attack could be established.

Applicant's submissions on section 30(c)

56. The Applicant did not accept that the information should be withheld under section 30(c) of FOISA.

The Commissioner's view on section 30(c)

57. Having considered the information in documents 1, 2, 3, 4 and 6, for which the Authority relied on the exemption in section 30(c) of FOISA, the Commissioner accepts that at the time the Authority responded to the Applicant's request for review most of this information would have been exempt from disclosure under section 30(c).

58. The Commissioner recognises the early stage that the Authority was at in terms of the investigation of the cyber-attack and building back its systems. He is satisfied that there was a realistic prospect of the harm anticipated by the Authority being caused as a direct result of the disclosure of most of the withheld information in response to this request. This would, or would have been likely to, prejudice substantially the ability of the Authority to carry out its day to day duties, which of course had to carry on, despite the affects of the cyber-attack. As a consequence, the Commissioner accepts that disclosure of most of the withheld information would prejudice substantially the effectiveness of the Authority and therefore the effective conduct of public affairs.

59. Having considered the information in document 5 (which was held by the Authority at the time of the response to the requirement for review), the Commissioner accepts that this would have given an insight into which systems/parts of systems were vulnerable and required attention to resolve and reinstate after the attack. The Commissioner also acknowledges that the withheld information provides an idea of the costs involved. Because, as stated above, this work was ongoing at the time of the Applicant's request and requirement for review, the Commissioner is satisfied that disclosure of this information

would, or would be likely to prejudice the Authority's ability to carry out its statutory functions effectively.

60. However, the Commissioner is not satisfied that disclosure of all of the withheld information in document 1 at the time the Authority responded to the request for review would cause the anticipated harm. This is because it is evident from reading page 1 of document 1 that certain data sets (details about which were included in the proceeding pages) had already been made publicly available by the Authority on its website in January 2021 (before the Applicant submitted his request). As a consequence, the Commissioner cannot accept that disclosure of that information on pages 2, 3, 4 and 5 of document 1 would be exempt from disclosure under section 30(c) of FOISA.

Public interest test - section 30(c)

61. As mentioned above, the exemption in section 30(c) is subject to the public interest test in section 2(1)(b) of FOISA. The Commissioner must therefore go on to consider whether, in all the circumstances of the case, the public interest in disclosing the information is outweighed by that in maintaining the exemption.

62. The public interest is not defined in FOISA, but has been described in previous decisions as "something which is of serious concern and benefit to the public", not merely something of individual interest. It has also been held that the public interest does not mean "of interest to the public" but "in the interests of the public", i.e. disclosure must serve the interests of the public.

63. The Authority recognised that as a taxpayer funded body it had a duty to be open and transparent, and that there is a public interest in its expenditure. It also acknowledged the public interest in its ability to regulate Scotland's environment and for the public to understand its processes.

64. Against this, however, the Authority argued that there is a greater public interest in withholding the information. The Authority advanced the same arguments it had relied upon in its reasoning for relying on section 30(c) of FOISA in support of this contention.

65. The Applicant argued that there is a very strong public interest in understanding the impact of the cyber-attack on SEPA.

The Commissioner's view on the public interest – section 30(c)

66. The Commissioner accepts there is a general public interest in ensuring transparency and accountability and a more significant one in understanding the effects of the cyber-attack on the Authority and its systems.

67. However, the public interest in disclosure must be balanced against the public interest in withholding the information. The Commissioner has accepted that disclosure would, or would be likely to, cause substantial prejudice to the effective conduct of public affairs, because the information could lead to the Authority being vulnerable to another attack and being unable to carry out its functions.

68. Given the significant impact of the cyber-attack on the Authority, there is a substantial public interest in understanding how well prepared the Authority was for such an attack, together with how quickly it had been able to recover, as well as the cost to it in doing so. There is, undeniably, a greater public interest in ensuring that the Authority was/and is able to recover and reinstate its systems as soon as possible without concern that potential vulnerabilities will be exposed and attacked. There is also clearly a greater public interest in ensuring that

any information relating to the costs incurred by the Authority in recovering and re-instating its systems is complete, accurate and verified.

69. On balance, therefore, the Commissioner is of the view that the public interest in withholding the information outweighs the public interest in disclosing it.

70. The Commissioner therefore finds that the Authority was entitled to withhold most of the information under section 30(c) of FOISA.

Section 18(1) – neither confirm nor deny

71. In its response to part g) of the Applicant's request (whether internal disciplinary action had been taken or whether contractors would incur any penalty as a consequence of the cyber-attack), the Authority refused to confirm or deny whether it held any information.

72. 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 which may or may not be held by it;
- 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;
- the authority considers that to reveal whether the information exists or is held by it would be contrary to the public interest.

73. Where an authority has chosen to rely on section 18, 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 authority, the authority would be justified in refusing to disclose that information by virtue of the exemptions in section 18.

74. In any case where section 18(1) is under consideration, the Commissioner must ensure that his decision does not confirm one way or the other whether the information requested actually exists or is held by the authority. This affects the ability of the Commissioner to comment on the reliance by the public authority on any of the exemptions listed in relation to section 18(1), or on other matters which could have the effect of indicating whether the information existed. The same applies to any submissions that are submitted by the Applicant.

75. In this case, during the course of the investigation, the Authority argued that the information, if it existed and was held, would be exempt from disclosure by virtue of sections 30(c), 35(1)(a) and 35(1)(c) of FOISA

76. It is not sufficient to claim that one or more of the relevant exemptions applies. Section 18(1) makes it clear that the authority must be able to give a refusal notice under section 16(1), on the basis that any relevant information (if it existed and were held) would be exempt information under one or more of the listed exemptions. Where the exemption(s) is/are subject to the public interest test in section 2(1)(b) of FOISA, the authority must also be able to satisfy the Commissioner that the public interest in maintaining the exemption(s) outweighs any public interest there would be in disclosing any relevant information it held.

77. The Commissioner must first, therefore, consider whether the Authority could have given a refusal notice under section 16(1) in relation to the information in question, if it existed and were held.

Section 30(c) – Effective conduct of public affairs

78. Paragraphs 46 to 48 set out the tests that must be fulfilled to successfully argue that information is exempt from disclosure under section 30(c) of FOISA.

Authority's submissions on section 30(c)

79. The Authority submitted that, were it to confirm or deny whether the requested information existed and was held, this could jeopardise its ability to fulfil its statutory purposes.

Applicant's submissions on section 30(c)

80. In his application to the Commissioner, the Applicant argued that the Authority had applied exemptions erroneously to the information he had requested.

The Commissioner's view on section 30(c)

81. Having considered all of the submissions on this point, the Commissioner is not satisfied that the Authority has provided a detailed enough argument to demonstrate why specifically, confirming or denying whether the information exists or is held, would have been detrimental at the time it responded to the Applicant's requirement for review.

82. For that reason, the Commissioner is unable to agree that such disclosure (if the information exists and was held) would have a prejudicial effect on the Authority. Therefore, the Commissioner cannot accept that the Authority would have been able to rely on the exemption in section 30(c) of FOISA for this information (if it exists and was held) at the time it responded to the Applicant's requirement for review.

83. As the Commissioner is not satisfied that the Authority would have been able to rely on the exemption in section 30(c) of FOISA, he is not required to go on to consider the application of the public interest test in section 2(1)(b).

84. As the Authority has stated that it also wishes to rely on section 18(1) in conjunction with sections 35(1)(a) and 35(1)(c) of FOISA, the Commissioner will now go on to consider whether those exemptions would apply in the event that the information existed and were held.

Section 35(1)(a) – Law enforcement (prevention and detection of crime)

85. Under section 35(1)(a) of FOISA, information is exempt information if its disclosure would, or would be likely to, prejudice substantially the prevention and detection of crime. As the Commissioner's guidance on section 35 notes[1], the term "prevention and detection of crime" is wide ranging. It encompasses actions taken to anticipate and prevent crime, or to establish the identity and secure prosecution, of people suspected of being responsible for committing a crime. This could mean activities in relation to a specific (anticipated) crime or wider strategies for crime reduction and detection.

86. The exemption in section 35(1)(a) can only apply where disclosure of the information in question would, or would be likely to, prejudice substantially the prevention or detection of crime. FOISA does not define "substantial prejudice", but, as noted above, the

[1] BriefingSection35LawEnforcement.pdf (itspublicknowledge.info)

Commissioner considers an authority would have to identify harm of real and demonstrable significance. The harm would also have to be at least likely and, therefore, more than a remote possibility. The Authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice the exemption is designed to protect against.

87. This exemption is subject to the public interest test in section 2(1)(b) of FOISA.

Authority's submissions on section 35(1)(a)

88. The Authority submitted that confirming or denying whether the requested information exists and was held by it could impact the ongoing Police Scotland criminal investigation into the cyber-attack, particularly given that the information request was received shortly after the attack.

Applicant's submissions on section 35(1)(a)

89. In his application to the Commissioner, the Applicant argued that the Authority had applied exemptions erroneously to the information he had requested

The Commissioner's view on section 35(1)(a)

90. Having considered the submissions from both the Applicant and the Authority, the Commissioner cannot accept that the information (if it existed and was held) would be exempt from disclosure under section 35(1)(a) of FOISA.

91. Within its submission, the Authority has not explained how confirming or denying that disciplinary action was taken or a penalty incurred by an external contractor would impact the ongoing investigation being carried out by Police Scotland. Nor has it shown how the timing of the Applicant's request in this case would make such a statement any more likely to lead to that harm occurring (if the information existed and was held).

92. In the absence of any specific submission, the Commissioner cannot uphold the Authority's contention that it could rely on section 35(1)(a) of FOISA for exempting this information from disclosure if it existed and was held.

93. Because the Commissioner is not satisfied that the Authority would have been able to rely on the exemption in section 35(1)(a) of FOISA, he is not required to go on to consider the application of the public interest test in section 2(1)(b).

Section 35(1)(c) – Substantial prejudice to the administration of justice

94. Under section 35(1)(c) of FOISA, information is exempt information if its disclosure would, or would be likely to, prejudice substantially the administration of justice.

95. The Commissioner's guidance on section 35[2] notes, at paragraph 22, that "administration of justice", although not defined in FOISA, will include the protection of basic rights such as the right to a fair trial and ensuring individuals have access to justice.

96. This exemption is subject to the public interest test in section 2(1)(b) of FOISA.

[2] BriefingSection35LawEnforcement.pdf (itspublicknowledge.info)

Authority's submissions on section 35(1)(c)

97. The Authority relied on the same submission set out above in relation to section 35(1)(a) of FOISA, to justify its view that the information (if it exists and was held) would be exempt under section 35(1)(c).

Applicant's submissions on section 35(1)(c)

98. In his application to the Commissioner, the Applicant argued that the Authority had applied exemptions erroneously to the information he had requested

The Commissioner's view on section 35(1)(c)

99. For the same reasons expressed in paragraphs 91 to 93 above, the Commissioner does not agree that the Authority was entitled to argue that the requested information (if it exists and was held) would be exempt from disclosure under section 35(1)(c) of FOISA.

100. Because the Commissioner is not satisfied that the Authority were entitled to rely on the exemption in section 35(1)(c) of FOISA, he is not required to go on to consider the application of the public interest test in section 2(1)(b).

Section 18: outcome

101. As a consequence of the Commissioner not agreeing that the Authority could rely on the exemptions in sections 30(c), 35(1)(a) and 35(1)(c) of FOISA for information covered by part g) of the request (if it exists and was held), he does not accept that the Authority could give a refusal notice under section 16(1) of FOISA. As a result, the Commissioner is not required to go on to consider whether the Authority was entitled to conclude that it would be contrary to the public interest to reveal whether the information existed or was held.

102. The Commissioner therefore finds that the Authority was not entitled to rely on section 18(1) of FOISA for refusing to confirm or deny whether specific information existed or was held which would fulfil part g) of the Applicant's request.

Decision

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

The Commissioner finds that the exemptions in sections 25 and 30(c) applied to certain of the information which would fulfil the Applicant's request.

However, the Commissioner finds that not all of the information for which the Authority relied on section 25 of FOISA was otherwise accessible to the Applicant. Furthermore, the Commissioner also finds that not all of the information withheld in document 1 was exempt from disclosure under section 30 (c) of FOISA. This was a breach of Part 1 of FOISA.

The Commissioner also finds that the Authority was not entitled to refuse to confirm or deny whether specific information existed and was held by it. This was a breach of section 18(1) of FOISA.

During the investigation, the Authority provided up to date links to information available in the public domain; disclosed certain information in document 1 which had previously been withheld and confirmed whether information was held in relation to request g), the Commissioner does not require the Authority to take any action in respect of these failures.

Appeal

Should either the Applicant or the Authority 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

15 February 2023

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.

(2) The person who makes such a request is in this Part and in Parts 2 and 7 referred to as the "applicant."

…

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

17 Notice that information is not held

(1) Where-

(a) a Scottish public authority receives a request which would require it either-

(i) to comply with section 1(1); or

(ii) to determine any question arising by virtue of paragraph (a) or (b) of section 2(1),

if it held the information to which the request relates; but

(b) the authority does not hold that information,

it must, within the time allowed by or by virtue of section 10 for complying with the request, give the applicant notice in writing that it does not hold it.

…

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.

…

25 Information otherwise accessible

(1) Information which the applicant can reasonably obtain other than by requesting it under section 1(1) is exempt information.

(2) For the purposes of subsection (1), information-

(a) may be reasonably obtainable even if payment is required for access to it;

(b) is to be taken to be reasonably obtainable if-

(i) the Scottish public authority which holds it, or any other person, is obliged by or under any enactment to communicate it (otherwise than by making it available for inspection) to; or

(ii) the Keeper of the Records of Scotland holds it and makes it available for inspection and (in so far as practicable) copying by,

members of the public on request, whether free of charge or on payment.

(3) For the purposes of subsection (1), information which does not fall within paragraph (b) of subsection (2) is not, merely because it is available on request from the Scottish public authority which holds it, reasonably obtainable unless it is made available in accordance with the authority's publication scheme and any payment required is specified in, or determined in accordance with, the scheme.

30 Prejudice to effective conduct of public affairs

Information is exempt information if its disclosure under this Act-

…

(c) would otherwise prejudice substantially, or be likely to prejudice substantially, the effective conduct of public affairs.

35 Law enforcement

(1) Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice substantially-

(a) the prevention and detection of crime;

…

(b) the administration of justice

…

47 Application for decision by Commissioner

(1) A person who is dissatisfied with -

(a) a notice under section 21(5) or (9); or

(b) the failure of a Scottish public authority to which a requirement for review was made to give such a notice.

may make application to the Commissioner for a decision whether, in any respect specified in that application, the request for information to which the requirement relates has been dealt with in accordance with Part 1 of this Act.

(2) An application under subsection (1) must -

(a) be in writing or in another form which, by reason of its having some permanency, is capable of being used for subsequent reference (as, for example, a recording made on audio or video tape);

(b) state the name of the applicant and an address for correspondence; and

(c) specify –

(i) the request for information to which the requirement for review relates;

(ii) the matter which was specified under sub-paragraph (ii) of section 20(3)(c); and

(iii_ the matter which gives rise to the dissatisfaction mentioned in subsection (1).

…