Decision Notice

Decision 198/2016: Mr Geoff White and Glasgow City Council

Ransomware infections

Reference No: 201601025
Decision Date: 19 September 2016

Scottish Information Commissioner

Summary

On 2 April 2016, Mr White asked Glasgow City Council (the Council) whether any of its IT equipment had been infected by ransomware in the previous three years.

The Council informed Mr White that the information was exempt from disclosure in terms of section 35(1)(a) of FOISA.

The Commissioner investigated and found that the Council did not hold the information requested. During the Commissioner's investigation, the Council submitted that the information was in fact held in a recorded format and was exempt from disclosure: the Commissioner did not accept this.

The Commissioner found that the Council was not entitled to apply an exemption to information it did not hold. The Council should have either given Mr White due notice that the information was not held, or applied section 18 to neither confirm nor deny whether the information existed or was held.

Relevant statutory provisions

Freedom of Information (Scotland) Act 2002 (FOISA) sections 1(1) and (4) (general entitlement); 16(1) (Refusal of request); 17(1) (Notice that information is not held); 73 (Interpretation) (definition of "information")

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 2 April 2016, Mr White made a request for information to the Council. The information requested was as follows:

   (i) In the last three years, has any of the Council's IT equipment been infected by so-called ransomware (malicious software that encrypts files and then demands payment in order for the files to be decrypted; examples include Cryptolocker, Cryptowall, CryptoDefense, Locky)?

   (ii) If so, how many infections have been detected?

   (iii) If so, what information was affected?

   (iv) If so, has the Council paid money in order to have the files decrypted?

   (v) If so, how much money was paid and by what means?

2. The Council responded on 4 April 2016. In relation to parts (i) to (iii) of the request, the Council informed Mr White that the information requested was exempt from disclosure in terms of section 35(1)(a) of FOISA. This was on the basis that disclosure of the information would, in the Council's view, be likely to prejudice substantially the prevention of crime. In relation to parts (iv) and (v) of the request, the Council informed Mr White that it had never made any such payment.

3. On 7 April 2016, Mr White wrote to the Council requiring a review of its decision. Mr White stated that he had received clear responses to the same request from other local authorities. In his view, the Council's refusal to provide the information jeopardised the reputations of those local authorities which had complied with his requests, as it could be inferred erroneously that their IT security systems were weaker than those of the Council. He submitted that it was in the interests of Council Tax payers to know if the Council was not following good practice in responding to such attacks. Mr White did not express dissatisfaction with the Council's response to parts (iv) and (v) of his request.

4. The Council notified Mr White of the outcome of its review on 5 May 2016. The Council upheld its previous decision without modification.

5. On 27 May 2016, Mr White wrote to the Commissioner. He applied to the Commissioner for a decision in terms of section 47(1) of FOISA. Mr White stated he was dissatisfied with the outcome of the Council's review. He stated that he had submitted identical information requests to a large number of public authorities, the vast majority of which had provided responses confirming whether or not they had been subject to such attacks. He also considered it was in the public interest to know whether the Council had successfully repelled or mitigated such attacks.

Investigation

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

7. On 20 June 2016, the Council was notified in writing that Mr White had made a valid application. The Council was asked to send the Commissioner the information withheld from Mr White. In response to her, the Council appeared to stating that, as far as it was aware, it had no record of its IT equipment being infected by ransomware. 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 Council was invited to comment on this application and answer specific questions, with particular reference to the steps it had taken to establish what relevant information (if any) it held.

9. At this stage, the investigating officer indicated to the Council that the Commissioner would not accept the application of an exemption to information that was not held. The investigating officer suggested to the Council that it should consider providing a further response to Mr White, informing him that it held no record of its IT systems being infected by ransomware.

10. In response, the Council refuse to accept that it did not hold the information and provided submissions in support of its position. This is considered in what follows.

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 her by both Mr White and the Council. She is satisfied that no matter of relevance has been overlooked.

12. In his requirement for review, Mr White did not express dissatisfaction with the Council's response to parts (iv) and (v) of his request. Consequently this decision notice considers only parts (i) to (iii).

Did the Council hold any information for the purposes of FOISA?

13. The Council's position, as stated to the Commissioner, was that there were no infections of its IT equipment by ransomware recorded. The Council submitted that this in itself comprised recorded information and was exempt from disclosure in terms of section 35(1)(a) of FOISA.

Searches undertaken by the Council

14. The Council explained the searches it had undertaken. These included searches of relevant anti-virus logs, registers and systems. None recorded any instance of ransomware infections.

15. The Council explained that the searches had been conducted by its IT provider and the search activity was coordinated by its IT Security Architect. If there were any records of ransomware infection across the Council, its IT provider would have been made aware of it and the key officer would have been involved personally in containment and remediation efforts. This officer had no recollection of the Council ever being infected by ransomware, over and above the formal searches that had been undertaken and instructed.

16. The Council explained that, if a ransomware infection had materialised, it would have rendered a large part of its electronic records unusable. Therefore, it would have been very difficult for any member of staff who had inadvertently allowed malware into the network to conceal the fact and remediation could only be effected by staff with IT administrator privileges, who would have recorded their involvement on Remedy. Any request for a ransom would have been passed to senior staff in Financial Services, who would have alerted Internal Audit and the IT provider.

17. The Council explained also that its automated monitoring was checked for evidence of ransomware infection, including for signs of infection which had not previously manifested themselves and which the Council might otherwise have been unaware of. The Council stated it was inconceivable that a successful ransomware infection of its systems could have occurred without being picked up by one or more of these searches.

18. The Commissioner has considered the Council's submissions and its explanation of the searches and enquiries undertaken in this case. Having done so, she is satisfied that the Council made reasonable, proportionate enquiries to establish whether it held any relevant information. She accepts that any evidence of successful ransomware infections would have been identified as a result of these enquiries and searches.

Definition of "information"

19. Section 73 of FOISA defines "information" (subject to conditions that are not relevant here) as meaning information recorded in any form.

20. The Council submitted that it did hold the information sought by Mr White. It argued that there was a distinction between information not being held and recorded information showing that the answer was zero ransomware infections.

21. In the Council's view, the logs to which it had referred constituted recorded information. The Council submitted that the fact that none of the entries on the log recorded a ransomware

infection meant the Council held recorded information answering the question posed by Mr White, the answer to which was zero. The Council stated that the log would record instances of ransomware infection and so the log was, in its view, the source of recorded information indicating that the answer was zero ransomware infections.

22. The Council submitted also that the anti-virus logs were another source of recorded information held, showing that its networks were attacked by ransomware that was successfully blocked.

23. In the Council's view, had it informed Mr White that it did not hold the information requested, this would have indicated that it was unable to determine whether or not its IT equipment had been infected by ransomware. In the Council's view, this would have been misleading.

24. In the Commissioner's view, the definition of information contained in section 73 of FOISA is unequivocal: it can apply only to information that is held in recorded form. She does not accept that the absence of information comprises "information" for the purposes of FOISA (as the Council has argued). It is not enough that there is a place in an electronic system where that information might be recorded, if there is nothing there: that would make no more sense than arguing that an empty (but labelled) drawer in a filing cabinet contained recorded information of the category indicated on the label. In the Commissioner's view, the absence of recorded information can only mean that information is not held for the purposes of FOISA. There is a distinction to be drawn between inferring an "answer" and identifying actual recorded information that gives that answer.

25. While the Council referred to logs as being recorded information, it did not provide this beyond describing it. Nor did it provide, or refer to, any reports (e.g. management or governance) where this was reported.

26. The Commissioner does not accept that a Scottish public authority can apply an exemption to information which is not recorded (and therefore is not held). The provisions in section 16(1) of FOISA, which relate to refusing a request under an exemption, apply only where the information in question is held. Where the information is not held, and the authority does not choose to apply section 18 of FOISA, the position is clear: section 17(1) of FOISA requires the authority to give the applicant notice to that effect.

27. The Commissioner is satisfied therefore, on the balance of probabilities, that the Council did not (on receiving the request) hold the information sought by Mr White. In such circumstances, the appropriate response from the Council should have been either to give notice to this effect, as required by section 17(1) of FOISA), or to have applied section 18 to say that it was not in the public interest to either confirm or deny whether the information existed or was held. By failing to do so, the Commissioner finds that the Council failed to comply with Part 1 (in particular section 1(1)) of FOISA.

28. While the Commissioner understands the Council's concerns about informing Mr White it did not hold recorded information, she would remind the Council that it was open to it to provide advice and assistance to Mr White, explaining why and, if it chose to do so, answering his question.

Decision

The Commissioner finds that Glasgow City Council (the Council) failed to comply with Part 1 of the Freedom of Information (Scotland) Act 2002 (FOISA) in responding to the information request made by Mr White.

The Commissioner finds that the Council did not hold the information requested. She finds that the Council failed to give an appropriate response to Mr White in terms of Part 1 of FOISA, by giving notice either:

i) that it did not hold the information requested, in terms of section 17(1) of FOISA, or

ii) that it was not in the public interest to reveal whether the information existed or was held by the Council, in terms of section 18 of FOISA.

Appeal

Should either Mr White or Glasgow City Council 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.

Rosemary Agnew
Scottish Information Commissioner

19 September 2016

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.

…

(4) The information to be given by the authority is that held by it at the time the request is received, except that, subject to subsection (5), any amendment or deletion which would have been made, regardless of the receipt of the request, between that time and the time it gives the information may be made before the information is given.

16 Refusal of request

(1) Subject to section 18, a Scottish public authority which, in relation to a request for information which it holds, to any extent claims that, by virtue of any provision of Part 2, the information is exempt information must, within the time allowed by or by virtue of section 10 for complying with the request, give the applicant a notice in writing (in this Act referred to as a "refusal notice") which-

(a) discloses that it holds the information;

(b) states that it so claims;

(c) specifies the exemption in question; and

(d) states (if not otherwise apparent) why the exemption applies.

…

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.

…

73 Interpretation

In this Act, unless the context requires a different interpretation –

…

“information” (subject to sections 50(9) and 64(2) means information recorded in any form;

…

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

t 01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

www.itspublicknowledge.info