Freedom of Information Act 2000 (FOIA)

Decision notice

Date:	**13 January 2021**
Public Authority:	**The Information Commissioner**
Address:	**Wycliffe House** **Wilmslow** **SK9 5AF**

Decision (including any steps ordered)

1. The complainant has requested a copy of the Register of Relevant Digital Service Providers. The Information Commissioner's Officer ("the ICO") withheld the information, relying on section 44(1) of the FOIA to do so, because it believed that disclosure would breach the Data Protection Act.

2. The Commissioner's decision is that disclosure of the information would breach the Data Protection Act and therefore the ICO has correctly relied on section 44(1) of the FOIA to withhold it

3. The Commissioner does not require further steps.

Jurisdiction and nomenclature

4. This decision notice concerns a complaint made against the Information Commissioner. The Information Commissioner is both the regulator of the FOIA and a public authority subject to the FOIA. She is therefore under a duty, as regulator, to make a formal determination of a complaint made against her in her capacity as a public authority – a duty confirmed by the First Tier Tribunal. It should be noted however that the complainant has a right of appeal against the Commissioner's decision, details of which are given at the end of this notice. This notice uses the term "the ICO" to refer to the Information Commissioner dealing with the request, and the term "the Commissioner" when referring to the Information Commissioner dealing with the complaint.

Request and response

5. On 12 February 2020, the complainant wrote to the ICO and requested information in the following terms:

> *"Please could you disclose to me the register of Relevant Digital Services Providers maintained by you under regulation 14 of The Network and Information Systems Regulations 2018?"*

6. The ICO responded on 11 March 2020. It withheld the requested information because it considered that disclosure would breach section 132 of the Data Protection Act 2018 ("DPA2018") and therefore the information would be exempt under section 44(1) of the FOIA.

7. The complainant sought an internal review on 12 March 2020, he argued that section 132 did not provide a statutory bar to *any* disclosure of information, only that which was done without lawful authority. He contended that there was lawful authority for disclosure and hence the exemption had been mis-applied. Following an internal review the ICO wrote to the complainant on 2 May 2020. It upheld its position that section 44 of the FOIA would apply.

Scope of the case

8. The complainant contacted the Commissioner on 11 May 2020 to complain about the way his request for information had been handled.

9. The scope of this notice is to determine whether the ICO is entitled to rely on section 44(1) of the FOIA to withhold the requested information.

Background

10. Regulation 14 of the Networks and Information Systems Regulations 2018 ("the NIS Regulations") requires the ICO to keep and maintain a register of all "Relevant Digital Service Providers" ("RDSPs") which provide services in the United Kingdom.

11. In addition to registering with the ICO, RDSPs must also take steps to ensure that they have appropriate security measures in place to protect themselves and their customers from attack – particularly cyber attack.

12. The Commissioner did not seek a copy of the withheld information, but she did ask the ICO to explain what data fields were included on the register. The ICO explained that most of the data was the contact details

of the RDSPs, but the register also contained the date on which registration was sought and information about the types of activity each organisation carried out.

Reasons for decision

13. Section 1(1) of the FOIA states that:

> *Any person making a request for information to a public authority is entitled –*
>
> *(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and*
> *(b) if that is the case, to have that information communicated to him.*

14. Section 44(1) of the FOIA provides an exemption from disclosure for any information whose disclosure would either be otherwise prohibited by another piece of legislation or would constitute a contempt of court.

15. In this particular case, the ICO is relying on section 132 of the DPA2018 as the statutory bar preventing disclosure. Section 132(1) of that Act states that:

> *A person who is or has been the Commissioner, or a member of the Commissioner's staff or an agent of the Commissioner, must not disclose information which—*
>
> *(a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the Commissioner's functions,*
>
> *(b) relates to an identified or identifiable individual or business, and*
>
> *(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources,*
>
> *unless the disclosure is made with lawful authority.*

16. Section 132(3) of the DPA2018 makes it a criminal offence for any person to disclose information in contravention of section 132(1).

17. All the parties agree that the information in question has been provided to the ICO for the purpose of the discharge of its functions – specifically

its function under Regulation 14 of the NIS Regulations to maintain a register of RDSPs. It is also common ground that the information would identify individual businesses and is not already in the public domain. The central dispute to this complaint is whether the ICO would have lawful authority to disclose this information to the world at large.

18. In its internal review, the ICO highlighted Section 132 of the DPA2018 as being permissive legislation – that is that, even if the ICO *could* disclose information with lawful authority, the legislation does not *require* it to do so. The Commissioner agrees that this reading of the DPA2018 is correct – but the consequential reading of section 44 of the FOIA is not. If the ICO *can* disclose the information without violating the DPA2018 (ie. if it considers that it *would* have lawful authority to disclose), but *chooses* not to, that is not a statutory bar to disclosure – it is a bar imposed by the ICO and must therefore be justified by reference to a different exemption from the FOIA.

19. Therefore the question for the Commissioner to consider is whether lawful authority exists for disclosure of this information to the world at large. If it does, section 132 of the DPA does not prevent disclosure and, hence, section 44(1) of the FOIA is not engaged.

20. Section 132(2) of the DPA2018 sets out six possible gateways through which disclosure can take place with lawful authority:

> *For the purposes of subsection (1), a disclosure is made with lawful authority only if and to the extent that—*
>
> *(a) the disclosure was made with the consent of the individual or of the person for the time being carrying on the business,*
>
> *(b) the information was obtained or provided as described in subsection (1)(a) for the purpose of its being made available to the public (in whatever manner),*
>
> *(c) the disclosure was made for the purposes of, and is necessary for, the discharge of one or more of the Commissioner's functions,*
>
> *(d) the disclosure was made for the purposes of, and is necessary for, the discharge of an EU obligation,*
>
> *(e) the disclosure was made for the purposes of criminal or civil proceedings, however arising, or*
>
> *(f) having regard to the rights, freedoms and legitimate interests of any person, the disclosure was necessary in the public interest.*

21. Of these six gateways, the Commissioner considers that two (a and e) can be immediately dismissed. The ICO does not have the consent of the RDSPs involved to disclose the information, nor is it required to seek such consent. Equally, disclosure under FOIA is not a criminal or civil proceedings.

22. In relation to gateways b, c and d, the Commissioner notes that the requirement on the ICO to maintain a register is set down in UK law and that that law derives from an EU Directive (Directive 2016/1148). However, neither the NIS Regulations nor the associated Directive require the ICO to *publish* the register – only to maintain it. The Commissioner is not aware of any other reason why the ICO would need to publish the register to discharge its functions. She therefore considers that none of these gateways would apply.

23. All parties are therefore agreed that Section 132(2)(f) is the only gateway that is potentially relevant to this information.

24. The construction of this particular clause bears a striking similarity to the test the Commissioner uses when adjudicating whether section 40(2) of the FOIA would apply to personal data. Firstly, any legitimate (public) interests in disclosure must be identified; second, it must be demonstrated that disclosure to the world at large is "necessary" to achieve those interests and that there is no less-intrusive means by which the interests can be achieved; finally, if disclosure is necessary, the interests in disclosure must be balanced against the rights and freedoms of the subject(s) of the information.

25. Considering the close connection between section 40 of the FOIA and the DPA2018, the Commissioner therefore considers it both helpful and appropriate to adopt a very similar three-step framework for considering the matters at hand. First she must identify any public interests in disclosure of the requested information; second, she must determine whether disclosure to the world at large is necessary to meet the public interest(s); finally, she must balance the public interest against the rights, freedoms and legitimate interests of the RDSPs. Only if all three tests are satisfied will the lawful authority gateway be opened.

Public interest

26. In seeking an internal review the complainant argued that there was a "clear public interest" in knowing which RDSPs were on the register – although he did not elaborate on what this clear public interest was.

27. The Commissioner considers that customers of RDSPs would have an interest in knowing whether the organisation they were interacting with

was registered or not as, if it were, it would be required to meet cybersecurity standards, protecting its customers.

28. Secondly the Commissioner considers that there is also a public interest in understanding how the ICO is discharging its functions.

Necessity

29. In judging whether disclosure is necessary, the Commissioner adopts the same test that she does when adjudicating on section 40(2) complaints: necessary does not mean absolutely necessity, but it must be the least intrusive method of achieving the interest. Therefore if the legitimate interest can be met by less intrusive means, disclosure will not be necessary to satisfy the interest.

30. When considering necessity, the Commissioner must also bear in mind that disclosure under the FOIA is disclosure to the world at large – not just to the complainant.

31. In relation to the second interest, the Commissioner is not persuaded that disclosure of the entire register to the world at large is necessary to demonstrate that the ICO is discharging its functions correctly – either in relation to the NIS Regulations or more generally. The ICO is accountable to Parliament, the PHSO and other bodies – who would be able to intervene if it was not performing its statutory functions. The Commissioner is aware of no widespread concern that the ICO is failing to perform its duties and, in any case, accusations alone would not render disclosure necessary.

32. The ICO also noted that it had previously published some aggregated data around the register and the types of RDSP registered, but nothing which would identify an individual RDSP. The Commissioner considers that this further reduces any interest in the withheld information.

33. However, in relation to the first interest, the Commissioner accepts that this interest (understanding which organisations are or aren't RDSPs) could only be achieved by publication of, at least, the list of names of the RDSPs. She is therefore satisfied that the second test has been met and thus disclosure is necessary to satisfy the public interest.

Balancing

34. Even where disclosure is necessary, the lawful authority gateway would still not be opened unless the public interest overrides the rights, freedoms and legitimate interests of the organisations that comprise the RDSP register.

35. Whilst the wording of DPA2018 refers to the "public interest", the Commissioner does not consider that this is equivalent to the sort of public interest test she is required to assess when considering a qualified FOIA exemption.

36. The Commissioner is guided in this approach by ruling of the First Tier Tribunal in *Lamb v Information Commissioner* EA/2010/0108. The Tribunal was asked to consider the ICO's reliance on the equivalent gateway in the Data Protection Act 1998[1] as preventing disclosure. The Tribunal commented that:

> *"Although a determination under section 59(2)(e) is based on a public interest test it is a very different test from the one commonly applied by the Information Commissioner and this Tribunal under FOIA section 2(2)(b), when deciding whether information should be disclosed by a public authority even though it is covered by a qualified exemption. The test there is that disclosure will be ordered unless the public interest in maintaining the exemption outweighs the public interest in disclosure. Under section 59 the information is required to be kept secret (on pain of criminal sanctions) unless the disclosure is necessary in the public interest. There is therefore an assumption in favour of non-disclosure and we are required to be satisfied that a relatively high threshold has been achieved before ordering disclosure."*

37. The complainant argued that there was a public interest in disclosure and that disclosure would have a negligible impact on the rights, freedoms and legitimate interests of the RDSPs.

38. The complainant also argued that the ICO was relying (or not relying) on section 132 of the DPA2018 in an inconsistent manner. He pointed to the fact that the ICO publishes registration details of all data controllers in the United Kingdom and that it had recently published details about individual security breach reports. He argued that such disclosures involved no less (and, in some cases, more) interference with the rights and freedoms of the organisations whose details were disclosed than in

---

[1] Section 59 of the Data Protection Act 1998 was the equivalent provision of section 132 of the DPA 2018 and section 59(2)(e) of the 1998 Act, the equivalent of section 132(2)(f) of the 2018 Act. For completeness, the precise wording of the 1998 Act is below. The Commissioner does not consider there is any meaningful difference in how this provision of the two Acts should be interpreted:

> *(e) having regard to the rights and freedoms or legitimate interests of any person, the disclosure is necessary in the public interest.*

the present case. He argued that if the ICO's logic were being applied consistently, the disclosures he had cited would constitute criminal offences.

39. Whilst the Commissioner notes the complainant's arguments about consistency, she also notes that she is not permitted to consider the "reasonableness" or otherwise of a public authority citing a statutory bar to disclosure. This was confirmed in a binding ruling of the Upper Tribunal in *Ofcom v Morrissey & Information Commissioner* [2011] UKUT 116 (AAC). It is the public authority's responsibility to decide whether it does or does not wish to rely on a statutory bar. The Commissioner's only concern is to determine whether that statutory bar does or does not prevent disclosure of the information that has been requested.

40. To assist her in making an assessment of the potential interference with the rights, freedoms and legitimate interests of the data subjects, the Commissioner asked the ICO to explain what assessment it had made of the RDSPs' reasonable expectations about disclosure. The ICO noted that when an RDSP registers:

> *"We confirm receipt, but don't make a specific statement about the possible publication or otherwise of their submission. On that basis, the reasonable expectation of the service providers will be that the information has been provided to us for a specific function related to our role and with an implication that it will be held securely and not further disseminated unless there is a legal or statutory requirement or other very compelling reason for us to do so."*

41. The Commissioner also asked why disclosure might have a detrimental impact on the RDSPs and their rights and freedoms to go about their business. The ICO responded to say that:

> *"Primarily our concern is that identifying the organisations registered with us would increase their profile and exposure to hacking, phishing and social engineering attacks aimed at compromising or disrupting the services they provide. NIS is designed to minimise the likelihood and impact of just such disruption, and is predicated by the assumption that such disruption is a constant risk. While we accept that organisations who register with us are also likely to have an online presence, carry out marketing and through various other avenues disclose information about themselves to the public, we hold that disclosure by us of the register (minus personal data) would risk providing bad actors not only with a list of targets, but also with information useful for phishing and social engineering attacks (for example, an email sent on the anniversary of their initial registration, purporting to appear to come from the ICO regarding an update to their registration*

details, designed to extract further information from them or persuade them to click on a link or download an attachment).

"The potential impact of such disruption extends to operators of essential services who rely on digital services to deliver critical economic and societal functions.

"There is potentially a wide variety of organisations on the register with different levels of capability, experience and resource to deal with the risk that heightened exposure would bring. Although there is a "carve-out" for micro and small enterprises within the NIS Regulations, the register may contain or come to contain details of a number of newer, smaller organisations that just tip over the "carve-out" threshold. A newer RDSP may for example not have exceeded those thresholds during its initial start-up phase but may have seen significant growth that now takes it over the thresholds, meaning NIS now applies and it needs to register; it may still have security that is less mature than older, larger, more established providers."

The Commissioner's view

42. Having considered the available evidence, the Commissioner is not satisfied that the gateway to disclosure at section 132(2)(f) of the DPA2018 is opened and therefore disclosure would be unlawful under DPA2018.

43. The Commissioner has issued a number of decision notices which considered whether disclosure of information was prohibited by the equivalent clause of the Data Protection Act 1998 and her approach in those cases has been upheld by the Tribunal.

44. What distinguishes the present request from the earlier ones is not so much that the legislation has changed (because the operative clause remains essentially the same) but that the nature of the information itself is different.

45. All the Commissioner's previous cases have, to some extent or other, involved information that was either acquired or created during the course of an investigation that the ICO had previously carried out. Very often this has involved a requestor seeking to use their FOIA rights to access previously-withheld information by a "back door" – which is, of course, part of the problem that section 132 seeks to avoid.

46. In those cases, the information had usually been provided, by the public authorities concerned, to the ICO, for the purpose of carrying out an investigation under section 50 of the FOIA – and the public authorities

concerned would have a reasonable expectation that any withheld or otherwise sensitive information would not be disclosed by the ICO.

47. In the present case, the information concerned has been acquired by the ICO as a result of RDSPs complying with their duty under the NIS Regulations to register with the ICO.

48. The Commissioner notes that any organisation or individual doing business with the ICO is (or, at least, should be) aware that the ICO is a public authority and thus subject to both the FOIA and the Subject Access Rights provisions of the DPA2018. She is also aware that the ICO, as an exemplar of information rights practices, regularly draws attention to this fact in its dealings with public authorities and data controllers. The Commissioner must therefore consider that any RDSP should have a reasonable expectation that information they provide has the potential to be disclosed under the FOIA – unless there are good reasons why it should be withheld.

49. Equally, the Commissioner is sceptical that the flow of information from organisations to the ICO will be harmed significantly by disclosure of the withheld information. Much of the information the RDSPs provide to the ICO, they do because they are required by the various provisions of the NIS Regulations. They will still be required to provide such information in the future, regardless of whether the ICO were to disclose the register. In terms of non-statutory engagement, the Commissioner considers that most sensible organisations will be able to draw a distinction between relatively mundane information (where there will be an expectation of disclosure) and information which is sensitive (where there will not be an expectation of disclosure), when determining what they will share with the ICO.

50. Whilst the wording of the legislation indicates that the Commissioner is able to take account of how the legitimate interests of the ICO might be affected by disclosure, she does not consider that they would be sufficiently damaged as to outweigh the public interest in disclosure.

51. However, the Commissioner has also had to have regard to the effects of disclosure of the rights and freedoms, both of the organisations who are named on the register and those who are not.

52. The purpose of the NIS Regulations is to protect important national infrastructure by ensuring that key providers of services are applying sufficient levels of security to the information and networks they maintain. The EU Directive that the NIS Regulations implement into UK law was aimed at ensuring that those standards were consistent across all the member nations of the EU.

53. The Commissioner accepts the ICO's argument that disclosing the register would provide would-be hackers with useful information that they could use to perpetrate cyber attacks. A potential hacker would be able to use the registration dates to identify targets providing key services which were more likely to have inadequate levels of security. Equally, providing information about the organisations who *are* on the register would simultaneously reveal the organisations who are *not* on the register – and hence not required to meet the required standards. That in turn could leave those organisations vulnerable to cyber attack.

54. The Commissioner notes that the fact that Parliament did not require the ICO to publish the register suggests that Parliament was not persuaded that the register should be published.

55. Finally, the Commissioner notes that, when the Government was consulting on the design of the NIS regulations, a number of organisations commented on the likelihood of competitive disadvantages occurring where particular organisations were stated to be "NIS-compliant." This would particularly disadvantage smaller providers who may risk being regarded as "less safe" than larger providers because they had not been labelled as "NIS-compliant" – even though they may not be required to register under the scheme.[2] Whilst the Commissioner does not consider such comments to be determinative, it is clearly of some concern within the relevant industries.

56. The Commissioner is thus satisfied that disclosure would interfere with the rights, freedoms and legitimate interests of the organisations on the register and others to go about their business unimpeded.

57. Given that the NIS Regulations were meant to improve security against the threat of cyber attacks, the Commissioner considers that there would be a strong presumption that information relating to the way organisations are complying with the regulations should not be disclosed without good reason.

58. The Commissioner notes the findings of previous Tribunals that the threshold for overriding the rights and freedoms of persons is a high one. She is not satisfied that the public interest in disclosure of this information is sufficiently strong in this particular case. As such she does not consider that the gateway for disclosure at section 132(2)(f) is

---

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677066/NIS_Consultation_Response_-_Analysis_of_Responses.pdf

opened and therefore any disclosure would take place without lawful authority.

59. As disclosure of this information could not take place with lawful authority, section 132(1) of the DPA2018 prohibits disclosure. It thus follows that section 44(1) of the FOIA will be engaged.

Right of appeal

60. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0300 1234504
    Fax: 0870 739 5836
    Email: grc@justice.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

61. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

62. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed

Phillip Angell
Group Manager
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF