Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **8 December 2020**

Public Authority: **The Home Office**
Address: **2 Marsham Street**
London
SW1P 4DF

Decision (including any steps ordered)

1. The complainant has requested two risk assessment documents from the Home Office. The Home Office refused to provide them, citing the exemptions at sections 31(1)(a) and (b) (Law enforcement), 23 (Information supplied by, or relating to, bodies dealing with security matters), 24 (National security) and 40 (Personal information) of the FOIA.

2. The Commissioner's decision is that section 31(1) is engaged and the public interest favours maintaining the exemption. No steps are required.

Background

3. The Home Office has advised that:

> *"The withheld information consists of two reports; one of which, created internally, by the NPIRMT* [National Policing Information Risk Management Team]*, the other externally, by Deloitte. The purpose of both, was to identify risks/threats (and the mitigations thereof), in relation to the Police use of Office 365, and the digital environment more broadly. This is part of the Police's strategic plan to ensure that all 48 police forces in the UK are digitally-enabled and Cloud ready by 2025".*

Request and response

4. On 1 November 2019, the complainant wrote to the Home Office and requested information in the following terms:

> *"I am writing to you under the Freedom of Information Act 2000 to request the following reports from the National Policing Information Risk Management Team (NPIRMT), the details/titles of which I will provide below:*
>
> *1. Office 365 for Policing - National SIRO Risk Decisions. There are two versions of this report, one from April 2017 and an updated version from January 2018.*
>
> *2. The risk assessment document for Office 365 that was completed by Deloitte.*
>
> *It is in the public interest for these documents to be released as the public deserves to know how police forces are ensuring the security of important data, as well as how they are assessing the risks of the solutions they choose.*
>
> *Please could you prioritise the requested information in the order listed above, and please could the reports be provided in an easily accessible format (either pdf or word if possible)?"*

5. The Home Office responded on 21 November 2019 and refused to provide the requested information, citing the following sections of the FOIA: 31(1)(a) and (b) (Law enforcement).

6. On 4 December 2019, the complainant requested an internal review. Following its internal review, the Home Office wrote to the complainant on 28 February 2020. It maintained its position.

7. On 28 September 2020, during the Commissioner's investigation, the Home Office revised its position. It added reliance on the following exemptions: section 23 (Information supplied by, or relating to, bodies dealing with security matters); section 24 (National security) and section 40 (Personal information) of the FOIA. It advised the complainant accordingly.

Scope of the case

8. The complainant contacted the Commissioner on 2 March 2020, to complain about the way his request for information had been handled. His grounds of complaint were as follows:

"*From my understanding there is nothing in the documents I am asking for that is marked confidential, and there is significant public interest in knowing what risks UK law enforcement are willing to accept with very sensitive data that, since the DPA 2018* [Data Protection Act]*, now has its own category. On top of this there were repeated delays in my appeal …*".

9. Following on from the Home Office's citing of further exemptions (see paragraph 7, above) the Commissioner asked the complainant to provide any further grounds of complaint. He responded as follows:

"*Firstly, I understand that a s.24 national security exemption needs to be approved by either the attorney general or a cabinet minister …*

On top of this, applying the s.24 exemption to the use of a commodity public cloud service, operated by a US national provider and supported by a range of staff of multiple nationalities on a global IT system, is ridiculous as the Home Office have not hidden that they are using these services and in doing so have intrinsically exposed themselves and their information to a level of disclosure that tends to undermine a National Security interest test.

Additionally, according to the GSCS here[1]*, paragraph 53 on page 35 expressly prohibits off-shoring of any data relating to National Security. From FOI'ing all forces implementing O365 I was sent this link*[2] *to the National Enabling Programmes data protection addendum with Microsoft, which explicitly says "Except as described elsewhere in the DPA, Customer Data and Personal Data that Microsoft processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its Subprocessors operate. Customer appoints Microsoft to perform any such transfer of Customer Data and Personal Data to any such country and to store and process Customer Data and Personal Data to provide the Online Services."*

If the Terms of Service have been accepted - and they appear to be based on my Force FOI returns as most of them provided this link -

[1]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

[2] https://uploads-ssl.webflow.com/5e6989f533b113f4745bd007/5f19fee0336ef960970ea052_Online-Service-DPA.pdf

then the data in scope cannot include anything relating to National Security interests, and this exemption cannot be used.

Secondly, I would also like you to consider that s.23 and s.24 are mutually exclusive (as per the ICO's guidance[3] on how they interact; please see para 25). In its response, the Home Office are seeking to apply BOTH S.23(1) and s.24(1) as a belt and braces approach - the ICO is pretty clear that this cannot be done unless they are specified as being 'in the contrary' - which I cannot see the Home Office have sought to do.

Thirdly, the s.40 argument presented by the Home Office regarding the need to with-hold the information on the grounds of public safety is an interesting one since I am in fact seeking to determine if Home Office have taken the diligence needed to ensure they comply with a legal obligation for a set of cloud services, which in themselves (via Schrems II and the ECJ [European Court of Justice] *judgement) have been identified to place the interests of the public at direct risk.*

On this point, I am also not seeking any personal information - the Home Office can easily obfuscate information relating to individuals who are not involved in the conduct of an official function, and from my understanding those who were fulfilling an official function are not intrinsically protected under this provision".

10. The Commissioner will consider the citing of exemptions below. She has referred to the time taken to conduct an internal review in 'Other matters' at the end of this notice. (It is also noted that a public authority is not required to seek approval from the attorney general or a cabinet minister in order to rely on section 24 of the FOIA).

11. The Commissioner has viewed the withheld information.

Reasons for decision

Section 31 – law enforcement

12. This has been cited in respect of the withheld information in its entirety.

[3] https://uploads-ssl.webflow.com/5e6989f533b113f4745bd007/5f19fee0336ef960970ea052_Online-Service-DPA.pdf

13. Section 31 of the FOIA creates an exemption from the right to know if disclosing the information would, or would be likely to, prejudice one or more of a range of law enforcement activities. Section 31 can be claimed by any public authority, not just those with law enforcement functions.

14. In order to engage a prejudice based exemption such as section 31, there must be the likelihood that disclosure would, or would be likely to, cause prejudice to the interest that the exemption protects. In the Commissioner's view, three criteria must be met in order to engage a prejudice based exemption:

- Firstly, the actual harm which the public authority alleges would, or would be likely to, occur if the withheld information was disclosed has to relate to the applicable interests within the relevant exemption;
- Secondly, the public authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice which the exemption is designed to protect. Furthermore, the resultant prejudice which is alleged must be real, actual or of substance; and,
- Thirdly, it is necessary to establish whether the level of likelihood of prejudice being relied upon by the public authority is met – ie disclosure 'would be likely' to result in prejudice or disclosure 'would' result in prejudice.

15. Consideration of the exemption at section 31 is a two-stage process: even if the exemption is engaged, the information should be disclosed unless the public interest in maintaining the exemption outweighs the public interest in disclosure.

16. In this case, the Home Office is relying on sections 31(1)(a) and (b) of the FOIA. Those subsections state that information is exempt if its disclosure would, or would be likely to, prejudice:

(a) the prevention or detection of crime;
(b) the apprehension or prosecution of offenders.

17. The Commissioner accepts that there is clearly some overlap between those subsection. As joint arguments have been submitted in respect of subsections (a) and (b), the Commissioner has considered these together.

The applicable interests

18. The first point for the Commissioner to consider is whether the arguments provided by the Home Office relate to the relevant applicable

interests, namely the prevention or detection of crime and the apprehension or prosecution of offenders.

19. The Home Office explained to the complainant that the documents were being withheld:

> *"… as there is the need to protect UK law enforcement activity and that it would not be in the interest of the UK's police forces to provide information about the risks and vulnerabilities in their IT systems. It was considered that disclosure could enable individuals to deduce how to conduct successful attacks against the systems"*.

20. It further explained that, having consulted the relevant business area,

> *"… the specific documents that you have requested contain sensitive information relating to the work of the police and the disclosure of what is contained within these documents could enable hackers to attack and possibly penetrate the network to access data. This could lead to the unauthorised disclosure of personal data and sensitive operational matters. This would prejudice law enforcement interests that are of paramount importance to the police and adversely impact on the prevention and detection of crime as well as the health and safety of police officers and members of the public".*

21. In corresponding with the Commissioner, the Home Office added further details, saying:

> *"… the withheld information consists of two reports which detail potential vulnerabilities/threats and associated risk, in the Police use of IT. The reports also detail mitigations intended to counter potential vulnerabilities/threats and associated risks.*
>
> *If this information was disclosed, it would reveal these risks, threats, and potential vulnerabilities and by doing so, would provide malicious actors with the information they would need to attempt to circumvent mitigations put in place to access sensitive Police information on the O365 platform, and/or instigate (cyber) attacks against the system more broadly.*
>
> *If such unauthorised access was obtained and/or some form of interference or attacks took place, these could have the potential to seriously disrupt the work of the police (and by extension, other law enforcement agencies … who, whether directly, or indirectly, rely on this platform (and the information contained within) to enable them to maintain law and order.*
>
> *If the circumstances described above were to occur as a result of disclosing the requested information, this would hinder the ability of*

the police and/or other law enforcement agencies in carrying-out their core functions – the prevention and detection of crime, in respect of section 31(1)(a), and/or equally, on their ability to apprehend or prosecute offenders of crimes, in respect of section 31(1)(b).

For example, once a risk or vulnerability is known (and the steps that can be taken to mitigate such), unwarranted access could be gained to the IT platform following an attack which could:

- *lead to the loss of availability of data on the O365 platform;*
- *prevent or delay the sharing of information in an effective and/or timely manner;*
- *jeopardize the integrity of the existing data stored on the platform;*
- *conceivably, lead to the loss of life.*

If any of these circumstances were to occur, the claimed prejudice would apply to at least one (though possibly both) of the sub-sections of section 31 which we are relying upon.

It would be the case that crucial information that law enforcement agencies rely upon, such as briefing documents, operational orders, sensitive intelligence reports etc. could now no longer be relied upon, which would hamper the ability of such agencies to do their job.

Furthermore, other key documents such as police training, tactics and methodologies used, for example, in policing public order events, or police use of firearms to name just two, could make such tactics less effective, or even ineffective, which could potentially place not only police officers at risk of serious injury or harm, but potentially the wider public too.

Likewise, warrants could be compromised, and evidence collated to prosecute could potentially be rejected by the Courts if interference has been shown to have taken place (or even just suspected to have taken place), thereby prejudicing the prosecution of offenders, potentially resulting in suspected criminals being released from detention, placing the public at greater risk of criminality and undermining confidence in the entire criminal justice system.

The above examples effectively demonstrate, in our view, why disclosure would prejudice law enforcement.

> *With increasing reliance on IT systems, and increases in cyber activity both at home and abroad (significantly as a result of COVID-19), together with the potential high profile nature of the target - the UK's Police Services - it is our view that the prejudice described above is clearly more likely than not to arise, even though it is not absolutely certain that it would do so, and so we wish to rely on the higher level of likelihood, 'would' prejudice".*

22. The Commissioner is satisfied that the arguments provided relate to the applicable interests cited so the first test is met.

The likelihood of prejudice

23. The Home Office has specified that it is relying on the higher threshold, that the prejudice envisaged 'would' occur, in this case.

Is the exemption engaged?

24. In a case such as this, it is not enough for the information to relate to an interest protected by sections 31(1)(a) and (b), its disclosure must also at least be likely to prejudice those interests. The onus is on the public authority to explain how that prejudice would arise and why it would occur.

25. Having considered the arguments put forward by the Home Office, the Commissioner accepts that the requested information would be useful to someone intent on establishing the risks and vulnerabilities in police IT systems, which would therefore be prejudicial to law enforcement.

26. Consequently, she is satisfied that its disclosure would represent a real and significant risk to law enforcement matters.

27. As the Commissioner accepts that the outcome of disclosure predicted by the Home Office would occur, she is therefore satisfied that the exemptions provided by sections 31(1)(a) and (b) are engaged.

Public interest test

28. Section 31 is a qualified exemption. The Commissioner must now consider whether, in all the circumstances of the case, the public interest in maintaining the exemption at sections 31(1)(a) and (b) of FOIA outweighs the public interest in disclosing the information requested by the complainant in part one of his request.

Public interest considerations favouring disclosure

29. The Home Office has argued:

"There is a public interest in understanding the risk assessment for cybersecurity in the Police use of Office 365. Disclosure would increase public awareness and reveal the extent of the challenges faced by the Police in trying to deliver world class public services whilst having to contend with attacks from malicious actors seeking to disrupt such important work.

Transparency on this issue would also allow the public to see how effective their money has been on measures in place to prevent such attacks. If the same information was requested for other public authorities, disclosure would provide an overall picture of the UK's ability to detect such crimes and could also increase public confidence in HM Government security".

Public interest considerations favouring withholding the information

30. The Home Office has argued:

"There is a very strong need to protect law enforcement activity. It would not be in the interest of the UK's Police forces to provide information about the risks to and vulnerabilities in their IT systems as this would enable individuals to deduce how to conduct successful attacks against the systems.

It is important to consider the broader picture, because if the same (or similar) information was revealed by other key public authorities, a UK-wide picture could be built-up of potential vulnerabilities.

Furthermore, it is to be reminded that any attempt to hack into an IT system is a criminal offence, and disclosure of known vulnerabilities could undermine any attempts by law enforcement agencies to identify, apprehend or prosecute offenders.

Releasing information which would allow malicious actors to potentially evade detection or arrest is not considered in the public interest, and hence the additional application of section 31".

Balance of the public interest arguments

31. In concluding its public interest test the Home Office found that:

"Disclosure under the FOIA is a release to the public at large and the safety of the public and, together with effective law enforcement, is of paramount importance and for the reasons outlined above, outweigh the public interest factors in favour of disclosure [sic]*".*

32. In reaching a view on where the public interest lies in this case, the Commissioner has taken into account the nature of the withheld information as well as the views of both the complainant and the Home Office.

33. The Commissioner has weighed the public interest in avoiding prejudice to the prevention or detection of crime and to the apprehension or prosecution of offenders, against the public interest in openness and transparency.

34. The Commissioner accepts that there is a presumption running through FOIA that openness is, in itself, to be regarded as something which is in the public interest. She also acknowledges the public interest arguments in favour of openness and transparency, and of scrutiny of policing methods.

35. The Commissioner considers that it is important that the general public has confidence in the police service, which is responsible for enforcing the law. Confidence will be increased by allowing scrutiny of how the police execute their duties and the technology that they use to do so. Accordingly, there is a general public interest in disclosing information that promotes accountability and transparency in order to maintain that confidence and trust.

36. It is noted that the complainant believes that: "*there is an overriding public interest in knowing if citizens' personal data is safe in the systems being used by police forces*". The Commissioner accepts that this is a strong and valid argument. However, this needs to be balanced against the harm to policing and the overarching responsibility to keep people safe by ensuring forces have effective IT capability without disclosing any vulnerabilities which have been identified and which could ultimately put the public at greater risk.

37. The Commissioner acknowledges the serious nature of the subject matter. She also recognises that the requested information is clearly of genuine interest to the complainant. However, disclosure under the FOIA is disclosure to the world at large. She must therefore consider whether the information is suitable for disclosure to anyone and everyone.

38. Clearly, disclosing information that may enable individuals seeking to conduct themselves improperly to adapt their behaviour, in order to evade detection, is not in the public interest. The Commissioner is also mindful that disclosure could allow those with criminal intent to exploit any current weaknesses, potentially leading to increasing numbers of victims of crime. This would be contrary to the policing purposes being relied on here, ie the prevention and detection of crime and the apprehension and prosecution of offenders.

39. In carrying out the statutory balancing exercise in this case, the Commissioner considers that appropriate weight must be afforded to the public interest inherent in the exemption - that is, the public interest in avoiding likely prejudice to law enforcement matters. Clearly, it is not in the public interest to disclose information that may compromise the police's ability to accomplish its core function of law enforcement.

40. In that respect, she recognises that there is a very strong public interest in protecting the law enforcement capabilities of a police force and she considers that appropriate weight must be afforded to the public interest inherent in the exemption – that is, the public interest in avoiding prejudice to the prevention or detection of crime and the apprehension or prosecution of offenders.

41. In the circumstances of this case, the Commissioner considers that the public interest in maintaining the exemption outweighs the public interest in disclosing the information. It follows that the Home Office was entitled to rely on sections 31(1)(a) and (b) of FOIA to refuse to disclose the requested information. As she has concluded that section 31(1) was properly cited, the Commissioner has not gone on to consider the other exemptions cited.

Other matters

42. Although they do not form part of this notice the Commissioner wishes to note the following.

Internal Review

43. The Commissioner cannot consider the amount of time it took a public authority to complete an internal review in a decision notice because such matters are not a formal requirement of the FOIA. Rather they are matters of good practice which are addressed in the code of practice issued under section 45 of the FOIA. However, the Commissioner has issued guidance in which she has stated that, in her view, internal reviews should take no longer than 20 working days to complete, and even in exceptional circumstances the total time taken should not exceed 40 working days.

44. In this case, the internal review was not completed in accordance with that guidance.

45. The Commissioner expects the Home Office to ensure that the internal reviews it handles in the future adhere to the timescales she has set out in her guidance.

46. The Commissioner will use intelligence gathered from individual cases to inform her insight and compliance function. This will align with the goal in her draft Openness by Design strategy[4] to improve standards of accountability, openness and transparency in a digital age. The Commissioner aims to increase the impact of FOIA enforcement activity through targeting of systemic non-compliance, consistent with the approaches set out in our Regulatory Action Policy[5].

[4] https://ico.org.uk/media/about-the-ico/consultations/2614120/foi-strategy-document.pdf

[5] https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

Right of appeal

47. 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

48. 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.

49. 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 ……

Carolyn Howes
Senior Case Officer
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF