Reference: 1665859

Information Rights
Information.requests@ofcom.org.uk

28 September 2023

Freedom of Information: Right to know request.

Thank you for your request for information about Ofcom's Storage and Cyber Security.

We received this request on 31 August 2023 and have considered it under the Freedom of Information Act 2000 ("the FOI Act").

Your request and our response

1. Storage
a. What is your annual spend on cloud storage and also on-prem storage (please split out the costs)
£225k annual spend including VAT for cloud storage. We no longer use On-prem storage.

b. Do you have a cloud strategy, if so when was it last assessed?
Yes, we have a Cloud first strategy. It is reviewed as part of the IT strategy on an ongoing basis.

c. How do you back up your data and with who e.g. Backup as a Service through XXX
The information you have requested is being withheld as we consider that it is exempt from disclosure under section 31(1)(a) of the FOI Act. This part of the act deals with information that, if disclosed would, or would be likely to, prejudice the prevention or detection of crime.

Section 31(1)(a) of the FOI Act is a qualified exemption which means that we have had to consider whether or not the public interest in disclosing the information you have requested outweighs the public interest in withholding the information. In this case, we consider the public interest favours withholding the information. The attached Annex A to this letter sets out the exemption in full, as well as the factors Ofcom considered when deciding where the public interest lay.

d. How much do you spend on data backup annually?
Approximately £160K including VAT for backup solutions over the last 12 months.

2. Security
a. How much do you spend on cyber security infrastructure?

We do not hold this information as security elements are part of bundles that we get from several service providers.

b. How many attempted cyber-attacks have you suffered?
There are approximately 30,000 attempted cyber-attacks per week.

c. How many successful cyber breaches have you suffered?
An Ofcom third party service, MOVEit, was subject to a successful breach. This was made public at the time.

d. If yes to 2c, did you pay the ransom and how long did it take for systems to come back online?
Ofcom have a policy of not paying a ransom. The impacted system was taken down for a few days while it was being secured.

e. If yes to 2c, were any of these ransomware attacks?
Yes, it was.

If you do not record the data by any of the above, please share the most similar you do record by. Please could provide data for the last 5 financial years. If you are unable to provide 5 years of data, please provide 3 years, otherwise please provide data for the last 2 years.

We have investigated your request and can confirm we do not hold information for 5 years. There has only been 1 successful breach in the last 5 years as mentioned in 1.c above. Average weekly hacking attempts have been 30,000 for the last 2 years.

I hope this information is helpful. If you have any further queries, then please send them to information.requests@ofcom.org.uk quoting the reference number above in any future communications.

Yours sincerely,

Information requests

If you are unhappy with the response you have received in relation to your request for information and/or consider that your request was refused without a reason valid under the law you may ask for an internal review. If you ask us for an internal review of our decision, it will be subject to an independent review within Ofcom.

The following outcomes are possible:
• the original decision is upheld; or
• the original decision is reversed or modified.

Timing
If you wish to exercise your right to an internal review **you should contact us within two months of the date of this letter**. There is no statutory deadline for responding to internal reviews and it will depend upon the complexity of the case. However, we aim to conclude all such reviews within 20 working days, and up to 40 working days in exceptional cases. We will keep you informed of the progress of any such review. If you wish to request an internal review, you should contact information.requests@ofcom.org.uk.

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. Further information about this, and the internal review process can be found on the Information Commissioner's Office here. Alternatively, the Information Commissioner can be contacted at:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Annex A

<table>
<tr><td colspan="2">Section 31 (1) of the FOI Act provides that:

Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice –

(a) the prevention or detection of crime;</td></tr>
<tr><td>Factors for disclosure</td><td>Factors for withholding</td></tr>
<tr><td>• Disclosure would promote general transparency with the public, increasing public confidence in how Ofcom operates.</td><td>Disclosure of detailed information about Ofcom’s IT systems may aid malicious parties to attack the systems concerned and compromise the security of our backup data.

Release of this information will prejudice the prevention of crime by facilitating the possibility of a criminal offence being carried out. Hacking into an IT system is a criminal offence.</td></tr>
<tr><td colspan="2">Reasons why public interest favours withholding information</td></tr>
<tr><td colspan="2">• We consider that, on balance, the public interest in withholding disclosure of the requested information outweighs the public interest in disclosing the information.

• Disclosure of detailed information about Ofcom’s IT systems could be used by offenders to hack into our systems. It is in the public interest for this not to happen to protect Ofcom against a potential cyber-attack so that Ofcom can carry on its work. The more specific any information is, the more useful it may be to an attacker.

• The consequences of any successful attack on Ofcom’s systems are significant. They include loss of personal data, confidential and commercially sensitive stakeholder and government information and access to it by third parties. This would also impair trust and confidence in Ofcom as a regulator and impact our ability to carry out our functions.</td></tr>
</table>