The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

1 May 2024

IC-298660-P1S6

Request

You asked us:

"1. Please provide the date on which the ICO started accepting proof of ID and address on its SAR tool form.

2. Please provide all the ICO's internal communications (including emails) to or from the team responsible for the SAR tool regarding the addition of the proof of ID and address functionality on the ICO's SAR tool.

3. Please provide the ICO's assessment regarding the security risks, and steps the ICO has taken to mitigate these, of requesters uploading proof of ID and address on the ICO's SAR tool and the ICO then sending these to the request recipient as attachments by email.

4. Please provide any advice ICO issues in its automated communication(s) sent to a data controller controller following a SAR submitted through the ICO's SAR tool, about the appropriate handling of the requester's proof of ID and address (e.g. in respect of retention, security measures etc.).

5. Please confirm what steps the ICO has taken, if any, to ensure that requesters' proof ID or address are not retained by Twilio, e.g. as random Sendgrid content samples (see https://ico.org.uk/global/privacy-notice/using-our-subject-access-request-service/)

6. Please provide the ICO's (equality) impact assessment for limiting its SAR tool's types of acceptable proof of ID to either a passport, driving licence or birth certificate; and types of acceptable proof of address to either a copy of a bank statement, utility bill, or TV licence.

The ICO's detailed SAR guidance states: "You can ask for enough information to judge whether the requester (or the person the request is made on behalf of) is the person that the data is about. The key point is that you must be reasonable and proportionate about what you ask for. You should not request more information if the requester's identity is obvious to you. This is particularly the case when you have an ongoing relationship with the individual. You should also not request formal identification documents unless necessary. First you should

think about other reasonable and proportionate ways you can verify an individual's identity." (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/what-should-we-consider-when-responding-to-a-request/)

The ICO's SAR guidance for small organisations states: "There's little point insisting on photo ID if you don't know what the requester looks like – it should be proportionate." (https://ico.org.uk/for-organisations/advice-for-small-organisations/how-to-deal-with-a-request-for-information-a-step-by-step-guide/)

There have also been numerous decisions by data protection supervisory authorities that it is not generally necessary or lawful for controllers to demand formal photo ID documents before responding to data subject requests. See for example page 37 of the Irish DPC's decision against Twitter: https://www.dataprotection.ie/sites/default/files/uploads/2022-07/Twitter%20International%20Company%20%20-%20Decision%20for%20publishing.pdf

7. Please provide any assessment the ICO holds of whether allowing and recommending that people upload proof of ID and address conforms with the above guidance and the data minimisation principle (Article 5(1)(c) UK GDPR).

8. Please provide any information about the steps the ICO takes to ensure it does not accept and send formal proof of ID and address, in cases where these are not necessary for the recipient organisation to deal with the request (and, as a consequence, their processing of such documents for that purpose would likely breach the UK GDPR).

9. Please provide the Information Commissioner's assessment of why, as a data controller, he considers it necessary to process and retain proof of ID and address for his public task when a person submits a request to different organisation through the ICO's SAR tool."

We have handled your request under the Freedom of Information Act 2000 (the FOIA).

Our response

We have searched our records based on the information you provided and can confirm that we hold information within the scope of your request.

For clarity, we have answered each of your questions in turn below. We have summarised some questions for ease of reading.

1. Please provide the date on which the ICO started accepting proof of ID and address on its SAR tool form.

The ICO started accepting ID and proof of address on its SAR tool form on 4 March 2024.

2. Please provide all the ICO's internal communications (including emails) to or from the team responsible for the SAR tool regarding the addition of the proof of ID and address functionality on the ICO's SAR tool.

Please find attached the internal correspondence to and from the SAR tool project team regarding the addition of proof of ID to the SAR tool. This includes emails regarding the project, as well as presentations for and notes from team meetings regarding the SAR tool. The correspondence is labelled 'IC-298660-P1S6 Disclosure – Q2 correspondence'.

Some correspondence has been withheld because it is exempt from disclosure under section 31 of the FOIA. This will be explained in more detail in response to question 3. Internal links and email addresses have also been redacted under section 31. However, the documents the internal links led to have been included in the disclosure bundle.

You will see that some of the third party personal data has been redacted in our response.

Section 40(2) of the FOIA exempts information if it is personal data belonging to an individual other than the requester and it satisfies one of the conditions listed in the legislation.

We find that the condition at section 40(3A)(a) applies in this instance: that disclosure would breach one of the data protection principles. The principles are outlined in the General Data Protection Regulation (GDPR) with the relevant principle on this occasion being the first principle as provided by Article 5(1): that personal data shall be processed lawfully, fairly and in a transparent manner.

We do not consider that disclosing this information into the public domain is necessary or justified. There is no strong legitimate interest that would override the prejudice to the rights and freedoms of the relevant data subjects. We have

therefore taken the decision that disclosing this information would be unlawful, triggering the exemption at section 40(2) of the FOIA.

Additionally, some correspondence has been redacted and withheld under section 42 of the FOIA. This will be explained below.

FOIA section 42

Some of the information you have requested is subject to legal professional privilege and is exempt from disclosure under section 42 of the FOIA. Section 42(1) of the FOIA states:

"Information in respect of which a claim to legal professional privilege or, in Scotland, to confidentiality of communications could be maintained in legal proceedings is exempt information."

There are two types of privilege covered by the exemption at section 42. These are:

- Litigation privilege; and
- Advice privilege.

Litigation privilege covers confidential communications between the client and lawyer made for the purpose of preparing for existing or anticipated legislation. Advice privilege covers such communications when they're made for the purpose of seeking or giving legal advice. We find that the information in scope of your request is subject to advice priviliege.

Section 42 is not an absolute exemption, so we must consider whether the public interest favours withholding or disclosing the information.

In this case the public interest factors in disclosing the information are:

Public interest factors in favour of disclosing the information are:

- The general public interest in the ICO being open and transparent as a regulator.
- The public interest in the reasons why the ICO decided to update the SAR tool in the way it did

Public interest factors in favour of maintaining the exemption are:

- The general public interest inherent in maintaining this exemption will always be strong due to the importance of the principle behind legal professional privilege.
- Disclosing legally privileged information threatens that principle.
- It is vital to safeguarding openness in all communications between client and lawyer, to ensure access to full and frank legal advice.
- The public interest is largely met through the disclosure of the other correspondence disclosed as it outlines the decision-making process regarding the SAR tool.

After consideration of the above factors, we conclude that the public interest in withholding this information outweighs the public interest in disclosing it.

No other information has been withheld or redacted from the internal communications for the SAR tool project team.

This concludes our response to this part of your request.

3. Please provide the ICO's assessment regarding the security risks, and steps the ICO has taken to mitigate these, of requesters uploading proof of ID and address on the ICO's SAR tool and the ICO then sending these to the request recipient as attachments by email.

Information regarding security risks associated with the SAR tool has been withheld from disclosure under section 31 of the FOIA.

Section 31(1)(a) of FOIA says:

Information is exempt if it's disclosure would *"likely prejudice:*

(a) The prevention or detection of a crime"

The security assessments for the SAR tool contain information regarding the ICO's cyber security systems. The disclosure of this information would directly impact our ability to perform our duties. This is because disclosure of this information to the wider world could create a security risk.

Clearly the ICO's capacity to defend itself from potential attacks relates to the purposes of crime prevention and thus s31(a) applies.

The exemption in section 31 is not absolute, and we must therefore consider the prejudice or harm which may be caused by disclosure of the information you

have requested. We must also conduct a public interest test by weighing up the factors in favour of disclosure against those in favour of maintaining the exemption.

In considering the prejudice or harm that disclosure may cause, we have taken into account the factors that would, in our view, impact on the release of the information.

Were the ICO to disclose the information about the specific security programs and protocols we use, it is likely that malicious parties could use the information to attack the ICO.

Please note that some information from the correspondence from Question 2 has also been withheld under section 31(1).

We have withheld internal email addresses and links in pursuant to section 31(1)(g) of the FOIA. This exemption refers to circumstances where the disclosure of information *"would, or would be likely to, prejudice…the exercise by any public authority of its functions for any of the purposes specified in subsection (2)."*

In this case the relevant purposes contained in subsection 31(2) are 31(2)(a) and 31(2)(c) which state:

" a. the purpose of ascertaining whether any person has failed to comply with the law, and
c. the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise."

We are satisfied that any misuse of internal non-public facing email addresses and internal links that exist to support ICO staff would likely prejudice our ability to perform our regulatory functions. Public disclosure would leave the email addresses vulnerable to phishing or other cyber-attacks, spam, or an increased volume of irrelevant correspondence which would divert resources to redirect correspondence to the relevant channels at the expense of assisting staff in matters of information security.

It may also help to explain that there are other channels that are more appropriate for the public to contact us through. These contact details are also publicly available via our website.

The exemption at section 31(1)(g) is not absolute. When considering whether to apply it in response to a request for information, there is a 'public interest test'. That is, we must consider whether the public interest favours withholding or disclosing the information.

In this case the public interest factors in favour of disclosing the information are as follows:

- General emphasis on transparency and increased transparency in the way in which the ICO conducts its investigations and its operations.

The public interest factors in maintaining the exemption are as follows:

- The public interest in maintain the ICO's ability to defend itself from secutiyy attack and thus continue to perform its public functions
- The public interest in the ICO's demonstrating good practice in not unduly facilitating the committing of crimes against it by maintaining its own security and system integrity.
- Internal email addresses being utilised for purposes contrary to their intended purpose will reduce the effectiveness and efficiency of our regulatory functions.
- The disclosure of internal email addresses isn't a critical part of the procedures and the information of primary relevance to the request is not affected by its redaction.

Having considered all of these factors we have taken the decision that the public interest in withholding the information outweighs the public interest in disclosing it.

This concludes our response to this part of your request.

4. Please provide any advice ICO issues in its automated communication(s) sent to a data controller controller following a SAR submitted through the ICO's SAR tool, about the appropriate handling of the requester's proof of ID and address (e.g. in respect of retention, security measures etc.).

Please find attached a test template of what is sent to data controllers when a SAR has been submitted through the ICO's SAR tool. It contains the guidance given to data controllers regarding their response. The form is labelled 'IC-298660-P1S6 Disclosure Q4 Letter to DCs'.

Some personal data has been redacted, for reasons explained under question 2.

This concludes our response to this part of your request.

5. Please confirm what steps the ICO has taken, if any, to ensure that requesters' proof ID or address are not retained by Twilio, e.g. as random Sendgrid content samples

Please find attached the DPIA for the SAR tool project, which outlines how the ICO will use Twilio as a part of this tool. The document is labelled 'IC-298660-P1S6 Disclosure - SAR tool DPIA'.

Some information regarding the ICO's cyber security has been redacted for the reasons explained above under question 3.

This concludes our response to this part of your request.

6. Please provide the ICO's (equality) impact assessment for limiting its SAR tool's types of acceptable proof of ID to either a passport, driving licence or birth certificate; and types of acceptable proof of address to either a copy of a bank statement, utility bill, or TV licence.

Please find a copy of the EQIA for the SAR tool attached. No information has been redacted from this document. The document is labelled 'IC-298660-P1S6 Disclosure – EQIA'.

7. Please provide any assessment the ICO holds of whether allowing and recommending that people upload proof of ID and address conforms with the above guidance and the data minimisation principle (Article 5(1)(c) UK GDPR).

This information is contained within the DPIA, which has been been attached, as well as in the attached correspondence bundle.

8. Please provide any information about the steps the ICO takes to ensure it does not accept and send formal proof of ID and address, in cases where these are not necessary for the recipient organisation to deal with the request (and, as a consequence, their processing of such documents for that purpose would likely breach the UK GDPR).

The uploading of proof of ID and address are not required to use the SAR tool. The use of this part of the tool is optional for all users. As described in the

attached documents, it was implemented following feedback from both data subjects and data controllers.

The requirement for proof of ID is made by data controllers on a case-by-case basis, as explained in our guidance. This means that the ICO cannot make a determination about whether or not a data controller will require ID until the request has been submitted.

This means that no information is held within the scope of this part of your request.

This concludes our response to this part of your request.

9. Please provide the Information Commissioner's assessment of why, as a data controller, he considers it necessary to process and retain proof of ID and address for his public task when a person submits a request to different organisation through the ICO's SAR tool.

Information regarding the SAR tool as part of the Commissioner's public task is described in the attached DPIA.

This concludes our response to your request. We hope this information is useful to you.

Next steps

You can ask us to review our response. Please let us know in writing if you want us to carry out a review. Please do so within 40 working days.

You can read a copy of our full review procedure here.

If we perform a review but you are still dissatisfied, you can complain to the ICO as regulator of the FOIA. This complaint will be handled just like a complaint made to the ICO about any other public authority.

You can raise a complaint through our website.

Your information

Our Privacy notice explains what we do with the personal data you provide to us, and set out your rights. Our retention schedule can be found here.

Yours sincerely

Information Access Team
Risk and Governance Department, Corporate Strategy and Planning Service
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
ico.org.uk twitter.com/iconews
Please consider the environment before printing this email