The ICO exists to empower you through information.

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

Date: 4 April 2024

IC-292189-Q2R4

Request

You asked us:

"I write in relation to the ICO's SAR tool available at https://ico.org.uk/for-the-public/make-a-subject-access-request/

When this was originally released, it did not allow nor recommend that requesters upload "proof of ID" (either a copy of a passport, driving licence or birth certificate), nor "proof of address" (either a copy of a bank statement, utility bill, or TV licence). However, I note that the initial page now states people "should" include these. The form itself also recommends uploading this information, but it is not clear why this is necessary or indeed recommended.

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) 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 to data controllers, 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 received your request on 5 March 2024. We have handled your request under the Freedom of Information Act 2000 (the FOIA).

Our response

Conducting the searches necessary to confirm if we hold the information you have asked for would exceed the cost limit set out by section 12 of the Freedom of Information Act 2000 (FOIA).

The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 states that the 'appropriate limit' for the ICO is £450. We have determined that £450 would equate to 18 hours work.

In particular, in point four of your request, you have asked for:

"*any advice ICO issues to data controllers, 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.).*"

Such advice could have been provided in a variety of contexts, including:

- A data controller could have emailed or called our Business Advice Service and made enquiries following receipt of a request submitted via our SAR tool;
- A data controller could have got in touch with us via Live Chat to request advice following receipt of a request submitted via our SAR tool;
- A member of the public could have complained about a company who did not respond to a SAR submitted via our SAR tool and we subsequently wrote to the data controller with advice and guidance; or
- A data controller could have submitted a PDB following some breach associated with a request submitted to them via our SAR tool and our PDB team provided them with advice.

The first two are most likely and the latter two are more remote, but this does not rule out the fact that I cannot definitively rule out that advice is not held in any of these contexts.

We do not hold any of this information in any way which would allow us to run an automated report to identify advice in scope of your request. With this in mind, to locate the information you have requested would require a manual search of all the records that we hold. The SAR tool was released approximately six months ago. Using the data in our latest annual report and other data sources available to me, I have established some approximate numbers for enquiries received via each channel for the past six months:

- 1,870 business services enquiries;
- 19,333 live chats (adjusted for a 100 day retention period);
- 16,876 data protection complaints; and
- 4,573 personal data breaches.
- Calls are not recorded and therefore it is unlikely there would be any record in that respect.

Ordinarily, we would carry out a dip check in order to demonstrate that these searches would exceed 18 hours. However, in this present case, I consider that it is so clear that the searches would exceed that time limit that I have not done so. Naturally, the discussion above has only focused on this point which would clear exceed the cost limit even before considering your eight other points. I have included some commentary on your other points in advice and assistance below.

In conclusion, I consider the provisions of section 12 of the FOIA apply and we are therefore refusing this request. I have provided some advice and assistance below that may

Advice and assistance

I do not consider there are any meaningful ways I can recommend to narrow the scope of point four of your request such that the scope of the searches was small enough to allow us to locate the information **and** the resultant information would be meaningful. Even if we were to limit the search to only enquiries made on a single day or via a single context, that would still require hundreds of checks with no guarantees of finding anything of interest.

Some alternatives may include requesting a copy of the template that we use to populate a SAR tool user's input before sending it to the data controller. This will give you an idea of what the email to data controllers will look like. You could also request whether we have produced, for example, a specific page on our website for data controllers who are in receipt of a SAR tool submission.

However, in the latter case, the advice we would provide to an organisation in receipt of ID may be exactly the same whether it is submitted through the SAR tool or received directly.

Although I have not spoken much about your other eight points, I will speak of them here. Your second point reads:

"*Please provide all the ICO's internal communications (including emails) regarding the addition of the proof of ID and address functionality on the ICO's SAR tool.*"

This is also a very broad request and may include correspondence held across the organisation. While I have not done a full assessment as to whether this point alone would exceed the cost limit, it may be wise to limit your request to internal communications with the project team responsible for the production of the SAR too. This is likely to yield the most relevant information without the need for broad searches.

In relation to point five of your request, you may be interested to know that we have published on our disclosure log a DPIA for the SAR tool. This was published on our disclosure log on 13 September 2023, so I appreciate things may have moved on since then. However, it does contain a few mentions of Twilio SendGrid which may be of interest.

In relation to point six of your request, we already proactively publish all of our equality impact assessments. I have reviewed the EQAs published on that page and cannot see one published, nor do I know if one has been completed, of a nature that you describe. However, I wanted to draw your attention to the fact that we do proactively publish EQAs that we complete.

While I am unable to guarantee how any future request will be handled, I believe the above recommendations regarding points two and four of your request may improve the prospects of success. This concludes our response to your request.

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 on our website.

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 sets out your rights. Our Retention and Disposal Policy details how long we keep information.

Yours sincerely

Information Access Team
Strategic Planning and Transformation
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
For information about what we do with personal data see our privacy notice