

From: [Andy Grocott](#)
To: [Chris Ashton](#); [Suzanne Gordon](#)
Cc: [Graham Rumens](#)
Subject: RE: SAR Change Request
Date: 21 September 2023 09:20:17
Attachments: [20230920_Request for change_SAR 0.1.docx](#)
[image001.jpg](#)

Apologies, I put the wrong date in for MMP going into Production.

Attached is the updated version.

Good spot Graham!

Cheers

Andy

From: Andy Grocott
Sent: Wednesday, September 20, 2023 3:19 PM
To: Chris Ashton <chris.ashton@ico.org.uk>; Suzanne Gordon <Suzanne.Gordon@ico.org.uk>
Cc: Graham Rumens <Graham.Rumens@ico.org.uk>
Subject: SAR Change Request

Chris/Suzanne,

I have attached a CR for the SAR project covering pushing the project closure out to mid-December and detailing the additional £28k of funding we need. [@Chris Ashton](#) I do not have a copy of your correspondence with Angela in August, so haven't referred to anything being ring-fenced or set aside, but happy for you to add something accordingly.

Regards

Andy



Andy Grocott

Digital, Data and Technology Business Partner
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

If you wish to submit an information request or want to exercise any of your data protection rights, please forward your email to the Information Access Team at accessicoinformation@ico.org.uk, or you can call us to make a verbal request relating to your personal data on our Helpline 0303 123 1113.

For information about what we do with personal data see our [privacy notice](#)

SAR Tool Project Request for Change

To:	Portfolio Board
From:	Andy Grocott, Scrum Master
Date of submission:	
Project name:	SAR Tool
SRO / Project Sponsor:	Suzanne Gordon
Programme Manager / Project Manager:	Scrum Master: Andy Grocott Project Manager: Graham Rummens
Change Requester:	Andy Grocott
Change Number: <i>(to be logged on Decision register)</i>	

Purpose of this document

The purpose of this form is to initiate a change request for the project. The change request will be tabled at the Project Steering Committee for approval, before progression to the Portfolio Board for assurance. The potential impact of this change requests has been assessed in relation to how its implementation might impact the outcomes, objectives and original business case for the project.

Change category

Check all that apply:

- Schedule Cost Scope Other
- Testing/Quality Resources Requirements/Deliverables

Type of change

Check all that apply:

Corrective Action Preventative Action Defect Repair Updates

✓ Other

Describe the change being requested

The ICO25 annual action plan outlines our commitment, in year one, to “develop a subject access request (SAR) tool to help people make requests in ways which will help organisations to respond effectively. The SAR Tool project mandate records that “there are no fixed deadlines however this is referred to in our Year 1 plan so some progress expected by Oct 2023”.

A minimum marketable product version of the tool (MMP) was put in to production on 02 August and to date has had in excess of 3,000 submissions. However, additional development work is required to improve the functionality of the tool and improve the user journey in line with feedback received, so this is a request to extend the project beyond October 2023, and access additional funding for further development work and tool enhancements.

The request asks for the project to be extended until 22/12/2023 and additional funding be allocated to allow for new functionality (all within the original scope of the project) to be developed.

Describe reason for change

The MMP version of the Tool has achieved a number of benefits and objectives set out for the project, for data subjects wanted to exercise their right of access. However, there are three key issues relating to the management and functionality of the service that need to be addressed and resolved before the service can be handed over to IT Help to manage and support in Production:

- Welsh Language version of the service – the ICO’s Compliance Notice for Welsh Language decrees that we must ensure “that when you publish a new page on your website or amend a page — (a) the text of that page is available in Welsh, (b) any Welsh language version of that page is fully functional, and (c) the Welsh language is treated no less favourably than the English language in relation to that page”.
- Email validation – Within the MMP version of the service, users are asked to enter the e-mail address of the organisation they wish to send the SAR to. Currently, as the email is sent from the ICO’s Outlook server, any auto responses or bounce backs for undeliverable emails are being returned to the ICO and not the user. This has resulted in the project team having to manage this work manually on a daily basis. Prior to the service being handed over to IT Help to manage and support in production, development work is required to integrate with an email validation cleansing service and additional development work to ensure auto responses and bounce backs are redirected to the service user.

- User Identity verification – Two of the key objectives of the project were for organisations to find it easier to respond appropriately to SARs, and for SAR's submitted through the tool to be clearer, more specific and more effective. User research carried out during the discovery phase of the project and initial feedback from Organisations who have received a SAR through the service is that there is an expectation that SAR's would arrive at the organisation with information and documentation that allows the organisation to verify and confirm the identity of the requester. Additional bespoke development work is required to add this functionality to the service.

Although the project mandate records no hard deadline for project closure, it does give a milestone for a deliverable by the end of October 2023. Whilst a working MMP version of the service has been delivered to Production, further enhancements are required in order to bring this service up to a level of an MVP that could be moved to BAU, where it would be managed by the Web Product Owner and supported by IT Help. It is estimated that two months additional development time is required to deliver these enhancements, extending the lifetime of the project to 22/12/2023.

Describe all alternatives considered

Remain As-Is – This is not a viable option as we have a legal duty to provide a Welsh language service for citizens living in or operating in the principality. Further, the service currently requires daily management by the project team to deal with email bounce backs. It is not conceivable for the service to be handed over to IT Help to support, as managing the current bounce backs would be too resource intensive and be tantamount to handing over a service with a P2 bug and no plan for resolution.

Describe any technical changes required to implement this change

Welsh language version requires development of a mirror service, translated in to Welsh Language. This work will be carried out by the project team in consultation with our Web development partner, Shout.

Email Validation – The SAR service will be integrated with the Data8 email cleansing look up service. This requires some minor development work carried out by the project team, supported by Shout.

User Identity Verification – the service will be iterated to add the functionality for a user to upload a document that is proof of identity and a second document that is proof of address. The project team have developed high fidelity wireframes for this functionality and shared them with Shout, who will carry out the development work.

All of these changes will be fully tested by both Shout's QA and the project team test engineer and must meet the project definition of done before they are approved for deployment in the Production environment.

Describe risks to consider for this change

The option to upload documentation to prove identity is optional, but if users elect to use this functionality the ICO will be processing volumes of personal data. The DPIA has been updated accordingly and this has also been documented accordingly on the project RAID log. Retention schedule remains the same with submissions and any uploaded attachment retained for 14 days in the event of service failure, so that the ICO can recover the submission and forward it on to the relevant organisation. The service clearly documents that it is the duty of the organisation receiving the SAR to verify the identity of the user, and not the duty of the ICO SAR service.

Estimate resources and costs needed to implement this change

Resource	No. of Days		When?	Source? (corporate, service, external)
	Total	Per Wk		
<i>Likely to be enablers below</i>			<i>Insert date</i>	<i>Insert source</i>
Shout Web Developer	25	2.5	Oct 2023 to Dec 2023	External
Scrum Master	25	2.5	Oct 2023 to Dec 2023	Corporate
Project Management	25	2.5	Oct 2023 to Dec 2023	Corporate
UR/UX Lead	25	2.5	Oct 2023 to Dec 2023	Corporate
Product Owner	25	2.5	Oct 2023 to Dec 2023	Corporate
QA/Test Engineer	25	3	Oct 2023 to Dec 2023	Corporate
Business Analyst	25	2.5	Oct 2023 to Dec 2023	Corporate.

- Shout developments costs for the 3 additional pieces of functionality are estimated at £20,250 (25 days Development x £675 & VAT); and
- Data8 Email Cleansing service - £8,000 per annum (package of up to 80,000 email look ups per annum.)

Total estimated costs - £28,250

Describe implications to the quality

Only quality implication would be in following an alternative course of action to remain As-Is (see "Describe all alternatives considered").

Describe impact on other deliverables

The project closure date will change from 31/10/2023 to 30/11/2023. The implications will be that the Scrum Team will need to remain stood up and prioritised to support this project.

Disposition

Approve Reject Defer

Justification of Approval, Rejection, or Deferral

Information and description (*instructions of important factors to consider when completing the template*)

Document Approvals

Role	Name	Signature	Date
Project Board Members:			
Portfolio Manager			

Approval:

Role	Name	Signature	Date
Project Sponsor	Suzanne Gordon		
ET Sponsor	Rob Holtom		

Version control:

Version	Date	Changes	By
0.1	20/09/2023	First draft	Andy Grocott

From: [Anthony Francis](#)
To: [Graham Rumens](#); [Hannah Smith](#); [Greer Schick](#); [Andy Grocott](#); [Asad Rahman](#)
Subject: RE: ID docs mock up
Date: 15 September 2023 08:59:45
Attachments: [image001.png](#)
[image002.jpg](#)

Hi Hannah

Some notes:

I think it's definitely valuable to the user putting the file names in the Preview page.

Shout will be able to easily tweak the File upload widget so that the prepended hexadecimal strings are removed.

The help text for the file upload widgets doesn't indicate to the user what valid file types will be acceptable. eg .png, .jpg, .pdf, etc.

Thanks
Tony

From: Graham Rumens <Graham.Rumens@ico.org.uk>
Sent: Friday, September 15, 2023 8:29 AM
To: Hannah Smith <Hannah.Smith@ico.org.uk>; Greer Schick <Greer.Schick@ico.org.uk>; Andy Grocott <andy.grocott@ico.org.uk>; Asad Rahman <Asad.Rahman@ico.org.uk>; Anthony Francis <Anthony.Francis@ico.org.uk>
Subject: RE: ID docs mock up

Hi Hannah

My observation is that the optional fields on the form are all called out in (brackets) – except the Proof of ID. This gives the impression its NOT optional (even though we say it is on the start screen). The uploading of docs is the most techy bit on the form and therefore most likely to discourage some users from completing unless we are clear alongside the field that it is not mandatory.

Thanks
Graham



From: Hannah Smith <Hannah.Smith@ico.org.uk>

Sent: Thursday, September 14, 2023 4:04 PM

To: Greer Schick <Greer.Schick@ico.org.uk>; Andy Grocott <andy.grocott@ico.org.uk>; Asad Rahman <Asad.Rahman@ico.org.uk>; Graham Rumens <Graham.Rumens@ico.org.uk>; Anthony Francis <Anthony.Francis@ico.org.uk>

Subject: ID docs mock up

Hi all,

I have made the changes to the staging site to gather ID docs. You can check it out here: [Make a subject access request | ICO](#). I thought we could discuss this in the workshop on Monday. Things I'd like to consider:

Start page:

- Is there now too much information on this page? We need to ensure we get people prepared to use the service, but I don't want to overwhelm them with info.

Form page:

- In the first instance, Greer and I decided just to include the upload options and have them as optional. The hope is we will get enough people using it that we can leave it like this. The next iteration would include making them mandatory and adding a tick box for those who cannot provide it. I'd like to discuss the measure of success for this – eg how many submissions without uploads is too many.
- Because they are not mandatory, I have put them at the bottom of the form – as the order org, request, info, uploads is more logical
- Do we think the titles and help text are clear for the uploads.

Preview

- I have included the uploads in the preview so that people can be assured that a file was uploaded – do you agree with that, even though it might be a file name of random numbers and letters.

Emails

1. I have made slight tweaks to the wording about ID to make it clear to both parties that further action may be needed – are we happy the guidance is clear enough?

Other:

Is there anything else we need to consider from a design, governance, or risk perspective?

Thanks
Hannah

| Hannah Smith (she/her)

Logo



Senior User Centred Design Manager

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](#)

From: [Andy Grocott](#)
To: [Chris Ashton](#); [Suzanne Gordon](#)
Cc: [Graham Rumens](#)
Subject: SAR Change Request
Date: 20 September 2023 15:19:37
Attachments: [image001.jpg](#)
[20230920_Request for change SAR 0.1.docx](#)

Chris/Suzanne,

I have attached a CR for the SAR project covering pushing the project closure out to mid-December and detailing the additional £28k of funding we need. [@Chris Ashton](#) I do not have a copy of your correspondence with Angela in August, so haven't referred to anything being ring-fenced or set aside, but happy for you to add something accordingly.

Regards

Andy



Andy Grocott

Digital, Data and Technology Business Partner
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

If you wish to submit an information request or want to exercise any of your data protection rights, please forward your email to the Information Access Team at accessicoinformation@ico.org.uk, or you can call us to make a verbal request relating to your personal data on our Helpline 0303 123 1113.

For information about what we do with personal data see our [privacy notice](#)

SAR Tool Project Request for Change

To:	Portfolio Board
From:	Andy Grocott, Scrum Master
Date of submission:	
Project name:	SAR Tool
SRO / Project Sponsor:	Suzanne Gordon
Programme Manager / Project Manager:	Scrum Master: Andy Grocott Project Manager: Graham Rummens
Change Requester:	Andy Grocott
Change Number: <i>(to be logged on Decision register)</i>	

Purpose of this document

The purpose of this form is to initiate a change request for the project. The change request will be tabled at the Project Steering Committee for approval, before progression to the Portfolio Board for assurance. The potential impact of this change requests has been assessed in relation to how its implementation might impact the outcomes, objectives and original business case for the project.

Change category

Check all that apply:

- Schedule Cost Scope Other
- Testing/Quality Resources Requirements/Deliverables

Type of change

Check all that apply:

Corrective Action Preventative Action Defect Repair Updates

✓ Other

Describe the change being requested

The ICO25 annual action plan outlines our commitment, in year one, to “develop a subject access request (SAR) tool to help people make requests in ways which will help organisations to respond effectively. The SAR Tool project mandate records that “there are no fixed deadlines however this is referred to in our Year 1 plan so some progress expected by Oct 2023”.

A minimum marketable product version of the tool (MMP) was put in to production on 02 November and to date has had in excess of 3,000 submissions. However, additional development work is required to improve the functionality of the tool and improve the user journey in line with feedback received, so this is a request to extend the project beyond October 2023, and access additional funding for further development work and tool enhancements.

The request asks for the project to be extended until 22/12/2023 and additional funding be allocated to allow for new functionality (all within the original scope of the project) to be developed.

Describe reason for change

The MMP version of the Tool has achieved a number of benefits and objectives set out for the project, for data subjects wanted to exercise their right of access. However, there are three key issues relating to the management and functionality of the service that need to be addressed and resolved before the service can be handed over to IT Help to manage and support in Production:

- Welsh Language version of the service – the ICO’s Compliance Notice for Welsh Language decrees that we must ensure “that when you publish a new page on your website or amend a page — (a) the text of that page is available in Welsh, (b) any Welsh language version of that page is fully functional, and (c) the Welsh language is treated no less favourably than the English language in relation to that page”.
- Email validation – Within the MMP version of the service, users are asked to enter the e-mail address of the organisation they wish to send the SAR to. Currently, as the email is sent from the ICO’s [REDACTED] server, any auto responses or bounce backs for undeliverable emails are being returned to the ICO and not the user. This has resulted in the project team having to manage this work manually on a daily basis. Prior to the service being handed over to IT Help to manage and support in production, development work is required to integrate with an email validation cleansing service and additional development work to ensure auto responses and bounce backs are redirected to the service user.

- User Identity verification – Two of the key objectives of the project were for organisations to find it easier to respond appropriately to SARs, and for SAR’s submitted through the tool to be clearer, more specific and more effective. User research carried out during the discovery phase of the project and initial feedback from Organisations who have received a SAR through the service is that there is an expectation that SAR’s would arrive at the organisation with information and documentation that allows the organisation to verify and confirm the identity of the requester. Additional bespoke development work is required to add this functionality to the service.

Although the project mandate records no hard deadline for project closure, it does give a milestone for a deliverable by the end of October 2023. Whilst a working MMP version of the service has been delivered to Production, further enhancements are required in order to bring this service up to a level of an MVP that could be moved to BAU, where it would be managed by the Web Product Owner and supported by IT Help. It is estimated that two months additional development time is required to deliver these enhancements, extending the lifetime of the project to 22/12/2023.

Describe all alternatives considered

Remain As-Is – This is not a viable option as we have a legal duty to provide a Welsh language service for citizens living in or operating in the principality. Further, the service currently requires daily management by the project team to deal with email bounce backs. It is not conceivable for the service to be handed over to IT Help to support, as managing the current bounce backs would be too resource intensive and be tantamount to handing over a service with a P2 bug and no plan for resolution.

Describe any technical changes required to implement this change

Welsh language version requires development of a mirror service, translated in to Welsh Language. This work will be carried out by the project team in consultation with our Web development partner, Shout.

Email Validation – The SAR service will be integrated with the [REDACTED] email cleansing look up service. This requires some minor development work carried out by the project team, supported by [REDACTED].

User Identity Verification – the service will be iterated to add the functionality for a user to upload a document that is proof of identity and a second document that is proof of address. The project team have developed high fidelity wireframes for this functionality and shared them with [REDACTED], who will carry out the development work.

All of these changes will be fully tested by both [REDACTED]’s QA and the project team test engineer and must meet the project definition of done before they are approved for deployment in the Production environment.

Describe risks to consider for this change

The option to upload documentation to prove identity is optional, but if users elect to use this functionality the ICO will be processing volumes of personal data. The DPIA has been updated accordingly and this has also been documented accordingly on the project RAID log. Retention schedule remains the same with submissions and any uploaded attachment retained for 14 days in the event of service failure, so that the ICO can recover the submission and forward it on to the relevant organisation. The service clearly documents that it is the duty of the organisation receiving the SAR to verify the identity of the user, and not the duty of the ICO SAR service.

Estimate resources and costs needed to implement this change

Resource	No. of Days		When?	Source? (corporate, service, external)
	Total	Per Wk		
<i>Likely to be enablers below</i>			<i>Insert date</i>	<i>Insert source</i>
Shout Web Developer	25	2.5	Oct 2023 to Dec 2023	External
Scrum Master	25	2.5	Oct 2023 to Dec 2023	Corporate
Project Management	25	2.5	Oct 2023 to Dec 2023	Corporate
UR/UX Lead	25	2.5	Oct 2023 to Dec 2023	Corporate
Product Owner	25	2.5	Oct 2023 to Dec 2023	Corporate
QA/Test Engineer	25	3	Oct 2023 to Dec 2023	Corporate
Business Analyst	25	2.5	Oct 2023 to Dec 2023	Corporate.

- Shout developments costs for the 3 additional pieces of functionality are estimated at £20,250 (25 days Development x £675 & VAT); and
- Data8 Email Cleansing service - £8,000 per annum (package of up to 80,000 email look ups per annum.)

Total estimated costs - £28,250

Describe implications to the quality

Only quality implication would be in following an alternative course of action to remain As-Is (see "Describe all alternatives considered").

Describe impact on other deliverables

The project closure date will change from 31/10/2023 to 30/11/2023. The implications will be that the Scrum Team will need to remain stood up and priroitised to support this project.

Disposition

Approve Reject Defer

Justification of Approval, Rejection, or Deferral

Information and description (*instructions of important factors to consider when completing the template*)

Document Approvals

Role	Name	Signature	Date
Project Board Members:			
Portfolio Manager			

Approval:

Role	Name	Signature	Date
Project Sponsor	Suzanne Gordon		
ET Sponsor	Rob Holtom		

Version control:

Version	Date	Changes	By
0.1	20/09/2023	First draft	Andy Grocott

From: [Hannah Smith](#)
To: [Jonathon Woodruff](#); [Daniel Barlow](#); [Greer Schick](#)
Cc: [Knowledge Services](#)
Subject: RE: KSA0147 - Request for internal advice
Date: 20 September 2023 11:26:00
Attachments: [image001.jpg](#)
[image002.png](#)
[image003.png](#)

Answered the questions below. [@Greer Schick](#) I've just asked you to clarify something on the last question.

Let me know if you need any more info.

H

From: Jonathon Woodruff <Jonathon.Woodruff@ico.org.uk>
Sent: Wednesday, September 20, 2023 9:51 AM
To: Hannah Smith <Hannah.Smith@ico.org.uk>; Daniel Barlow <Daniel.Barlow@ico.org.uk>
Cc: Knowledge Services [REDACTED]
Subject: RE: KSA0147 - Request for internal advice

Good morning Hannah

Many thanks for your request for internal advice.

Based on some initial discussions, we think this will benefit from a legal steer.

But before we refer this to Legal, it'd be helpful if you could please provide us with some additional information:

- Were there any discussions around the decision to include the ICO logo in these generated emails? Was there a specific intention behind that (eg to help add 'weight' to SAR requests)?

It was to give it more authenticity so that organisations could feel the emails were trustworthy – eg not spam or phishing.

- Just to confirm, will all the generated SAR emails appear to be sent/generated from an ICO email address? From the demonstration video, it looks like they'll come from 'noreply@ico.org.uk'.

They come from noreply@ico.org.uk. When the org presses reply though – the reply is sent to the requester not noreply@.

- What has prompted you to raise this request with us? Eg have there already been concerns/push back around our role internally or externally?

We are about to make a change to the service, which will ask users to upload proof of ID and address to support orgs validating ID. But we do not claim that this is us validating ID. We just wanted to be 100% on this point ahead of the change. There has been no concerns/push back with the service in it's current state as far as I am aware.

- Do we keep a copy of the SAR or any other information people enter into the tool? Do we pull any data from the tool (eg how many SARs are being made to certain organisations)? What personal data of the requesters ends up on our servers and do we retain any of it?

We keep all the data from the request for 14 days, just in case there is any technical issues on our end that stop the requests being sent so we can rectify the problem. We have pulled the email addresses of orgs to ask them for feedback on their experience (which was agreed with info management). [@Greer Schick](#) is Tony using any of the data for testing or reviewing?

Once the service is up and running as BAU – we will not use the data for any purpose and just store as laid out above

It might be good to discuss this further on a call. If you agree, please let me know what day is best for you.

Hi [Daniel Barlow](#) – please let me know if there's anything else from your perspective that needs covering off.

Many thanks

Jon



Jonathon Woodruff
Senior Policy Officer – Knowledge and Internal
Communications Services
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](#)

From: Hannah Smith <Hannah.Smith@ico.org.uk>

Sent: Monday, September 11, 2023 12:39 PM

To: Knowledge Services <KnowledgeServices@ico.org.uk>

Subject: KSA0147 - Request for internal advice

Name, team, and department of requester

Hannah Smith on behalf of the SAR project team.

What's your specific deadline or SLA associated with your query?

NA

What's your question? Please be as clear as possible.

Is the ICO acting on behalf of individuals when they make a request via the [Make a subject access request](#) service?

Please briefly provide:

Our [detailed SAR guidance](#) states that it is the responsibility of any third party portal to provide an organisation with evidence it can act on behalf of an individual making a subject access request. The SAR project team believe that we do not have to produce this evidence if we were asked, as we are not acting on behalf of the individual. We have provided as service that makes it easier for an individual to make a request on their own behalf but, as we play no part in the wording of the request or in the interactions between the requester and org after it has been submitted – we are not making the request on their behalf. Would you agree with this?

From: [Hannah Smith](#)
To: [Andy Grocott](#); [Greer Schick](#)
Subject: RE: SAR comms to organisations
Date: 30 October 2023 15:40:00
Attachments: [ICO SAR Tool Organisation comms.docx](#)
[image001.jpg](#)

Some suggested changes from me.

I've tried to make it a bit shorter and keep it focused on the information that is relevant to orgs only.

H

From: Andy Grocott <andy.grocott@ico.org.uk>
Sent: Wednesday, October 25, 2023 2:06 PM
To: Greer Schick <Greer.Schick@ico.org.uk>; Hannah Smith <Hannah.Smith@ico.org.uk>
Subject: SAR comms to organisations

Hi Hanah/Greer,

I have followed up on the SAR comms with Claire, and she is now out of the office until mid-November.

Rather than waiting further, I think we can agree the comms and "polish" it up between the three of us.

I have attached what I shared with Claire. It is not top and tailed, but this is the messaging I felt we wanted to get out.

I would appreciate your comments and "polish".

Many thanks

Andy



Andy Grocott

Senior Digital Delivery Manager
Digital, Data and Technology

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

If you wish to submit an information request or want to exercise any of your data protection rights, please forward your email to the Information Access Team at accessicoinformation@ico.org.uk, or you can call us to make a verbal request relating to your personal data on our Helpline 0303 123 1113.

For information about what we do with personal data see our [privacy notice](#)

The ICO has launched a Beta version of our 'Make a subject access request service' which aims to support organisations and data subjects through the subject access request (SAR) process.

People requesting information from organisations can now make and send a SAR from the service hosted on the ICO's website, directly to the organisation. The service went live early August, so some organisations may have already had SAR requests through it.

When a person makes a request through the service, the organisation will get an ICO branded email containing the details of the request and guidance on how to respond. The requester will also get an email with a copy of their request and information about what should happen next.

What are the benefits of the new service for organisations?

- **More specific requests**

The service will help requesters be as specific as possible about the information they want. This should help organisations find the information quickly and stop requesters receiving massive amounts of information they may not need.

- **Managing requesters' expectations**

The email requesters receive after submitting their SAR gives them guidance about what should happen next and when organisations are allowed to withhold or redact information.

The aim is to encourage requesters to engage with organisations when they're asked to validate their identity or provide clarity. It hopefully gives them a better understanding about when the "clock stops" on responses and what information they are (and are not) able to access.

This should hopefully reduce the number of misguided complaints being made to both organisations and the ICO.

- **Provides guidance to organisations at the time they need it**

The email sent to organisations will include advice and links to guidance about how to action the SAR.

For those organisations who are unaware or unsure about their obligations, this should hopefully help them to take action quickly and effectively.

- **A free and user friendly online SAR service**

Many organisations don't have the money or resources to create an online SAR service. They are reliant on emails from requesters, which can be hard to action.

Organisations can link to our, which we hope will improve the experience for them and the requesters.

The SAR service was a deliverable in the ICO25 strategic plan [\[link\]](#). It has been designed and built based on user research and with user needs in mind.

We continue to make improvements based on user feedback. Future changes will include:

- validating email addresses against a real-time checking service to make sure requests are sent to valid email addresses and to reduce the risk of spam emails;
- proof of ID and address uploads to support organisations to quickly validate requesters identity; and
- functionality that allows people to use the service to make requests for other people, with the facility to upload a letter of authority or consent.

From: [Andy Grocott](#)
To: [Greer Schick](#); [Graham Rumens](#)
Cc: [Anthony Francis](#); [Hannah Smith](#)
Subject: RE: Risk re document malware
Date: 16 November 2023 15:37:00
Attachments: [image001.jpg](#)

Thanks for the update, Greer.

I think we are mitigating the risk, and in most cases will be applying more rigorous cyber defence than many customers would have in place if they received something directly from the SAR requester.

Further, those organisations that have more rigorous controls than us, will by that very fact, apply their own virus scanning checks, even on email from ourselves and other public sector bodies. I can see the sense in including messaging that cautions organisations that we have virus scanned documents but do not attest to their safety, but I do wonder if some organisations would use that as an excuse to not deal with the email – even though we are not expecting them to do anything different to what they would do if they received it direct from the data subject.

I think you are right in suggesting we log the risk and it is then up to Suzanne and/or Rob to accept the risk.

Regards

Andy

From: Greer Schick <Greer.Schick@ico.org.uk>
Sent: Thursday, November 16, 2023 2:33 PM
To: Graham Rumens <Graham.Rumens@ico.org.uk>
Cc: Anthony Francis <Anthony.Francis@ico.org.uk>; Hannah Smith <Hannah.Smith@ico.org.uk>; Andy Grocott <andy.grocott@ico.org.uk>
Subject: Risk re document malware

Hi Graham and cc all,

I spoke with Alan McGann yesterday. He'd raised some queries at TDA about the on-upload malware scanning solution we've proposed for the SAR tool to support uploading of ID docs and third parties acting on behalf of a requester. In principle he supports it from a cyber and technology perspective. The risk he was raising he said was part cyber, but more reputational.

Here's my wording of the risk he was raising.

Can we please add it to the risk register? Alan was suggesting that it might need to go to some forum (IRGG?) for review but I'd suggest we first document it in the usual way, score it, and then depending on that

have a conversation with Suzanne about whether it's appropriate for her to sign it off.

Risk:

Due to a requester uploading a document containing malware as part of their request, this may lead to an organisation receiving malware and if this became public it could damage the ICO's reputation, and/or a claim for damages.

Mitigation:

[REDACTED] will be implemented. [REDACTED] provides mitigation against malicious content by performing a full malware scan on uploaded content in near real time, using [REDACTED] capabilities. Uploaded files will not be forwarded to the recipient organisation unless they pass the malware scan.

Considerations:

In order for this risk to materialise, an attacker would need to be in possession of a piece of malware that was not detected by MS Defender, eg a zero-day exploit; choose to use the ICO Make a subject access request service to launch an attack; the malware would need to cause damage to the recipient's systems and; the receiving organisation would make the situation public or otherwise make a claim against ICO. Our main defence would be likely to explain that we assessed the risk, mitigated the risk in an appropriate way using available technologies, advised recipient organisations to conduct their own checks, and considered that the benefits outweighed the residual risk.

Risk assessment: Likelihood – low; Impact – medium.

For project team to consider – add advice re virus checking to organisation email?

Existing text in black; possible addition in purple.

We've asked the requester to provide proof of ID and address where possible. The ICO has not checked the identity of the requester. You must be satisfied that you know the identity of the requester, and that the data you hold relates to them.

We've also asked for evidence of third party authority, where relevant. The ICO has not checked the third party requester has consent to act on the person's behalf. You must be sure any third party has permission to make this request.

We have checked any attached files for viruses, but we don't guarantee that they are safe. You should perform your own checks.

Logo



Greer Schick
Senior Product Owner - Web

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

T. 0330 414 6783 F. 01625 524510 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](#)

From: Greer Schick
To: Steven Johnston
Subject: FW: DPIA for SAR service for review and signoff -- upload of ID documents
Date: 07 December 2023 16:20:00
Attachments: image001.jpg
image002.png

Hi Steve,

Just confirming that Suzanne has signed off the updated SAR DPIA. I've accepted all the changes now.

Thanks again for your help with this.

[REDACTED]

(same master doc as before)

Cheers, Greer.



Greer Schick
Senior Product Owner - Web

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
[REDACTED] ico.org.uk twitter.com/iconews

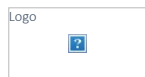
Please consider the environment before printing this email
For information about what we do with personal data see our [privacy notice](#)

From: Suzanne Gordon <Suzanne.Gordon@ico.org.uk>
Sent: Thursday, December 7, 2023 3:17 PM
To: Greer Schick <Greer.Schick@ico.org.uk>
Cc: Graham Rumens <Graham.Rumens@ico.org.uk>; Andy Grocott <andy.grocott@ico.org.uk>
Subject: RE: DPIA for SAR service for review and signoff -- upload of ID documents

Thanks Greer, Andy, Graham and I discussed the malware scanning solution at our last SAR catch up, so I am comfortable with the changes made to the DPIA.

Thanks

Suzanne



Suzanne Gordon (she/her)

Director of Public Advice & Data Protection Complaints Services

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Suzanne.Gordon@ico.org.uk
twitter.com/iconews

For information about what we do with personal data see our [privacy notice](#)
Please consider the environment before printing this email

From: Greer Schick <Greer.Schick@ico.org.uk>
Sent: Thursday, December 7, 2023 9:06 AM
To: Suzanne Gordon <Suzanne.Gordon@ico.org.uk>
Cc: Graham Rumens <Graham.Rumens@ico.org.uk>; Andy Grocott <andy.grocott@ico.org.uk>
Subject: DPIA for SAR service for review and signoff -- upload of ID documents

Hi Suzanne,

Hope you're well.

I think this will be the last (or second-to-last) update to the DPIA before we close the project down and move to the Live phase

Please can you review the updated DPIA below. I've made some changes to reflect the **malware scanning solution** we're building to mitigate the risk that a person's SAR request sends a virus to an organisation, which will allow us to add fields for customers to upload their ID documents. You'll see the changes in tracked changes.

As before if you would please review and, if you're happy, sign and date on page 42.

If you're able to sign by end of play Monday that'd be great as the request to deploy the functionality is going to CAB on Tuesday morning.

[REDACTED]

Kind regards, Greer.



Greer Schick
Senior Product Owner - Web

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

[REDACTED] 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](#)

From: Steven Johnston <Steven.Johnston@ico.org.uk>
Sent: Wednesday, December 6, 2023 10:38 AM
To: Greer Schick <Greer.Schick@ico.org.uk>

Cc: Information Management <[REDACTED]>
Subject: RE: Website SAR service -- upload of ID documents

Hi Greer,

That all sounds good, thanks for the explanation and I think you're good to approach Suzanne for sign off.

Thanks



Steven Johnston
Team Manager, Information Management & Compliance
Digital, Data and Technology Directorate
Information Commissioner's Office, Wycliff House, Water Lane, Wilmslow, Cheshire SK9 5AF
[REDACTED] 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](#)

From: Greer Schick <Greer.Schick@ico.org.uk>
Sent: Wednesday, December 6, 2023 10:34 AM
To: Steven Johnston <Steven.Johnston@ico.org.uk>
Cc: Information Management <[REDACTED]>
Subject: RE: Website SAR service -- upload of ID documents

Thanks Steve,

I've updated the document with the following.

The request is still sent to the organisation and the copy to the customer, but any files that have not been scanned and passed are removed and in their place is a message 'This file was removed for security reasons'.

Before submitting the request to the organisation (and the copy to the customer), only files that have been scanned and passed will be attached; otherwise they will be removed. When a file is removed, the recipient emails will contain a message 'This file was removed for security reasons' alongside the name of the file and the form question it related to.

Where docs have been removed, the expectation is that the organisation will follow their existing processes for ensuring that they have all the info they need before sending the personal data. This may mean that they need to contact the requester to supply any docs that were removed, but it's up to them and their processes. (Some orgs may have processes where there's enough information already provided that they may not need the removed docs.)

Let me know if you think the above is OK and any other feedback and/or if I can go ahead and ask Suzanne to review and sign off.

Cheers, Greer.



Greer Schick
Senior Product Owner - Web
Information Commissioner's Office, Wycliff House, Water Lane, Wilmslow, Cheshire SK9 5AF
[REDACTED] 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](#)

From: Steven Johnston <Steven.Johnston@ico.org.uk>
Sent: Tuesday, December 5, 2023 9:33 AM
To: Greer Schick <Greer.Schick@ico.org.uk>
Cc: Information Management <[REDACTED]>
Subject: RE: Website SAR service -- upload of ID documents

Morning Greer,

Sorry it's taken me a while to reply, we've a bit of a backlog at present. I've had a read of the changes, and they seem minor. Only query from me is what happens if the scanned documents don't pass the defender scan? Does the request still get sent to recipient just minus the attachments? Or does the entire request fail? Is the requester notified that the request has failed or been sent but without the attachments?

I think it would be good to add a few additional sentences just so this is clear. I'm just mindful of doing what we can to facilitate the request and / or notify the customer of any failure to send request or attachments so they can send in a different way to recipient.

Thanks



Steven Johnston
Team Manager, Information Management & Compliance
Digital, Data and Technology Directorate
Information Commissioner's Office, Wycliff House, Water Lane, Wilmslow, Cheshire SK9 5AF
[REDACTED] 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](#)

From: Greer Schick <Greer.Schick@ico.org.uk>
Sent: Monday, November 27, 2023 3:49 PM
To: Steven Johnston <Steven.Johnston@ico.org.uk>
Subject: RE: Website SAR service -- upload of ID documents

Hi Steven,

As promised, I've made a few updates to the Subject Access Service DPIA to reflect that we're planning to allow users to upload ID documents. Please would you review it?

To support this, we're using existing file upload functionality but we're extending it to incorporate malware scanning as the file is uploaded, to mitigate the risk that our service is used to send malware to the recipient organisation.

The updates themselves are pretty small/minor.

As before, I've left tracked changes on for the time being. It would be good to get any feedback from you; I'll then plan to pass it on to Suzanne as IAO.



Greer Schick
Senior Product Owner - Web
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](#)

From: Greer Schick
Sent: Wednesday, November 22, 2023 4:30 PM
To: Steven Johnston <Steven.Johnston@ico.org.uk>
Subject: Website SAR service -- upload of ID documents

No sooner have we got that signed off ...

We're about to start developing a new feature which aims to reduce the time it takes and make it easier for orgs to respond to SARs by allow customers to upload their ID docs as they submit their request. To do this we'll be introducing a file upload feature that incorporates malware scanning.

I'm going to make a start on updating the DPIA again to cover this, so I'll plan to get in touch in the next few days for another review.

Cheers, Greer.



Greer Schick
Senior Product Owner - Web
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](#)

From: Steven Johnston <Steven.Johnston@ico.org.uk>
Sent: Wednesday, November 22, 2023 9:30 AM
To: Greer Schick <Greer.Schick@ico.org.uk>
Subject: RE: Website SAR service -- signoff for updated DPIA (automated alert and advice email for non-deliverable SAR requests)

Thanks Greer, I really appreciate both you and Susan updating the master version! It makes my life so much easier!



Steven Johnston
Team Manager, Information Management & Compliance
Digital, Data and Technology Directorate
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](#)

From: Greer Schick <Greer.Schick@ico.org.uk>
Sent: Tuesday, November 21, 2023 5:21 PM
To: Steven Johnston <Steven.Johnston@ico.org.uk>
Subject: FW: Website SAR service -- signoff for updated DPIA (automated alert and advice email for non-deliverable SAR requests)

Hi Steven,

Thanks again for your help with this – Suzanne has again signed off the updated version so letting you know that I've accepted the tracked changes. (Same link as before.)





Greer Schick
Senior Product Owner - Web

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6783 F. 01625 524510 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](#)

From: Greer Schick
Sent: Tuesday, November 21, 2023 5:12 PM
To: Suzanne Gordon <Suzanne.Gordon@ico.org.uk>
Cc: Andy Grocott <andy.grocott@ico.org.uk>; Graham Rumens <Graham.Rumens@ico.org.uk>
Subject: RE: Website SAR service -- signoff for updated DPIA (automated alert and advice email for non-deliverable SAR requests)

Nice one, thanks Suzanne.



Greer Schick
Senior Product Owner - Web

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
[REDACTED] 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](#)

From: Suzanne Gordon <Suzanne.Gordon@ico.org.uk>
Sent: Tuesday, November 21, 2023 5:11 PM
To: Greer Schick <Greer.Schick@ico.org.uk>
Cc: Andy Grocott <andy.grocott@ico.org.uk>; Graham Rumens <Graham.Rumens@ico.org.uk>
Subject: RE: Website SAR service -- signoff for updated DPIA (automated alert and advice email for non-deliverable SAR requests)

Hi Greer, I'm comfortable signing the amendments off. I just wanted to familiarise myself with the cross over between the DPIA and the risk register. I have done that now.

Thanks,

Suzanne



Suzanne Gordon (she/her)
Director of Public Advice & Data Protection Complaints Services

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Suzanne.Gordon@ico.org.uk
twitter.com/iconews
For information about what we do with personal data see our [privacy notice](#)
Please consider the environment before printing this email

From: Greer Schick <Greer.Schick@ico.org.uk>
Sent: Tuesday, November 14, 2023 9:10 AM
To: Suzanne Gordon <Suzanne.Gordon@ico.org.uk>
Cc: Andy Grocott <andy.grocott@ico.org.uk>; Graham Rumens <Graham.Rumens@ico.org.uk>
Subject: Website SAR service -- signoff for updated DPIA (automated alert and advice email for non-deliverable SAR requests)

Hi Suzanne,

Hope you're well.

Coming to you for signoff again!

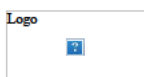
We've updated our DPIA for SAR again, this time to reflect the **automated alert and advice emails** that we're introducing, that will automate the process of alerting and advising customers in cases where they've typed the organisation's address incorrectly and it hasn't been picked up by any of our validation methods. This will remove the daily checks that are currently needed by us, and daily sending of emails to customers by PADPCS.

For info, Info Management were comfortable that the addition was minor from a data privacy point of view so it didn't need to go to the DPIA committee, just to you for signoff.

If you could please review and add your name and date as before, to pages 41 and 42.

Any questions, or if it'd be useful for me to talk you through how it works, let me know.

Cheers, Greer.



Greer Schick
Senior Product Owner - Web

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6783 F. 01625 524510 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](#)

From: Steven Johnston <Steven.Johnston@ico.org.uk>
Sent: Thursday, November 9, 2023 11:41 AM

To: Greer Schick <Greer.Schick@ico.org.uk>

Subject: RE: Website SAR service -- updates to DPIA (automated alert and advice email for non-deliverable SAR requests)

Hi Greer,

I've read through and the changes you've made look good to me. Only comment I'd make is you could probably do without this addition to your data inventory:

All of the above, for those individuals whose request email was non-deliverable	Members of the public requesting access to the data an organisation holds on them but whose request email was non-deliverable	Customer, Microsoft, Sendgrid.	Yes If yes, list the countries the data will be transferred to: Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.	Data may be retained by Twilio for quality control purposes, for no more than 61 days.
---	---	--------------------------------	---	--

If I'm understanding this right, I think the only thing you're trying to reflect here is that there's a new category of data subjects i.e. people whose request email was non-deliverable? However, as the categories of data are all the same as what's already in your inventory, and we have the processors identified as recipients of each data category already, this addition isn't really required. A new row in the inventory is only really needed if it's a new category of personal data being processed and I don't think these are changing as a result of the automated alert.

All other updates look good, and I can't see any need for this to go back via Forum since it's just leveraging existing tech that has previously been assessed. You should get the change signed off again by Suzanne and update the DPIA to reflect her approval.

Thanks



Steven Johnston

Team Manager, Information Management & Compliance

Digital, Data and Technology Directorate

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](#)

From: Greer Schick <Greer.Schick@ico.org.uk>

Sent: Friday, November 3, 2023 5:00 PM

To: Steven Johnston <Steven.Johnston@ico.org.uk>

Subject: Website SAR service -- updates to DPIA (automated alert and advice email for non-deliverable SAR requests)

Hi Steven,

Further to my email below, I've drafted a further update to the DPIA for the SAR service.

If you could please review it and let me have your comments, and also whether it needs to go to the forum or if again, it just needs to go back to Suzanne as IAO for signoff.

This time it's to reflect an automated alert and advice email we've been developing. This is to remove the need for ICO staff to manually contact customers when we find that the request hasn't been able to be delivered to an organisation (ie the SAR request email has bounced). It will receive the bounce notification, and automatically send an email to the customer to alert them to the bounce and give advice on what to do.

Happy to discuss as needed.

Cheers, Greer.



Greer Schick

Senior Product Owner - Web

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](#)

From: Greer Schick

Sent: Thursday, November 2, 2023 9:55 AM

To: Steven Johnston <Steven.Johnston@ico.org.uk>

Subject: FW: Website SAR service -- updates to DPIA

Hi Steven,

Just to confirm that Suzanne signed the updated DPIA for the SAR service.

I've accepted the tracked changes and saved the updated version at the master location.

For info, I'm expecting to update it further to reflect some new functionality which will send an automated email with advice to the customer if the generated request email was undeliverable to the organisation.

I'll be in touch when I've got a draft update together.

Cheers, Greer.



Greer Schick
Senior Product Owner - Web

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
ico.org.uk twitter.com/iconews

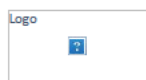
Please consider the environment before printing this email
For information about what we do with personal data see our [privacy notice](#)

From: Suzanne Gordon <Suzanne.Gordon@ico.org.uk>
Sent: Thursday, October 19, 2023 1:32 PM
To: Greer Schick <Greer.Schick@ico.org.uk>
Cc: Andy Grocott <andy.grocott@ico.org.uk>; Graham Rumens <Graham.Rumens@ico.org.uk>
Subject: RE: Website SAR service -- updates to DPIA

Hi Greer, thanks so much for sending this through and all of the work to date on this. I have approved this and signed the doc.

Kind regards

Suzanne



Suzanne Gordon (she/her)
Director of Public Advice & Data Protection Complaints Services

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Suzanne.Gordon@ico.org.uk
twitter.com/iconews

For information about what we do with personal data see our [privacy notice](#)
Please consider the environment before printing this email

From: Greer Schick <Greer.Schick@ico.org.uk>
Sent: Wednesday, October 18, 2023 8:57 AM
To: Suzanne Gordon <Suzanne.Gordon@ico.org.uk>
Cc: Andy Grocott <andy.grocott@ico.org.uk>; Graham Rumens <Graham.Rumens@ico.org.uk>
Subject: RE: Website SAR service -- updates to DPIA

Hi Suzanne,

Just realised the link probably wasn't clear (it was the link from the previous email in the chain) so here it is:



Greer Schick
Senior Product Owner - Web

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](#)

From: Greer Schick
Sent: Tuesday, October 17, 2023 6:44 PM
To: Suzanne Gordon <Suzanne.Gordon@ico.org.uk>
Cc: Andy Grocott <andy.grocott@ico.org.uk>; Graham Rumens <Graham.Rumens@ico.org.uk>
Subject: Website SAR service -- updates to DPIA

Hi Suzanne,

As promised, here's the update to the SAR service DPIA.

Tracked changes are on to make it easy to see the latest additions. If you could please review, and then add your name and date to pages 41 (signoff) and 42 (update log) that'd be great. Happy for you to either accept the changes or I can do that once you've finished.

Any questions, please just give me a call and I'm happy to chat through.

As you can see from the trail below, Steven Johnston (info management) was comfortable enough that this was a minor change / low enough risk that didn't need to go back to the committee for review.

Cheers, Greer.



Greer Schick
Senior Product Owner - Web

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](#)

From: Steven Johnston <Steven.Johnston@ico.org.uk>

Sent: Tuesday, October 17, 2023 4:43 PM

To: Greer Schick <Greer.Schick@ico.org.uk>

Cc: Graham Rumens <Graham.Rumens@ico.org.uk>; Information Management: [REDACTED]

Subject: RE: Website SAR service -- proposed updates to DPIA

Sorry forgot to include a link:

[REDACTED]



Steven Johnston

Team Manager, Information Management & Compliance

Digital, Data and Technology Directorate

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](#)



From: Steven Johnston

Sent: Tuesday, October 17, 2023 4:42 PM

To: Greer Schick <Greer.Schick@ico.org.uk>

Cc: Graham Rumens <Graham.Rumens@ico.org.uk>; Information Management: [REDACTED]

Subject: RE: Website SAR service -- proposed updates to DPIA

Hi Greer,

Thanks for the call earlier. As discussed, I've incorporated your changes into the master DPIA and I've made a few minor additions based on our conversation. I've just marked up with comments so you can see. Hopefully, all make sense but just edit if I've got anything wrong.

I didn't substantially change the risk in part 4 as having read it back I can understand it following our call. I did change the impact score from 2 to 3 as I feel the impact of the SAR not being submitted or going to an incorrect address could be a bit more significant for the individual. But it doesn't change the overall residual risk which still comes out as low.

If you can just review changes, then get Suzanne as IAO to sign off on it, and then finally accept all track changes so we have a clean version it looks ok.

Thanks



Steven Johnston

Team Manager, Information Management & Compliance

Digital, Data and Technology Directorate

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](#)



From: Greer Schick <Greer.Schick@ico.org.uk>

Sent: Wednesday, October 11, 2023 5:48 PM

To: Steven Johnston <Steven.Johnston@ico.org.uk>

Cc: Graham Rumens <Graham.Rumens@ico.org.uk>

Subject: Website SAR service -- proposed updates to DPIA

Hi Steven,

Hope you're well.

Hoping you can give the attached a once-over and come back with any comments, and a view on whether this needs to go to the DPIA committee or what the next steps would be (assuming approval by our IAO and Sponsor is required at some point).

We've been working on an iteration to the website Subject access request service to introduce instant validation of the organisation email address that gets inputted by the requester. This is to help improve the quality of the email address, reducing the likelihood that the requester types an address that's incorrect and the organisation doesn't receive the request (until we pick up the bounce and contact the customer). We're using a service provided by Data-8, an existing contracted supplier of web-enabled data validation services to the ICO. The service checks that the email domain is live, and the servers will accept the full email address entered, stopping users from submitting if the address is invalid.

Hopefully I've populated all the relevant bits in the attached SAR DPIA.

I've used tracked changes. (I've also used the opportunity to tidy up a few bits.)

One thing I haven't explained, is that I don't think the Privacy notice needs updating. The main reason is that the Data-8 service is

only checking the organisation email address, and because they're the recipient, I don't think it's useful or relevant to notify them via the privacy notice that their email address might be processed by Data-8.

Grateful for any and all thoughts you may have!

Also once you're happy please could you save this in your repo so it's held centrally? I didn't seem able to save back to that folder.

Cheers, Greer.



Greer Schick
Digital Architect

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](#)

Data Protection Impact Assessment (DPIA) – SAR Project

Document Name	Data Protection Impact Assessment – SAR Project
Author/Owner (name and job title)	Andy Grocott – Project Scrum Master Graham Rumens – Project Manager
Department/Team	Digital, Data and Technology
Document Status	Published
Version Number	V3.3
Release Date	19/07/2023
Approver (if applicable)	Suzanne Gordon, Director of Public Advice and DP Complaints
Review Date	19/07/2024
Distribution	Internal

Guidance for completing this DPIA template

- If you're unsure whether you need to complete a DPIA, use the [Screening assessment - do I need to do a DPIA?](#) first to help you decide.
- **Must** and **should** are used throughout the guidance notes in this template to help you understand which things are a legislative requirement and **must** be done versus things that the ICO considers **should** be done as best practice to comply effectively with the law.
- You **must** complete this DPIA template if your screening assessment indicates a DPIA is required.
- You **should** aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you won't be able to continue with your plans without changing them, or at all.
- We recommend that you fill out each section of this template in order, as each subsequent section builds upon the last. You will not be able to complete later sections correctly if you skip ahead. You **should** read the guidance notes throughout this template to help you with each section.
- If you are struggling with completing this template the [Information Management and Compliance Service](#) is available to provide advice and support. Please keep in mind their [service standards](#) if you require help.

1. Data processing overview

1.1 Ownership

Guidance notes:

- There **must** be a clear owner for any residual risk resulting from your data processing. At the ICO our Information Asset Owners (service directors) are our senior risk owners and **must** sign off on your plans.
- We **must** understand our role in relation to the personal data being processed. Our obligations will vary depending on whether we are a controller, joint controller or processor.
- If you are procuring a new product or service from a third party, you will typically find information about data protection roles and responsibilities within the service terms and conditions, or any contract being agreed between us and the third party.

Guidance Link: [Controllers and processors | ICO](#)

Project Title:	SAR Project
Project Manager:	Graham Rumens
Information Asset Owner:	Suzanne Gordon Director of Public Advice and DP Complaints
Controller(s):	ICO
Data processor(s):	Sendgrid, Cloudflare, Microsoft (existing technologies currently in use). Data-8 (use of new service with existing supplier).

1.2 Describe your new service or process

Guidance notes:

- Provide a summary of the service or process you want to implement. Include any relevant background information and your key aims/objectives.

Individuals have an important legal right to access information held on them by businesses, through making SARs. Reporting indicates that SARs going in to businesses are often formulated badly, meaning that requests are unclear or unnecessarily wide in scope. This slows down the process of the individual accessing the information they need, and gives businesses an extra administrative burden of trying to understand and meet the request. We believe that this is because individuals don't understand how to make a request in the best way, which may stop individuals exercising their right to make a request. The aim of this project is to help individuals understand their rights and how best to make a SAR, thereby supporting individuals, reducing the burden of poorly formulated SARs on businesses, and reducing complaints to the ICO.

The ICO currently has guidance on its website that aids data subjects in making a SAR request ([Preparing and submitting your subject access request | ICO](#)). The project will replace the current SAR template letter in this guidance with a digital web service, whereby an individual, can create a more specific and detailed subject access request, which will then be routed to the Organisation email address specified by the user. The requester will have the ability to specify the personal data information they are requesting, the time period relevant to the data being requested, give a reference number that better allows the organisation to identify the data requested and explain the reasons for the request. Some of these elements will be in free text, so the ICO will have no control over what data the user chooses to share with the organisation they are submitting the request to.

Once the user has completed the service (link to staging copy attached - [REDACTED]) they will receive an email containing a copy of their request and guidance on what to expect and next steps, and an email of the request is also sent to the Organisation email address the user specified in the service, again with guidance explaining the organisations responsibilities in handling the SAR.

Updated 19/9/23:

Following feedback from organisations, functionality will be added to the service to allow data subjects to upload documents, eg copy of their passport, and eg copy of a utility bill. This is designed to make it quicker and easier for organisations to carry out necessary proof of ID and proof of address checks.

Updated 22/11/23: The existing file upload feature will be enhanced with malware scanning on file upload. This will mean that as customers upload their documents to the service, they will be scanned using [REDACTED]

[REDACTED]. Before submitting the request to the organisation (and the copy to the customer), only files that have been scanned and passed will be attached; otherwise they will be removed. When a file is removed, the recipient emails will contain a message 'This file was removed for security reasons' alongside the name of the file and the form question it related to.

Updated 11/10/23:

The service requires customer to enter the email address of the organisation they are making their request to. Despite pattern validation of this address, analysis shows that entered addresses can remain invalid resulting in some requests not being received and the ICO needing to contact the customer. An instant email validation service, supplied by Data-8, will be integrated which will check:

- the supplied domain exists and is set up to receive email;
- at least one of the mail servers advertised for the domain is actually live; and
- that the mail server accepts mail for the full email address.

This is designed to further reduce the likelihood of an incorrect organisation email address being entered.

The only data processed for this element of the service is the email address typed by the customer.

Updated 3/11/23:

If requests (sent by email) are not able to be delivered to the organisation (despite the checks described above), there is currently a manual process to contact customers to alert them and give advice about what to do.

A new process will be created to do this automatically.

This will not collect any new data, and will use existing technologies (MS Azure, Sendgrid) that are already used within the service.

Updated 17/01/2023:

Users of the service have always been able to use the service to make requests on behalf of other people – however we have never explicitly said that was the case. Following feedback from users that it is difficult to use the service when they are making 3rd party requests and feedback from organisations that they are not receiving all the information they need to action SARs that come through the service – we are making changes to the form that will make it easier for users to make 3rd party requests.

This will involve adding a new section to the form that asks for information about the 3rd party and the ability to upload a letter of consent or PoA document. None of this information is mandatory. This change does not mean we have authenticated that the 3rd party has consent to make the request – this responsibility still lies with the organisation, which is stated in the email they receive.

This iteration to the service uses no new technology.

1.3 Personal data inventory

Guidance notes:

- We **must** have a clear understanding of the personal data being processed. This is **essential** for identifying and managing risks.
- Use the table below to list each category of personal data being processing. Use a new row for each data category. You can add as many rows to the table as you need.
- Categories of data may not be obvious to you from the outset e.g. tracking data (IP or location) or data collated via cookies and you need to take the time to fully understand the extent of the personal data you will process.
- Your data subjects are the individuals the personal data relates to. For example, these could be members of the public, ICO employees, our contractors etc.
- Recipients will be anyone who the data is shared with.
- UK GDPR restricts transfers of personal data outside of the UK so any overseas transfers **must** be identified.
- Personal data should be kept for no longer than is necessary. You **must** identify a retention period for the personal data you intend to process.

Guidance Link: [What is personal data? | ICO](#)

Category of data	Data subjects	Recipients	Overseas transfers	Retention period
Mandatory – Data subjects name and email address.	Members of the public requesting access to the data an organisation holds on them.	Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.	Yes If yes, list the countries the data will be transferred to: Data may be processed by Twilio and its sub-processor Amazon Web Services,	Other (please specify time period below) If selecting other, please specify the length of time personal data will be retained:

			located in the US, for routing and transmission of emails worldwide as may be necessary.	<p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days.</p>
Optional – Data subjects Date of birth or other identifier (such as NHS patient number, customer reference number etc) so that an organisation can easier identify the individual making the request.	Members of the public requesting access to the data an organisation holds on them.	Organisations data subject submits request to Customer Data processors as listed above.	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p>

				<p>loss or failure</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days.</p>
<p>Optional – Data subjects contact telephone number (in the event the organisation has to call the requester for further information to help them satisfy the SAR request).</p>	<p>Members of the public requesting access to the data an organisation holds on them.</p>	<p>Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.</p>	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure</p>
<p>Optional – Data subject Address (this is to assist the receiving organisation in identifying the individual, satisfying the SAR request and in verifying identity)</p>	<p>Members of the public requesting access to the data an organisation holds on them.</p>	<p>Organisations data subject submits request to Customer (copy of their request)</p>	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time</p>

		Data processors as listed above.	Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.	<p>personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days.</p>
Optional – Data subject proof of ID and proof of address documents	Members of the public requesting access to the data an organisation holds on them.	Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control</p>

				purposes, for no more than 61 days.
Name and email address	Any third party submitting a request on behalf of a data subject.	Organisations who receive the request, 3 rd party requesters, Data processors as listed above.	Yes If yes, list the countries the data will be transferred to: Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.	Other (please specify time period below) If selecting other, please specify the length of time personal data will be retained: The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure. Data may be retained by Twilio for quality control purposes, for no more than 61 days.
Optional – evidence that someone has permission to make 3 rd party request, this could be a letter of consent, power of attorney, birth certificate or adoption certificate	Any third party submitting a request on behalf of a data subject and the data subject.	Organisations who receive the request, 3 rd party requesters, Data processors as listed above.	Yes If yes, list the countries the data will be transferred to: Data may be processed by Twilio and its sub-processor	Other (please specify time period below) If selecting other, please specify the length of time

			Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.	<p>personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days.</p>
Email address of the receiving organisation, which could be an identifiable individual	Named individuals at recipient organisation, identifiable by e-mail address	Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control</p>

				<p>purposes, for no more than 61 days.</p> <p>(Email validation requests are not stored.)</p>
<p>An individual making a request could provide personal data which forms part of Special Category or Criminal Offence data</p>	<p>Members of the public requesting access to the data an organisation holds on them.</p>	<p>Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.</p>	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days</p>

<p>Personal data could be included in the “details of the personal information being requested” – although this is not requested</p>	<p>Members of the public requesting access to the data an organisation holds on them.</p>	<p>Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.</p>	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days.</p>
<p>Individuals in providing a date range for their enquiry could enter personal data i.e. dates of a prison sentence</p>	<p>Members of the public requesting access to the data an organisation holds on them.</p>	<p>Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.</p>	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it</p>

			worldwide as may be necessary.	can recover and resend the request in event of service loss or failure. Data may be retained by Twilio for quality control purposes, for no more than 61 days.
--	--	--	--------------------------------	---

1.4 Lawful basis for processing

Guidance notes:

- To process personal data, you **must** have a lawful basis. Select a lawful basis for processing the personal data in your inventory from the drop-down lists below.

Guidance Links: [Lawful basis for processing](#) & [Lawful basis interactive guidance tool](#)

First, select a lawful basis from Article 6 of the UK GDPR.

Article 6(1)(e) - public task

If more than one lawful basis applies to your processing, please list any additional basis here:

Guidance notes:

- If your personal data inventory includes any **special category data**, you **must** identify an additional condition for processing from Article 9 of the UK GDPR.

Guidance link: [Special category data](#)

Next, if applicable, select an additional condition for processing from Article 9 of the UK GDPR:

Article 9(2)(g) - reasons of substantial public interest

If you have selected conditions (b), (h), (i) or (j) above, you also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018. Please select from the following:

Choose an item.

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of the conditions set out in Part 2 of Schedule 1 of the DPA 2018. Please select from the following:

6. Statutory and government purposes

Guidance notes:

- If you are processing **criminal offence data**, you **must** meet one of the 28 conditions for processing criminal offence data set out in paragraphs 1 to 37 Schedule 1 of the DPA 2018.

Guidance Link: [Criminal offence data](#)

Finally, if applicable select an additional condition for processing any criminal offence data:

6. Statutory and government purposes

1.5 Necessity and proportionality

Guidance note:

- You **must** assess whether your plans to process personal data are both necessary and proportionate to you achieving your purpose. You should explain why this is the case below.
- You **must** take steps to minimise the personal data you process; processing only what is adequate, relevant and necessary.
- You **should** think about any personal data you can remove without affecting your objective.
- You **should** consider if there's any opportunity to anonymise or pseudonymise the data you're using.

The SAR digital web service is entirely voluntary and designed to assist both individuals and organisations. Individuals can make SAR requests using alternative methods i.e. letter, e-mail etc if they chose to do so – the use of this service is an option for their convenience.

In using the service the mandatory fields are name, e-mail address (customer), email address (organisation), details of personal data being requested and a date range for the period of coverage being requested.

Research has shown that including these details:

- Reduces the time organisations will spend producing the SAR – therefore giving a better service to the requestors
- Reduce enquiries and complaints to the ICO
- Provide individuals with an increased chance of obtaining what they need in a more timely manner

The data we are requesting is the minimum required to be able to deliver this improved service and the likelihood of sensitive data being entered is low.

The project seeks to further the Commissioners tasks in Article 57 of the UK GDPR. Specifically:

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

And;

(d) promote the awareness of controllers and processors of their obligations under this Regulation

Update 11/10/2023

Metrics on use of the tool so far indicate that approximately 4% of SARs submitted through the service don't have a valid recipient email address. This means some SARs aren't received by the intended organisation as they fail/ bounce back. To improve this we're introducing the instant email validation service provided by Data-8. The only data processed by Data-8 to provide this service is the recipient email address (which often doesn't contain any personal data) and we consider this additional processing a necessary and proportionate way of reducing the 4% of failed requests.

Update on 3/11/2023

Metrics indicate that the Data-8 integration will reduce the likelihood of request emails being non-deliverable from about 4% to about 1%. To reduce the manual effort required to check for non-deliverables and contact customers, we're introducing an automated email. The automation will use the same data processors as the existing service (Microsoft and Sendgrid). We consider this additional processing a necessary and proportionate way to provide important alert and advice to customers, negating the need for ICO staff to further process their data.

1.6 Consulting with stakeholders

Guidance notes:

- You **should** consult with relevant stakeholders both internally (for example Cyber Security, Legal Services, IT etc.) and externally to help you identify any risks to your data subjects.
- Briefly outline who you will be consulting with to inform your DPIA.

- Where appropriate you **should** seek the views of your data subjects, or their representatives, on your intended processing. Where this isn't possible, you should explain why below.

This project deliverable has been widely presented and demonstrated (in test form) to stakeholders across the business. These include, live services, ET members, Director of DP advise and complaints, and DDaT. In producing this solution, which will be released in Beta form, we have consulted with organisations in the preceding user research process, and we will be actively capturing feedback from individuals, testers, and organisations as part of the post Go Live assessment.

2. Personal data lifecycle

Guidance Note:

- You **must** provide a systematic description of your processing from the point that personal data is first collected through to its disposal.
- This **must** include the source of the data, how it is obtained, what technology is used to process it, who has access to it, where it is stored and how and when it is disposed of.
- If your plans involve the use of any new technology, for example a new piece of software, you **must** explain how this technology works and outline any 'privacy friendly' features that are available.
- If helpful you can use the headings provided below to help you construct your lifecycle. You can include a flow diagram if this helps your explanation.

Data source and collection:

Customer enters metadata, eg description, dates, type of data, to describe the personal data that the organisation holds about them.

Technology used for the processing:

The service will use existing technology that supports the ICO website to process the information. Key technologies are [REDACTED]

[REDACTED] The file upload feature uses the existing [REDACTED] service, with [REDACTED] providing anti-malware scanning. The email validation component uses a service provided by an existing supplier contracted with the ICO, Data-8. The automated alert and advice email for requests that are non-deliverable uses existing [REDACTED] technologies [REDACTED] and [REDACTED].

Storage location:

All locations are existing. Data collected by the website will be processed and stored in the [REDACTED], which uses [REDACTED] (DP and security documentation exists). Data processed by Sendgrid may be processed on Twilio's network and by its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary (DPIA, SOR and Transfer Risk Assessment existing). Data processed by Data-8 will be processed within [REDACTED] which uses [REDACTED]. The locations of storage and processing will not be changed as a result of this project.

Access controls:

Existing access controls are implemented across all relevant resources ([REDACTED]) using the principle of least privilege and will not be changed by the introduction of this service. [REDACTED] operates an [REDACTED] certified system that includes access controls based on the principle of least privilege. Examples: Access controls for [REDACTED] resources and [REDACTED] additionally require [REDACTED]. Access controls for [REDACTED] additionally require [REDACTED], and [REDACTED]. When processing non-deliverable notifications, [REDACTED] uses [REDACTED] to access [REDACTED].

Data sharing:

Data will be shared with the customer, and the organisation, at the email addresses supplied by the customer, for the purpose of providing the service. Data shared with Data-8 will be for the purpose of checking that the recipient email address is valid. Other data sharing for the purpose of delivering the website and digital services is existing and covered by existing DPIAs and SORs

(ICO website and Azure, Silktide analytics, Cloudflare, Sendgrid) and will not be changed by the introduction of this service.

Disposal:

Subject access requests made through the service, including any uploaded documents, will be retained for 14 days after which they will be deleted. Email validation requests to Data-8 are not stored by Data-8. Alert and advice emails for non-deliverable requests are subject to the same retention schedule for Sendgrid; they are processed in real-time and are not otherwise stored. Other retention and disposal schedules are existing and will not be changed by the introduction of this service.

3. Key UK GDPR principles and requirements

Guidance notes:

- Answering the questions in this section will help you comply with essential data protection requirements.
- You may identify specific actions that are needed and you should add these to your list of DPIA outcomes in section 6.0.

3.1 Purpose & Transparency

Guidance notes:

- In most cases you will need to communicate essential information about your data processing to your data subjects. A privacy notice is the most common way of doing this.
- You **must** review the existing [privacy notice](#) on the ICO website. If your data processing involves the personal data of ICO staff, review our [Staff Privacy Notice](#) on IRIS.

- You need to decide if our existing privacy notices sufficiently cover your plans. If not, you **must** get them updated or you **must** provide your data subjects with a separate, bespoke privacy notice.

Q1. How will you provide your data subjects with information about your data processing?

An update is required to our existing privacy notice/s. This required action has been added to the DPIA outcomes (see section 6.0).

Guidance notes:

- If you identified consent as your lawful basis for processing in section 1.4 you **must** maintain appropriate records of the data subjects consent.

Guidance Link: [Consent](#)

Q2. Are you satisfied you're maintaining appropriate records of data subjects' consent?

N/A - no processing based on data subjects consent

Guidance notes:

- If you identified legitimate interests as your lawful basis for processing in section 1.4 you **should** complete a Legitimate Interests Assessment (LIA). A template LIA is available [here](#).

Guidance Link: [How do we apply legitimate interests in practice?](#)

Q3. If legitimate interests is your lawful basis for processing have you completed a [legitimate interest assessment](#)?

N/A - no processing based on legitimate interests lawful basis

If applicable, please provide a link to your completed assessment.

3.2 Accuracy

Guidance notes:

- All reasonable steps should be taken to ensure personal data is kept accurate and up to date. Steps **must** be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

Q4. Are you satisfied the personal data you're processing is accurate?

Yes

Q5. How will you ensure the personal data remains accurate for the duration of your processing?

All data is provided by the data subject themselves, or their representative (eg family member, friend, solicitor) and the ICO do not amend, update, or review this information at any stage.

The introduction of the email validation check with Data-8 is intended to improve the likelihood of the recipient's email being valid but it remains the responsibility of the customer to enter a valid email address to send their request to.

3.3 Minimisation, Retention & Deletion

Guidance notes:

- You should only collect and hold the minimum amount of personal data you need to fulfil your purpose. Data should be retained for no longer than is needed for that purpose and then deleted without delay.

Q6. Have you done everything you can to minimise the personal data you're processing?

Yes

Q7. How will you ensure the personal data are deleted at the end of the retention period?

This is an established process whereby a retention job runs every day and deletes all records, including any uploaded documents, older than 14 days.

Q8. Will you need to update the ICO [retention and disposal schedule](#)?

Yes

3.4 Security: Confidentiality, integrity and availability

Guidance notes:

- Personal data **must** be processed in a way that ensures it is appropriately secure and protected from unauthorised access, accidental loss, destruction or damage.
- You **must** make sure access to the personal data is limited to the appropriate people and ensure you're confident the processing system being used is secure.

Guidance link: [Security](#)

Q9. Where will the personal data be stored and what measures will you put in place to maintain confidentiality, integrity and availability?

Storage will be in the existing website database. Storage for any uploaded files will use the existing [REDACTED] service within the website subscription. Both are restricted to authorised users and subject to role-based access controls. There are no proposals to change those controls or give access to any additional members of staff.

There are no new storage or web services being used as part of this solution and all existing technologies have been approved elsewhere and subject to their own contracts and DPIA coverage.

We use [REDACTED] to support our email infrastructure and the operation of these services. Any personal information shared with the ICO in the SAR service may be shared with Twilio and this can include the transfer of data to the USA. We have in place Standard Contractual Clauses to safeguard this transfer and data is retained by Twilio for no more than 61 days.

Q10. Have you confirmed there are appropriate access controls to keep the personal data secure?

Yes

Q11. Has the [cyber security team](#) completed a security assessment of your plans?

In progress

Q12. If yes what was the outcome of their assessment?

We are consulting with cyber and will review/implement their recommendations as part of the Go Live process

Q13. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

The Beta will be a soft launch. We have briefed and demonstrated the service to live services and will provide recordings for future reference. We are not introducing a new business service but have consulted with live services for awareness, should they receive any customer contact.
The initial service will capture data from the requestor and pass it to the organisation without ICO intervention.
Any queries or issues resulting from the Beta (failure or service loss) will be handled by the project team, this is the purpose of the 14 day retention period - we have the ability to support the process, should it be needed.

3.5 Accountability and governance

Guidance notes:

- The accountability principle makes us responsible for demonstrating our compliance with the UK GDPR. We do this by clearly assigning responsibilities for compliance tasks, and by maintaining relevant records relating to our processing activities and decision making.
- Your Information Asset Owner is the risk owner for any residual risk associated with your data processing and **must** sign off this DPIA.

Q14. Is your Information Asset Owner aware of your plans?

Yes

Q15. Will you need to update our article 30 record of processing activities?

Yes

Q16. If you are using a data processor, have you agreed, or will you be agreeing, a written contract with them?

Yes

3.6 Individual Rights

Guidance Note:

- UK GDPR provides a number of rights to data subjects when their personal data is being processed.
- As some rights are not absolute, and only apply in limited circumstances, we may have grounds to refuse a specific request from an individual data subject. But you **must** be sure your new service or process can facilitate the exercise of these rights and it should be technically feasible for us to action a request if required.

Guidance Link: [Individual rights](#)

Q17. Is there a means of providing the data subjects with access to the personal data being processed?

Yes

Q18. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

No

As all data is input by the data subject and sent immediately on submission to the controller the ICO can not edit this. However the data subject can use the service to submit to the controller any clarification, amendment etc.

Records retained by the ICO until our retention period expires will be an accurate reflection of data submitted by the data subject when using the SAR tool and is only retained for a limited period.

Q19. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes

Q20. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes

Q21. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes

Q22. Can we erase the personal data on receipt of a request from the data subject?

Yes

4. Risk assessment

Guidance Note:

- You **must** use the table below to identify and assess risks to individuals. You can add as many rows to the table as you need.
- **Remember:** we have an **Averse** risk appetite towards compliance risks (see our [Risk Management Policy and Appetite Statement](#) for more information).
- You **must** identify measures to reduce the level of risk where possible.
- In the risk description column, you can select from common risks to individuals in the drop-down list provided. Alternatively, you can enter your own risk descriptions if preferred.
- **The drop-down list is not exhaustive**, and you must identify and assess risks within the context of your planned processing.
- Mitigation measures can be existing, i.e. they're already in place and reduce the risk without any further action being needed. Or they're expected i.e. these are additional measures you intend to take before the data processing begins in order to further reduce risk.
- Use the risk scoring criteria in [Appendix 1](#) to score your risks. You **must** score both the impact (I) and probability (P). The expected risk score total is the result of I multiplied by P.
- When considering probability, you should score based on all your mitigation measures having been implemented in order to get an *expected* risk score.

Risk description	Response to Risk	Risk Mitigation	Expected Risk Score		
			Impact	Probability	Total
<i>Example:</i> <i>Access controls are not implemented correctly, and personal</i>	Choose an item.	<i>Existing mitigation: We have checked that the system we intend to procure allows us to</i>	3	1	3 - low

	<i>data is accessible to an unauthorised party.</i>		<i>set access permissions for different users.</i> <i><u>Expected mitigation:</u> We will appoint and train a system administrator who will be responsible for implementing access controls and monitoring access. The system administrator will also audit the system periodically to review access permissions.</i>			
1.	Risk 20: A customer entering their own e-mail address incorrectly could lead to an organisation sending the response back to an unintended recipient (information breach)	Tolerate: this risk is being accepted	This requires an incorrect e-mail address being entered twice by the customer, and the incorrect address being valid in its own right. We use 'check your details' and tell organisations that they are obliged to validate the requestor as part of the process – both of these should catch incorrect e-mail addresses	1	3	3 - low
2.	Risk 21: Cyber threat, ICO e-mails could be copied and used for phishing or as spoof e-mails by bad actors.	Tolerate: this risk is being accepted	We have accepted that this could happen today. We stress to organisations that they must validate the requestor. We will refer to cyber for further advise	1	4	4- low
3.	Choose an item.		Existing mitigation:	3	1	3 - low

	<p>A customer could enter the organisation email address incorrectly, resulting in non-delivery of a request or a request going to a third party</p>	<p>Treat: this risk is being reduced by management action such as implementing controls or tackling the cause</p> <p>Tolerate: the remaining residual risk (addresses where validity cannot be determined) is accepted.</p>	<p>A pattern validation control exists in the service, to ensure that email addresses conform to a known pattern, eg organisation@domain.com</p> <p>Expected mitigation: An 'instant email validation' service provided by Data-8 will help ensure that emails are additionally addressed to an address of a live mail server that accepts email to the full email address, and where responses are 'invalid' the customer will be unable to send their request.</p> <p>Residual risk (low likelihood): Where it's not possible to determine the validity of an email address, a requester will be able to submit their request. Email bounces will be monitored and an automated service will alert and advise customers.</p>			
4.	<p>A 3rd party could try and access a data subjects information unlawfully by making a inauthentic 3rd party request.</p>	<p>Transfer: this risk is being passed on to someone else</p>	<p>Existing mitigation: We have made it clear in the correspondence with organisations that we have not validated that the 3rd</p>	3	1	3 - low

			<p>party has the right to make a request on behalf of the data subject and they must follow their own procedures for validating this.</p> <p>We have provided the functionality for people to provide evidence of their right to act on someone else's behalf.</p>			
--	--	--	--	--	--	--

5. Consult the DPO

Guidance Note:

- Once you have completed all of the sections above you **must** submit your DPIA for consideration by the DPIA Forum who will provide you with recommendations on behalf of our Data Protection Officer (DPO). The process to follow is [here](#).
- Any recommendations from the DPOs team will be recorded below and your DPIA will then be returned to you. You **must** then record your response to each recommendation, and then proceed with completing the rest of this template.

	Recommendation	Date and project stage	Project Team Response
1.	You have listed Sendgrid as a data processor in section 1.1 but not identified other data processors associated with the website. These are however mentioned elsewhere in your assessment (Microsoft, Cloudflare etc.). Some clarification is required about the role of any data processors involved here to ensure the scope of this DPIA is clearly defined. Your response in section 3 to Q16 indicates no data processors are involved, so you need to clarify this contradiction. Suggest discussing when IM&C	07/07/2023	<p>Accept</p> <p>Any comments: Q16 has been updated along with section 1.1.</p> <p>The SAR online solution is using existing website infrastructure, currently in use and covered by DPIA's and security arrangements elsewhere.</p> <p>If rejecting DPO recommendations explain why:</p>

	Service and Project Team meet on 17/7/23.		
2.	<p>There appears to be additional categories of personal data being processed that aren't included in your data inventory at 1.3. You should also include:</p> <ul style="list-style-type: none"> Name and contact details of the controller. Names can be expected as part of the email address input by requester and/or within the body of the request. E.g. My medical record held by Dr C" You also need to include the personal data individuals will include within the body of the request. For example I've been receiving treatment for cancer by Doctor C and want to request a copy of my medical record. Or I was a prisoner at HMP serving 5 years for robbery and want a copy of my file. You should expect to receive both special category data and criminal offence data via this tool. You need to identify additional 	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>Data of receiving individual at the organisation has been added to section 1.3.</p> <p>Section 1.4 Lawful basis has been updated and updated privacy policy need made in section 6.</p> <p>If rejecting DPO recommendations explain why:</p>

	lawful basis' for processing these data categories, and consider any risks resulting from this processing. Suggest discussing when IM&C Service and Project Team meet on 17/7/23.		
3.	As far as we're aware there isn't any intention to have age verification on the ICO website to restrict access the SAR generator. We recommend you work on the assumption that the SAR tool could therefore be used by children to make access requests, and the ICO may therefore process childrens data as a result. Consideration should be given to ICO guidance on processing the data of children and you need to factor this into your plans. Suggest discussing when IM&C Service and Project Team meet on 17/7/23.	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>Children have a right to submit a SAR on their own behalf and therefore we would not prevent a child from using this service - however, we think it is unlikely it will be used by many children. Our lawful basis for processing children's data remains the same - public task - as it is related to our need to support people (incl. children) to exercise their rights. Our style guide (which the tool is following) ensures we use language that is plain and accessible and should be readable by someone with a key stage 2 reading age. This is the same for our privacy notice - it should be accessible and readable by anyone so we shouldn't need a special "children's" PN. The processing is unlikely to result in high risk to children's rights and freedoms. We are not covered by the age appropriate design code. We will not be testing the product with children the level of data processing we would have to do to recruit children for testing and then test with them is disproportionate to the risks to children using the service. However, all our online services are designed to accessible and usable by anyone with access to a computer or mobile device.</p>

			If rejecting DPO recommendations explain why:
4.	We recommend removing the sentence " <i>Organisation receiving the request, who already hold the data subjects data</i> " from your data inventory as this isn't always going to be true and shouldn't be assumed. Individuals will often make speculative access requests to organisations who they suspect might hold data about them, but they don't. It is also possible the requester will include additional personal data previously not processed by the organisation within their access request. You should consider if removing this assumption presents any new risks to your data subjects.	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>Updated section 1.3 to reflect that an organisation approached may not actually hold individuals data, and included data processors as a recipient.</p> <p>We do not think that this presents any new risk.</p> <p>If rejecting DPO recommendations explain why:</p>
5.	Section 1.5 – This is currently very limited and some further justification is required here to support the public task basis for processing this data, and satisfy necessity and proportionality requirements. Some of what you've mentioned in 1.2 can be expanded upon. For example consider justifications such as reducing volume of complaints to ICO,	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>Sections 1.3 and 1.5 have been updated.</p> <p>If rejecting DPO recommendations explain why:</p>

	<p>promoting individuals rights and helping them to exercise these, educating controllers on their responsibilities and reducing burdens on business' from poorly formulated SARs.</p> <p>You should also link back to the categories of data being processed and consider opportunities, if any, to minimise the data processed and still achieve your purpose.</p> <p>It was also noted that the statement "<i>the only mandatory fields are name and e-mail address....all other information on the web service is optional</i>" might not be accurate, as a number of other elements of the tool currently indicate via * they are mandatory. Please double check this and update the DPIA accordingly.</p> <p>Suggest discussing when IM&C Service and Project Team meet on 17/7/23.</p>		
6.	<p>If you haven't already, we'd recommend you consider the scenario where an individual uses the tool to submit an access request on behalf of somebody else. It needs to be made clear to the</p>	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>The online solution accommodates 'on behalf of' requests and the guidance sent to an organisation makes clear</p>


	<p>controller receiving the request that the ICO has taken no steps to verify authorisation to act, and they should do so.</p> <p>Similarly this will presumably be the case for regular requests, we'll be asking the controller to take steps to verify the requesters identity?</p> <p>There needs to generally be more explanation in this DPIA about what information will be provided to both data subjects using the tool and controllers receiving the request as a means of mitigating risks. Suggest discussing when IM&C Service and Project Team meet on 17/7/23.</p>		<p>that the ICO has not validated the request in any way, and that they are required to carry out their normal validation checks. In the email issued to the Organisation it clearly states, "You must be satisfied that you know the identity of the requestor, and that the data you hold relates to them. You may need to contact the requestor to check their identity."</p> <p>@Steve We are actually updating the wording to include something along the lines of "The ICO has forwarded this request on behalf of the requestor and has not taken steps to validate their identity" but want to get Hannah's input on that when she returns to work on 24/07.</p> <p>If rejecting DPO recommendations explain why:</p>
7.	<p>Personal data lifecycle / Response to Q9 in section 3 - it's not completely clear where personal data will be stored and there is indication copies may be held in multiple locations. It's important there is developed understanding of all places this data might be duplicated so the same retention rules can be applied. Without this there is a risk we retain data longer than required (14 days) and risk misinforming data subjects.</p>	07/07/2023	<p>Accept</p> <p>Any comments: Section 3 Q9 has been updated, as there are no new web services being introduced we are utilising existing time-served retention practices.</p> <p>@Steve I have clarified that Sendgrid will store minimal random content samples for 61 days, as is the case with our other online web form services – such as making a complaint or data protection fee. The following extract is taken from our current website privacy notice, so am proposing to include it in S3. Q9:</p>

			<p>“We use Twilio Sendgrid to support our email infrastructure and the operation of these services. Any personal information you share with us may be shared with Twilio and this can include the transfer of data to the USA. We have in place Standard Contractual Clauses to safeguard this transfer and data is retained by Twilio for no more than 61 days”.</p> <p>If rejecting DPO recommendations explain why:</p>
8.	<p>Access Controls –</p> <p>Access is described as limited to authorised users: website editors in comms, Tony Francis, Greer Schick and Hannah Smith in DDat. Please expand on how these accounts are managed. As per recommendation 7 if data is being held in multiple locations you should consider whether access to this data is actually wider than this pool of individuals and consider any risks.</p>	07/07/2023	<p>Accept</p> <p>Any comments: We are not introducing any new technologies and will continue with existing access practices used elsewhere, and approved, in the the business.</p> <p>If rejecting DPO recommendations explain why:</p>
9.	<p>Section 3</p> <p>Q2. - We’re unable to identify any data processing that relies on an individuals consent. Your response here should be N/A so it has been changed.</p>	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>If rejecting DPO recommendations explain why:</p>

	<p>Q8. – an update to the retention schedule will be required and response should be Yes so this has been changed. Action added to section 6.</p> <p>Q15. - An update to the ROPA will be needed. Response changed to Yes and added as an action in section 6.</p> <p>Q16. - See recommendation 1, clarification required on data processors.</p> <p>Q18, 19 & 20. – clarification required as to why these questions have been answered no as these are fundamental GDPR rights. Suggest discussing when IM&C Service and Project Team meet on 17/7/23.</p>		<p>The part that the ICO plays in the process is to forward the SAR request to external organisations. These questions have been answered on the basis that once we have delivered the mail we cannot then retrieve it, or amend it with the organisation is question. We should review these q's and our understanding of whats being asked.</p> <p>SJ 18/07/2023 – explanation for no response added to Q18. Q19 and Q20 reviewed and response changed to Yes.</p>
<p>10.</p>	<p>Risk Assessment – generally the risk assessment is very limited and will need to be reconsidered once the above recommendations have been addressed.</p>	<p>07/07/2023</p>	<p>Reject</p> <p>Any comments:</p> <p>If rejecting DPO recommendations explain why:</p>

	<p>A few additional risks (not exclusive list) we suggest you consider are:</p> <ul style="list-style-type: none"> • 1. the risk of the SAR tool failing, and an individual being unable to exercise rights. E.g. they think they've made a SAR but it's not been submitted correctly. Consider what controls are in place to alert us to send failures, bounce backs etc. and how do we intend to alert individuals if an email fails. • 2. Security controls are inadequate for protecting personal data resulting in a loss of confidentiality, integrity, availability. • 3. Risk of an individual sending their SAR request to wrong org – what validation measures / warnings are in place to prevent this. • 4. Individuals are unable to exercise their rights in relation to our processing (unless responses to Q18, 19 & 20 change). 		<p>The project has a formal Risk register which is fluid and will be signed off by the project sponsor, and any caveats completed before Go live.</p> <p>All the risks mentioned opposite are listed on the register, with the exception of:</p> <p>4. See above comments in point 9 ref these q's</p> <p>5. This has been addressed in point 3 above</p> <p>6. Addressed in point 7 above</p> <p>Key DPIA risks in project risk register include:</p> <p>7. In creating a tool, with contact data provided by the ICO, with an inferred responsibility for accuracy and delivery to an organisation, we risk legal challenge in the event of an error. If we direct a request to an inaccurate address, this could lead to the disclosure of personal data to a 3rd party.</p> <p>15. Due to the generator tool capturing data from requestors completing a SAR request, we are processing (potentially sensitive) person information, which could run risks to individuals if redirected or used incorrectly.</p> <p>16. The MMP solution tool hosts the routing of SAR requests via e-mail to the intended recipient. The ICO could become responsible for any delay in delivering the SAR request, as any 'bounce back' failure messages, from organisations, are not sent back to the originator - in the</p>
--	---	--	--

	<ul style="list-style-type: none"> • 5. Lack of age verification and risks associated with processing childrens data. • 6. Data retained for longer than is necessary 		<p>event of an incorrect e-mail being entered by the customer.</p> <p>19. The organisation receiving the request via the tool doesn't recognise it as a SAR or doesn't trust that it's legitimate, leading to the customer not receiving a response.</p> <p>20. The customer entering an incorrect email address as their own email address may lead to the organisation sending the response to an email address that doesn't exist, or sending it to the wrong recipient (information breach).</p> <p>21. Cyber Threat, partially linked to Risk 20. In sending ICO branded e-mails to requestors and organisations, as part of our intermediary role for SAR requests, There is a risk that these will be copied by bad actors and issued as part of phishing campaigns, spoof e-mails or other purposes to illegally capture or intercept personal data. Does an ICO branded SAR request being received by an organisation give the impression that the ICO have validated the requestor? Could this assumption lead to some organisations releasing personal data without carrying out security validations when receiving these requests?</p> <p>23. An individual could add personal special category data or criminal record data to the online solution. This could be a risk to individuals if redirected or used incorrectly (related to 15)</p>
--	---	--	---

			<p>Attached is a link to project risk register with risk scores and mitigations in place for each of these risks –</p> <p> Project%20RAID%20og%20-%20SAR%20</p>
--	--	--	--

6. Integrate the DPIA outcomes

Guidance Note:

- Completing sections 1 to 5 of your DPIA will have helped you identify a number of key actions that you now **must** take to meet UK GDPR requirements and minimise risks to your data subjects. For example, you may now need to draft a privacy notice for your data subjects; or you could have risk mitigations that you need to go and implement.
- You **should** also consider whether any additional actions are required as a result of any recommendations you received from the DPOs team.
- Use the table below to list the actions you need to take and track your progress with implementation. Most actions will typically need to be completed **before** you can start your processing.

Action	Date for completion	Responsibility for Action	Completed Date
Review/update of privacy policy	14 th July 23	SAT Tool project team	01/08/2023 - SJ
Review of cyber feedback	14 th July 23	Greer Schick/Graham Rumens	31/7/23 - GS
Update retention Schedule	ASAP	Greer Schick/Graham Rumens/ IM&C Service	07/08/2023 - SJ
Update ROPA	ASAP	Greer Schick/Graham Rumens/ IM&C Service	07/08/2023 - SJ

7. Expected residual risk and sign off by the IAO

Guidance note:

- Summarise the expected residual risk below for the benefit of your IAO. This is any remaining risk **after** you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank.
- If the expected residual risk remains high (i.e. red on the traffic light scoring in the Appendix) then you **must** consult the ICO as the regulator by following the process used by external organisations.

--

7.1 IAO sign off

Guidance Note:

- Your IAO owns the risks associated with your processing and they have final sign off on your plans. You **must** get your IAO to review the expected residual risk and confirm their acceptance of this risk before you proceed.
- Once your DPIA has been signed off it is complete. You should review it periodically or when there are any changes to your data processing.

IAO (name and role)	Date of sign off
Suzanne Gordon, Director of Public Advice and DP Complaints	19 July 2023
Suzanne Gordon, Director of Public Advice and DP Complaints	19 October 2023
Suzanne Gordon, Director of Public Advice and DP Complaints	21 November 2023
Suzanne Gordon, Director of Public Advice and DP Complaints	7 December 2023
Suzanne Gordon, Director of Public Advice and DP Complaints	19 January 2024

8. DPIA change history

Guidance note:

- You should track all significant changes to your DPIA by updating the table below.

Version	Date	Author	Change description
V0.1	30/6/23	Andy Grocott	First Draft
V0.1	4 th July 23	Graham Rumens	Draft and form completion
V0.1	07/07/2023	Steven Johnston	DPIA Forum Recommendations added to section 5. Actions updated in section 6.
V0.1	18/07/2023	Steven Johnston	Update to 1.5, 3.0 (Q18,19 & 20) made to support project team.
V1.0	19/07/2023	Suzanne Gordon	IAO Sign Off and first release
V1.1	07/08/2023	Steven Johnston	Update to section 6 – actions completed.
V1.2	14/9/23	Graham Rumens	Added optional capture of address data to Personal Data Inventory section 1.3
V1.2	19/9/23	Greer Schick	Added description of file upload functionality. Updated section 1.3 to reflect section 5 recommendation 4. Updated section 1.3 to clarify overseas data transfer due to use of Sendgrid.
V1.3	11/10/23	Greer Schick	Updated to reflect integration with Data-8 instant email validation integration.
V2.0	19/10/23	Suzanne Gordon	IAO Sign Off for addition of Data-8 email validation feature
V2.1	3/11/23	Greer Schick	Updated to reflect addition of automated alert and advice emails for non-deliverable emails
V3.0	21/11/23	Suzanne Gordon	IAO Sign Off for addition of automated alert and advice emails feature
V3.1	22/11/23	Greer Schick	Updated to Section 1.2 and Section 2 to reflect addition of anti-malware scanning feature on uploaded documents.
V3.2	7/12/23	Suzanne Gordon	IAO Sign Off for addition of anti-malware scanning feature.
V3.3	18/01/2024	Hannah Smith	Updates to 1.2, 1.3, Section 3 and Section 4 to account for iteration of service to improve SARs by third parties.

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (e.g. does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability and is represented by a RAG rating.

Probability \ Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted, and immediate action is required to reduce, avoid or transfer the risk.

From: [Greer Schick](#)
To: [Andy Grocott](#)
Subject: FW: Website feedback
Date: 18 December 2023 14:42:05
Attachments: [image001.jpg](#)



Greer Schick
Senior Product Owner - Web

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](#)

From: Greer Schick
Sent: Thursday, December 14, 2023 9:12 AM
To: [REDACTED]
Cc: Katie Makepeace-Warne <Katie.Makepeace-Warne@ico.org.uk>
Subject: RE: Website feedback

Dear [REDACTED],

Thanks for your feedback, suggestion and questions about the Make a subject access request service on our website.

Really appreciate the feedback. One of the main objectives of the service was to make subject access requests more specific, so I'm pleased that you also think it will do this.

Thanks also for the suggestion about allowing making it clear to customers that organisations may need confirmation of their ID. We currently include an instruction in the email that gets sent to the customer that advises them that the organisation will usually want to confirm their identity before providing them with any information. And that the organisation may also ask them to clarify their request. We are working on adding functionality so that customers can upload proof of ID, eg a copy of their passport or other document when they make their request, to reduce the amount of back and forth between the customer and organisation.

Re the organisation email address. We have some validation built in that is designed to reduce the likelihood of an incorrect email, however if the email is incorrect then the service will send an email back to the customer advising them that their request wasn't able to be delivered and giving advice about what to do next.

Hope that helps and thanks again for the feedback.

Kind regards, Greer.



Greer Schick
Senior Product Owner - Web

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](#)

From: noreply@ico.org.uk <noreply@ico.org.uk>

Sent: Tuesday, November 28, 2023 11:37 AM

To: Website Feedback <Web.Site@ico.org.uk>

Subject: Website feedback

External: This email originated outside the ICO.

The following was received via the website feedback form on the website.

Interview Date: 28/11/2023 11:36:57

Field	Value
What's your feedback about?	A specific page or section
URL of the page or section	https://ico.org.uk/for-the-public/make-a-subject-access-request/
Your message	<p>Hi, as someone who works for an organisation that gets a significant number of SARs the ICO template looks broadly very useful in that it guides people in terms of specificity when making a request, which is often something that can slow the process down as we have to go back and forth with the requester. I had just one suggestion and one query though.</p> <p>As a suggestion it would be useful if you make it clear that organisations may need confirmation of your ID via things like a scan of passport or driving licence.</p>

	<p>My question relates to the organisational email address. I was wondering what happens if the requester inputs this incorrectly, obviously the ICO will get a mailer daemon but will this be passed to the requester? I'm just concerned that they will think a request has been made when it hasn't.</p> <p>As I say on the whole I think this is a very positive step.</p>
Text field	-
Name	██████████
Email	████████████████████

From: [Suzanne Gordon](#)
To: [Rob Holtom](#); [Andy Grocott](#)
Subject: RE: SAR Tool - Request to "progress at risk" for next iteration of service
Date: 31 January 2024 11:14:34
Attachments: [image001.jpg](#)

Hi Andy,

I am comfortable with this risk and agree with Rob that as long as we complete the SOR within an agreed timeframe, we should proceed.

Thanks

Suzanne

From: Rob Holtom <Rob.Holtom@ico.org.uk>
Sent: Wednesday, January 31, 2024 10:56 AM
To: Andy Grocott <andy.grocott@ico.org.uk>; Suzanne Gordon <Suzanne.Gordon@ico.org.uk>
Subject: RE: SAR Tool - Request to "progress at risk" for next iteration of service

I am comfortable with progressing at risk, if we can agree a timeframe for the SoR to be completed within say 3 months.
R



Rob Holtom

Executive Director - Digital, Data and Technology (DDaT), Transformation & Delivery
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

If you wish to submit an information request or want to exercise any of your data protection rights, please forward your email to the Information Access Team at accessicoinformation@ico.org.uk, or you can call us to make a verbal request relating to your personal data on our Helpline 0303 123 1113.

For information about what we do with personal data see our [privacy notice](#)

From: Andy Grocott <andy.grocott@ico.org.uk>
Sent: Wednesday, January 31, 2024 10:48 AM
To: Suzanne Gordon <Suzanne.Gordon@ico.org.uk>; Rob Holtom <Rob.Holtom@ico.org.uk>
Subject: SAR Tool - Request to "progress at risk" for next iteration of service

Suzanne/Rob,

In line with user feedback of the SAR service, we have been working on one further iteration of the SAR service adding functionality to the service to allow data subjects to upload documents, eg copy of their passport, and copy of a utility bill. This is designed to make it quicker and easier for organisations to carry out necessary proof of ID and proof of address checks.

We are also addressing user feedback from both data subjects and Organisation relating to difficulties using the service to process requests on behalf of a another person (3rd party requests). This will involve adding a new section to the form that asks for information about the 3rd party and the ability to upload a letter of consent or PoA document. None of this information is mandatory. This change does not mean we have authenticated that the 3rd party has consent to make the request – this responsibility still lies with the organisation, which is stated in the email they receive.

To support this functionality, the existing file upload feature will be enhanced with malware scanning on file upload. This will mean that as customers upload their documents to the service, they will be scanned using [REDACTED]. Before submitting the request to the organisation (and the copy to the customer), only files that have been scanned and passed will be attached; otherwise, they will be removed. When a file is removed, the recipient emails will contain a message 'This file was removed for security reasons' alongside the name of the file and the form question it related to.

We have presented the solution to TDA and CAB and had approval and have updated the DPIA to account for these changes and had them agreed with Information Management and Suzanne as Project Sponsor. We have tested the solution to our satisfaction and have been waiting for an updated SOR (security opinion report) from colleagues in Cyber Security, prior to launching the new functionality into Production. However, colleagues in Cyber Security have informed us yesterday that,

[REDACTED]

The Scrum team are comfortable with the solution and the level of testing we have carried out, but wanted a Cyber Sec take on the solution in case we had missed something. The enhanced malware scanning is using a [REDACTED], so again we have confidence in it, but in theory there is a risk that an Organisation could make a claim that we had exposed their systems to risk by forwarding SAR requests with attached documents. As explained, documents have been virus scanned and passed using [REDACTED] before we forward them to the organisation, so I believe we can defend any complaint, but as with all things, there is an element of risk.

Our definition of done for a release calls for, amongst other things, a

"Met" SOR and a sponsor sign off of known risks associated with any release. I am therefore approaching you for your sign off and permission to "progress at risk" with the release without a "Met" SOR.

Happy to discuss.

Kind regards

Andy



Andy Grocott

Senior Digital Delivery Manager
Digital, Data and Technology

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

If you wish to submit an information request or want to exercise any of your data protection rights, please forward your email to the Information Access Team at accessicoinformation@ico.org.uk, or you can call us to make a verbal request relating to your personal data on our Helpline 0303 123 1113.

For information about what we do with personal data see our [privacy notice](#)

From: [Andy Grocott](#)
To: [Graham Rumens](#)
Subject: FW: SAR Tool - decision to "progress at risk"
Date: 02 February 2024 10:30:00
Attachments: [image001.jpg](#)
[RE SAR Tool - Request to progress at risk for next iteration of service.msg](#)

From: Andy Grocott
Sent: Wednesday, January 31, 2024 4:23 PM
To: Alan McGann <Alan.McGann@ico.org.uk>; Steven Rook <Steven.Rook@ico.org.uk>
Subject: SAR Tool - decision to "progress at risk"

Alan/Steven,

Following on from a series of IM's I had with both of you in the last day (and acting on Alan's advice), I contacted Rob Holtom and Suzanne Gordon in their roles as Executive Sponsor and Sponsor for the SAR Tool project.

I explained to Rob and Suzanne that, in line with user feedback on the SAR service, we have been working on one further iteration of the SAR service adding functionality to the service to allow data subjects to upload documents, eg copy of their passport, and copy of a utility bill. This is designed to make it quicker and easier for organisations to carry out necessary proof of ID and proof of address checks, as well as giving the functionality for individuals to raise requests on behalf of another person, in doing so uploading a document proving they had consent to act on behalf of the data subject.

I explained that to support this functionality, the existing file upload feature will be enhanced with malware scanning on file upload. This will mean that as customers upload their documents to the service, they will be scanned using [REDACTED]. Before submitting the request to the organisation (and the copy to the customer), only files that have been scanned and passed will be attached; otherwise, they will be removed. When a file is removed, the recipient emails will contain a message 'This file was removed for security reasons' alongside the name of the file and the form question it related to.

I informed them that we had taken the design to both TDA and CAB, updated the service DPIA accordingly and tested the solution in our test instance, but had been in contact with yourselves re getting an updated SOT completed for the new service functionality, but due to resource challenges/capacity and other priorities, you did not have the capacity to complete SOR's presently and Alan had proposed we raise a "progress at risk" request with the IAO/Project Sponsors.

I explained to them that, as our service release definition of done calls for, amongst other things, a "Met" SOR and a sponsor sign off of known risks associated with any release, I was requesting their authority to

"progress at risk" with the release without a "Met" SOR.

Rob and Suzanne were both the request to progress at risk with the production deployment if we could get an agreement for the SOR to be completed "within say 3 months".

Having spoken with Alan, I understand that this is an acceptable timeframe and the SOR will be scheduled for completion before the end of April 2024. As agreed with Alan, I have dropped this into an email for clarification, and so you have a record of the authority to progress at risk.

I have attached the email chain with Rob and Suzanne, in which they agreed to progress at risk, subject to an agreed timeframe for the SOR completion.

Let me know if you require anything further.

Many Thanks

Andy



Andy Grocott

Senior Digital Delivery Manager
Digital, Data and Technology

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

If you wish to submit an information request or want to exercise any of your data protection rights, please forward your email to the Information Access Team at accessicoinformation@ico.org.uk, or you can call us to make a verbal request relating to your personal data on our Helpline 0303 123 1113.

For information about what we do with personal data see our [privacy notice](#)

From: [Suzanne Gordon](#)
To: [Rob Holtom](#); [Andy Grocott](#)
Subject: RE: SAR Tool - Request to "progress at risk" for next iteration of service
Date: 31 January 2024 11:14:34
Attachments: [image001.jpg](#)

Hi Andy,

I am comfortable with this risk and agree with Rob that as long as we complete the SOR within an agreed timeframe, we should proceed.

Thanks

Suzanne

From: Rob Holtom <Rob.Holtom@ico.org.uk>
Sent: Wednesday, January 31, 2024 10:56 AM
To: Andy Grocott <andy.grocott@ico.org.uk>; Suzanne Gordon <Suzanne.Gordon@ico.org.uk>
Subject: RE: SAR Tool - Request to "progress at risk" for next iteration of service

I am comfortable with progressing at risk, if we can agree a timeframe for the SoR to be completed within say 3 months.
R



Rob Holtom

Executive Director - Digital, Data and Technology (DDaT), Transformation & Delivery
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

If you wish to submit an information request or want to exercise any of your data protection rights, please forward your email to the Information Access Team at accessicoinformation@ico.org.uk, or you can call us to make a verbal request relating to your personal data on our Helpline 0303 123 1113.

For information about what we do with personal data see our [privacy notice](#)

From: Andy Grocott <andy.grocott@ico.org.uk>
Sent: Wednesday, January 31, 2024 10:48 AM
To: Suzanne Gordon <Suzanne.Gordon@ico.org.uk>; Rob Holtom <Rob.Holtom@ico.org.uk>
Subject: SAR Tool - Request to "progress at risk" for next iteration of service

Suzanne/Rob,

In line with user feedback of the SAR service, we have been working on one further iteration of the SAR service adding functionality to the service to allow data subjects to upload documents, eg copy of their passport, and copy of a utility bill. This is designed to make it quicker and easier for organisations to carry out necessary proof of ID and proof of address checks.

We are also addressing user feedback from both data subjects and Organisation relating to difficulties using the service to process requests on behalf of a another person (3rd party requests). This will involve adding a new section to the form that asks for information about the 3rd party and the ability to upload a letter of consent or PoA document. None of this information is mandatory. This change does not mean we have authenticated that the 3rd party has consent to make the request – this responsibility still lies with the organisation, which is stated in the email they receive.

To support this functionality, the existing file upload feature will be enhanced with malware scanning on file upload. This will mean that as customers upload their documents to the service, they will be scanned using [REDACTED]. Before submitting the request to the organisation (and the copy to the customer), only files that have been scanned and passed will be attached; otherwise, they will be removed. When a file is removed, the recipient emails will contain a message 'This file was removed for security reasons' alongside the name of the file and the form question it related to.

We have presented the solution to TDA and CAB and had approval and have updated the DPIA to account for these changes and had them agreed with Information Management and Suzanne as Project Sponsor. We have tested the solution to our satisfaction and have been waiting for an updated SOR (security opinion report) from colleagues in Cyber Security, prior to launching the new functionality into Production.

[REDACTED]

The Scrum team are comfortable with the solution and the level of testing we have carried out, but wanted a Cyber Sec take on the solution in case we had missed something. The enhanced malware scanning is using a Microsoft product, so again we have confidence in it, but in theory there is a risk that an Organisation could make a claim that we had exposed their systems to risk by forwarding SAR requests with attached documents. As explained, documents have been virus scanned and passed using MS Defender before we forward them to the organisation, so I believe we can defend any complaint, but as with all things, there is an element of risk.

Our definition of done for a release calls for, amongst other things, a

"Met" SOR and a sponsor sign off of known risks associated with any release. I am therefore approaching you for your sign off and permission to "progress at risk" with the release without a "Met" SOR.

Happy to discuss.

Kind regards

Andy



Andy Grocott

Senior Digital Delivery Manager
Digital, Data and Technology

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

If you wish to submit an information request or want to exercise any of your data protection rights, please forward your email to the Information Access Team at accessicoinformation@ico.org.uk, or you can call us to make a verbal request relating to your personal data on our Helpline 0303 123 1113.

For information about what we do with personal data see our [privacy notice](#)

From: [Digital Content](#)
To: [Graham Rumens](#)
Subject: RE: SAR on Iris
Date: 21 February 2024 10:06:45
Attachments: [image002.gif](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)
[image006.jpg](#)
[image007.png](#)
[image008.png](#)
[image009.png](#)
[image010.png](#)
[image011.png](#)

Thanks, updated.



Stephen Morris
Senior Communications Officer

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

If you wish to submit an information request or want to exercise any of your data protection rights, please forward your email to the Information Access Team at accessicoinformation@ico.org.uk, or you can call us to make a verbal request relating to your personal data on our Helpline 0303 123 1113.

For information about what we do with personal data see our [privacy notice](#)

From: Graham Rumens <Graham.Rumens@ico.org.uk>
Sent: Wednesday, February 21, 2024 9:54 AM
To: Digital Content <[\[REDACTED\]](#)>
Subject: RE: SAR on Iris

Please could you make the following changes to this page please?

What?

The team engaged in user research during spring 2023 and established some key problems and requirements for both SAR requestors and organisations. This produced several potential solutions and we developed and tested a digital tool, which was released as a Beta in August 2023.

Following the release of the Beta version, we have continued to capture feedback from both requestors and organisations using the service. This established a prioritised list of additional requirements - which have

subsequently been developed and released. Real-time email 'validation' of organisations the requestor is contacting, full Welsh language service, automated email 'bounce-back' process which notifies requestors when their email to an organisation has not been delivered, are now all live.

Additional functionality to facilitate 3rd party requests and file uploads will be released in **late February 2024**.

When?

The Beta version went live in August, with additional functionality releases in October and November and full go live expected in **late February 2024**.

Thanks
Graham



From: Digital Content <[REDACTED]>
Sent: Monday, November 20, 2023 11:13 AM
To: Graham Rumens <Graham.Rumens@ico.org.uk>
Subject: RE: SAR on Iris

Thanks Graham, updated.



Stephen Morris
Senior Communications Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

[REDACTED] ico.org.uk twitter.com/iconews

Please consider the environment before printing this email

If you wish to submit an information request or want to exercise any of your data protection rights, please forward your email to the Information Access Team at accessicoinformation@ico.org.uk, or you can call us to make a verbal request relating to your personal data on our Helpline 0303 123 1113.

For information about what we do with personal data see our [privacy notice](#)

From: Graham Rumens <Graham.Rumens@ico.org.uk>

Sent: Monday, November 20, 2023 9:42 AM

To: Digital Content [REDACTED]

Subject: RE: SAR on Iris

Morning could I please make the following updates to the SAR Tool page on IRIS?

What?

The team engaged in user research during spring 2023 and established some key problems and requirements for both SAR requestors and organisations. This produced several potential solutions and we developed and tested a digital tool, which was released as a Beta in August 2023.

Following the release of the Beta version, we have continued to capture feedback from both requestors and organisations using the service. This established a prioritised list of additional requirements - which are being released in product upgrades, during November. These include, Live E-mail 'validation' of organisations the requestor is contacting, file upload capabilities, improved guidance, and an automated e-mail 'bounce-back' process which notifies requestors when their E-mail to an organisation has not been delivered. In addition, the service is now fully available in Welsh language.

When?

The Beta version went Live in August, additional functionality releases in October and November with full Go Live expected in December 23.

Thanks

Graham



From: Graham Rumens

Sent: Thursday, August 24, 2023 10:24 AM

To: Digital Content [REDACTED] >

Subject: RE: SAR on Iris

Thanks, he's doing a lot of testing so Product Tester works



From: Digital Content <[REDACTED]>
Sent: Thursday, August 24, 2023 10:15 AM
To: Graham Rumens <Graham.Rumens@ico.org.uk>
Subject: RE: SAR on Iris

Thanks, updates made. What's Anthony's role in the project?

	<p>Stephen Morris Senior Communications Officer</p> <p>Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF ico.org.uk twitter.com/iconews For information about what we do with personal data see our privacy notice Please consider the environment before printing this email</p>
--	---

From: Graham Rumens <Graham.Rumens@ico.org.uk>
Sent: Thursday, August 24, 2023 8:46 AM
To: Digital Content <[REDACTED]>
Subject: RE: SAR on Iris

Morning

Please could you update the SAR IRIS project page?

WHY? – **unchanged on current text**

What?

The team engaged in user research, during the spring 23, and established some key problems and requirements for both SAR requestors and organisations. This produced **several** potential solutions and we **developed and tested a digital tool - which was released as a Beta in August 23. We are actively monitoring the use of the Beta and**

capturing feedback from both requestors and organisations. Initial measures show that the Tool is being used three times more than the Word document it replaced, and satisfaction scores from users are 4.5+ out of 5. Future versions of the Tool are now being developed, including a Welsh language translation together with other functionality requested in customer feedback.

When ?

The first Beta version of the Tool is now live, with further iterations scheduled this Autumn.

Please could you also add Anthony Francis to the project team?

Thanks
Graham



From: Digital Content <digitalcontent@ico.org.uk>
Sent: Tuesday, June 27, 2023 10:37 AM
To: Graham Rumens <Graham.Rumens@ico.org.uk>
Subject: RE: SAR on Iris

Thanks Graham, updated.

	<p>Stephen Morris Senior Communications Officer</p> <p>Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF ico.org.uk twitter.com/iconews</p> <p>For information about what we do with personal data see our privacy notice</p> <p>Please consider the environment before printing this email</p>
--	---

From: Graham Rumens <Graham.Rumens@ico.org.uk>
Sent: Tuesday, June 27, 2023 8:32 AM
To: Digital Content <digitalcontent@ico.org.uk>
Subject: RE: SAR on Iris

Please can you update the Iris project Tile for SAR please?

[Subject Access Requests \(sharepoint.com\)](#)

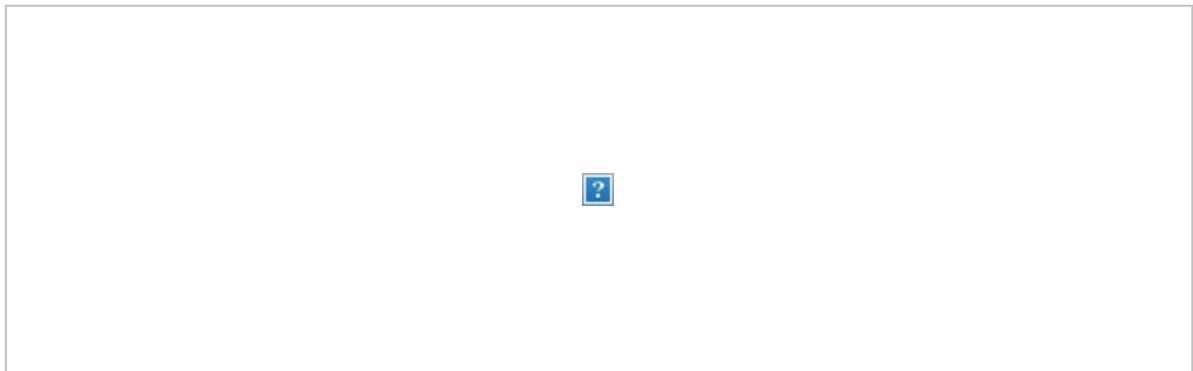
What?

The team engaged in user research, during the spring 23, and established some key problems and requirements for both SAR requestors and organisations. This produced some potential solutions and we currently have two versions of a prototype Tool under development. The first iteration of the Tool is scheduled to be released as a Beta launch soon.

When ?

The first Beta version of the Tool is scheduled to be released in early Jul 23.

Thanks
Graham



From: Digital Content <digitalcontent@ico.org.uk>

Sent: Thursday, May 25, 2023 12:43 PM

To: Graham.Rumens <Graham.Rumens@ico.org.uk>; Digital Content <digitalcontent@ico.org.uk>

Subject: RE: SAR on Iris

Hi Graham, can confirm this has now been added.

Let me know if you need anything else.

Thanks

Michael

From: Graham.Rumens <Graham.Rumens@ico.org.uk>

Sent: 25 May 2023 11:24

To: Digital Content <digitalcontent@ico.org.uk>

Subject: RE: SAR on Iris

Many thanks

We would like to populate the What? Section have produced the following:

The team have engaged in User Research, during the foundation stage, to establish the key problems and requirements. This has produced some potential solutions which we are currently developing as prototypes during an Alpha phase. These will be introduced to users for testing and feedback to gauge the potential to further develop these possible solutions.

Thanks
Graham



From: Digital Content <digitalcontent@ico.org.uk>
Sent: Wednesday, May 24, 2023 10:31 AM
To: Graham.Rumens <Graham.Rumens@ico.org.uk>
Subject: RE: SAR on Iris

Thanks Graham, I've added [Subject Access Requests \(sharepoint.com\)](#) and added it to the main projects section [Projects - Home \(sharepoint.com\)](#)

Have left the 'What' section as TBC for now – please get in touch when you know what specifically is being developed and we'll update.

From: Graham.Rumens <Graham.Rumens@ico.org.uk>
Sent: Monday, May 22, 2023 8:53 AM
To: Digital Content <digitalcontent@ico.org.uk>
Subject: RE: SAR on Iris

Thanks Stephen

Details requested below:

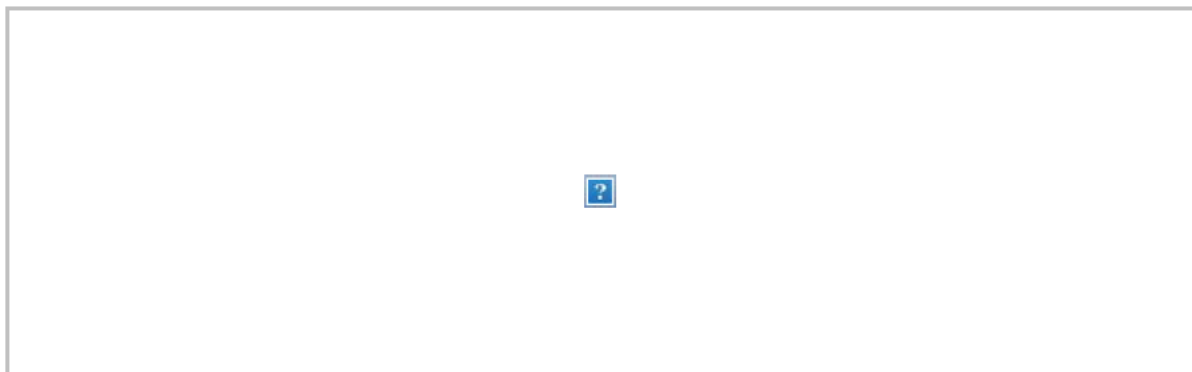
Code 297

Strapline: Implement a tool and/or guidance to assist both individuals and organisations in making and managing SAR requests

Why? A significant proportion of data protection complaints that we receive are from people **who feel they have not been given access** to the personal data an organisation holds about them. These are called Subject Access Requests (SARs). To help improve outcomes for people raising SARs, make it easier for organisations to respond to them, and lower complaints to the ICO, we have started designing and developing improved online SAR tools and guidance. We are aiming to launch changes by autumn 2023.

Project Team: Andy Grocott Scrum Master, Greer Schick Web/Tool Development, Hannah Smith User Research, Asad Rahman Technical BA, Suzanne Gordon Project Sponsor, Rob Holtom ET Sponsor, Graham Rumens PMO Project Manager

Thanks
Graham



From: Digital Content <digitalcontent@ico.org.uk>
Sent: Friday, May 19, 2023 1:57 PM
To: Graham.Rumens <Graham.Rumens@ico.org.uk>
Subject: RE: SAR on Iris

Hi Graham,

Our PMO Iris rep is Sophie McKenna who can work with us to get a page set up. However I can see she's on leave at the moment – if you can send the following info we'll get a page set up:

- Project strapline – 1 sentence on the goal of the project
- Project code
- Text for Why?, What? And When? Sections
- Project team (including their roles in the project)

For examples please see existing pages on [Projects - Home \(sharepoint.com\)](#)

Thanks,

Stephen

From: Graham.Rumens <Graham.Rumens@ico.org.uk>
Sent: 19 May 2023 13:35
To: Digital Content <digitalcontent@ico.org.uk>

Subject: SAR on Iris

Please can we set up a project overview for the SAR project on IRIS within the PMO project page?

What's the process and how do I submit the content?

Thanks
Graham



From: [Greer Schick](#)
To: [IThelp](#)
Subject: RE: SAR Service update - Ticket Update [CR:1060296]
Date: 05 March 2024 19:38:00
Attachments: [image001.jpg](#)

This change was completed successfully



Greer Schick
Senior Product Owner - Web

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](#)

From: IThelp [REDACTED]
Sent: Tuesday, March 5, 2024 10:20 AM
To: Greer Schick <Greer.Schick@ico.org.uk>
Subject: Re: SAR Service update - Ticket Update [CR:1060296]

Hi, Greer Schick

Your change has been approved. If you could please reply to this email with any update / the outcome of the change.

Details:	
Change Title	Website – Subject access request service - Adding proof of ID and ability to make requests on behalf of someone else
ID	1060296
Username	Greer Schick
Date Occurred	22/02/2024 20:42
Change Reference Number	240049
Change Type	Normal
Change Owner	Greer Schick
Technical Owner	Greer Schick
Product Owner aware of change	Yes - Consulted
Change Start Date & Time	05/03/2024 11:00
Estimated time to Implement	30 minutes
Change End Time * Date	05/03/2024 11:40
Outage required	No

Outage duration	
Site access required	No
Summary of Change	<p>This change is to make an update to the Make a subject access request service.</p> <p>The update will allow customers to upload proof of identity and proof of address documents to the service, so that organisations have everything they need to progress their request. It will also make it more explicit that third parties can complete the service on behalf of someone else, for example an elderly relative or a client, to make the service more accessible.</p> <p>The expected result is that the service will be updated to include additional fields that ask customers for documents. This will also bring on-upload malware scanning in to live use.</p>

Implementation Plan

Prerequisites

Changes completed on pre-production environments, all tests and regression tests passed.

Updated web form copied into Production environment.

29 February

ICO, Greer Schick:

1. Temporarily remove 'Start' button from start page and replace with holding text explaining that the service is temporarily unavailable, and to try again later.
2. Wait 10 minutes for any existing traffic to clear the form.
3. Replace the form residing on the Make a subject access request page with the updated form, save and publish.
4. Reinstate start button.
5. Smoke test access to the updated form.
6. Check that subject access requests are being completed.
7. Once checks have passed, delete previous version of form.

Test Plan

Smoke testing as above.

Testing Resource

Anthony Francis

Backout plan

As needed:

1. Temporarily remove 'Start' button from start page and replace with holding text explaining that the service is temporarily unavailable, and to try again later.
2. Wait 10 minutes for any existing traffic to clear the form.
3. Replace the form residing on the Make a subject access request page with the previous version of the form, save and publish.
4. Reinstate start button.
5. Smoke test access to the updated form.

6. Check that subject access requests are being completed.

Time to backout

15 minutes

DPIA Screening complete

Yes - DPIA Required

DPIA Signed Off

Yes

DPIA Link (EDRM)

https://edrm/sites/corp/im/GovAccount/_layouts/15/DocIdRedir.aspx?ID=CORP-1937519151-692

Risk

Low

Impact

Low

Impact if not completed

- Opportunity not taken / delay to updating form to make it easier for organisations receiving subject access requests and make it more accessible for users who want someone to use the service on their behalf.

Residual risk and impact

The risks of introducing on-upload malware scanning have been accepted and it is considered a robust and proportionate solution. The architecture was designed with Shout and design approved by TDA.

Change to DR

Yes

Summary of Changes to DR

\$ChangeChangesToDRSummary

Disk Addition

No

Additional details on disks affected

Security Risk Assessment

The residual risk of malware contained in an uploaded file not being detected and going on to a recipient organisation have been accepted. The on-upload malware scanning has been accepted as a robust and proportionate mitigation. The architecture was designed with Shout and design approved by TDA.

Affected CI's

ICO website in Digital Service subscription

Please reply to this e-mail to respond.

Thank you.

PS. If you want to see a full history and the status of your tickets , please visit HALO, the IT Help Self-Service portal at: <https://digitalandit.haloitsm.com/portal/tickets>



Jonny Wicks

Incident, Problem and Change Manager

Information Commissioner's Office, Wycliffe House, Water Lane,
Wilmslow, Cheshire SK9 5AF

T. 0330 414 6260 F. 01625 524510 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](#)

Data Protection Impact Assessment (DPIA) – SAR Project

Document Name	Data Protection Impact Assessment – SAR Project
Author/Owner (name and job title)	Andy Grocott – Project Scrum Master Graham Rumens – Project Manager
Department/Team	Digital, Data and Technology
Document Status	Published
Version Number	V3.3
Release Date	19/07/2023
Approver (if applicable)	Suzanne Gordon, Director of Public Advice and DP Complaints
Review Date	19/07/2024
Distribution	Internal

Guidance for completing this DPIA template

- If you're unsure whether you need to complete a DPIA, use the [Screening assessment - do I need to do a DPIA?](#) first to help you decide.
- **Must** and **should** are used throughout the guidance notes in this template to help you understand which things are a legislative requirement and **must** be done versus things that the ICO considers **should** be done as best practice to comply effectively with the law.
- You **must** complete this DPIA template if your screening assessment indicates a DPIA is required.
- You **should** aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you won't be able to continue with your plans without changing them, or at all.
- We recommend that you fill out each section of this template in order, as each subsequent section builds upon the last. You will not be able to complete later sections correctly if you skip ahead. You **should** read the guidance notes throughout this template to help you with each section.
- If you are struggling with completing this template the [Information Management and Compliance Service](#) is available to provide advice and support. Please keep in mind their [service standards](#) if you require help.

1. Data processing overview

1.1 Ownership

Guidance notes:

- There **must** be a clear owner for any residual risk resulting from your data processing. At the ICO our Information Asset Owners (service directors) are our senior risk owners and **must** sign off on your plans.
- We **must** understand our role in relation to the personal data being processed. Our obligations will vary depending on whether we are a controller, joint controller or processor.
- If you are procuring a new product or service from a third party, you will typically find information about data protection roles and responsibilities within the service terms and conditions, or any contract being agreed between us and the third party.

Guidance Link: [Controllers and processors | ICO](#)

Project Title:	SAR Project
Project Manager:	Graham Rumens
Information Asset Owner:	Suzanne Gordon Director of Public Advice and DP Complaints
Controller(s):	ICO
Data processor(s):	Sendgrid, Cloudflare, Microsoft (existing technologies currently in use). Data-8 (use of new service with existing supplier).

1.2 Describe your new service or process

Guidance notes:

- Provide a summary of the service or process you want to implement. Include any relevant background information and your key aims/objectives.

Individuals have an important legal right to access information held on them by businesses, through making SARs. Reporting indicates that SARs going in to businesses are often formulated badly, meaning that requests are unclear or unnecessarily wide in scope. This slows down the process of the individual accessing the information they need, and gives businesses an extra administrative burden of trying to understand and meet the request. We believe that this is because individuals don't understand how to make a request in the best way, which may stop individuals exercising their right to make a request. The aim of this project is to help individuals understand their rights and how best to make a SAR, thereby supporting individuals, reducing the burden of poorly formulated SARs on businesses, and reducing complaints to the ICO.

The ICO currently has guidance on its website that aids data subjects in making a SAR request ([Preparing and submitting your subject access request | ICO](#)). The project will replace the current SAR template letter in this guidance with a digital web service, whereby an individual, can create a more specific and detailed subject access request, which will then be routed to the Organisation email address specified by the user. The requester will have the ability to specify the personal data information they are requesting, the time period relevant to the data being requested, give a reference number that better allows the organisation to identify the data requested and explain the reasons for the request. Some of these elements will be in free text, so the ICO will have no control over what data the user chooses to share with the organisation they are submitting the request to.

Once the user has completed the service (link to staging copy attached - [REDACTED]) they will receive an email containing a copy of their request and guidance on what to expect and next steps, and an email of the request is also sent to the Organisation email address the user specified in the service, again with guidance explaining the organisations responsibilities in handling the SAR.

Updated 19/9/23:

Following feedback from organisations, functionality will be added to the service to allow data subjects to upload documents, eg copy of their passport, and eg copy of a utility bill. This is designed to make it quicker and easier for organisations to carry out necessary proof of ID and proof of address checks.

Updated 22/11/23: The existing file upload feature will be enhanced with malware scanning on file upload. This will mean that as customers upload their documents to the service, they will be scanned using [REDACTED]

[REDACTED]. Before submitting the request to the organisation (and the copy to the customer), only files that have been scanned and passed will be attached; otherwise they will be removed. When a file is removed, the recipient emails will contain a message 'This file was removed for security reasons' alongside the name of the file and the form question it related to.

Updated 11/10/23:

The service requires customer to enter the email address of the organisation they are making their request to. Despite pattern validation of this address, analysis shows that entered addresses can remain invalid resulting in some requests not being received and the ICO needing to contact the customer. An instant email validation service, supplied by Data-8, will be integrated which will check:

- the supplied domain exists and is set up to receive email;
- at least one of the mail servers advertised for the domain is actually live; and
- that the mail server accepts mail for the full email address.

This is designed to further reduce the likelihood of an incorrect organisation email address being entered.

The only data processed for this element of the service is the email address typed by the customer.

Updated 3/11/23:

If requests (sent by email) are not able to be delivered to the organisation (despite the checks described above), there is currently a manual process to contact customers to alert them and give advice about what to do.

A new process will be created to do this automatically.

This will not collect any new data, and will use existing technologies (MS Azure, Sendgrid) that are already used within the service.

Updated 17/01/2023:

Users of the service have always been able to use the service to make requests on behalf of other people – however we have never explicitly said that was the case. Following feedback from users that it is difficult to use the service when they are making 3rd party requests and feedback from organisations that they are not receiving all the information they need to action SARs that come through the service – we are making changes to the form that will make it easier for users to make 3rd party requests.

This will involve adding a new section to the form that asks for information about the 3rd party and the ability to upload a letter of consent or PoA document. None of this information is mandatory. This change does not mean we have authenticated that the 3rd party has consent to make the request – this responsibility still lies with the organisation, which is stated in the email they receive.

This iteration to the service uses no new technology.

1.3 Personal data inventory

Guidance notes:

- We **must** have a clear understanding of the personal data being processed. This is **essential** for identifying and managing risks.
- Use the table below to list each category of personal data being processing. Use a new row for each data category. You can add as many rows to the table as you need.
- Categories of data may not be obvious to you from the outset e.g. tracking data (IP or location) or data collated via cookies and you need to take the time to fully understand the extent of the personal data you will process.
- Your data subjects are the individuals the personal data relates to. For example, these could be members of the public, ICO employees, our contractors etc.
- Recipients will be anyone who the data is shared with.
- UK GDPR restricts transfers of personal data outside of the UK so any overseas transfers **must** be identified.
- Personal data should be kept for no longer than is necessary. You **must** identify a retention period for the personal data you intend to process.

Guidance Link: [What is personal data? | ICO](#)

Category of data	Data subjects	Recipients	Overseas transfers	Retention period
Mandatory – Data subjects name and email address.	Members of the public requesting access to the data an organisation holds on them.	Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.	Yes If yes, list the countries the data will be transferred to: Data may be processed by Twilio and its sub-processor Amazon Web Services,	Other (please specify time period below) If selecting other, please specify the length of time personal data will be retained:

			located in the US, for routing and transmission of emails worldwide as may be necessary.	<p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days.</p>
Optional – Data subjects Date of birth or other identifier (such as NHS patient number, customer reference number etc) so that an organisation can easier identify the individual making the request.	Members of the public requesting access to the data an organisation holds on them.	Organisations data subject submits request to Customer Data processors as listed above.	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p>

				<p>loss or failure</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days.</p>
<p>Optional – Data subjects contact telephone number (in the event the organisation has to call the requester for further information to help them satisfy the SAR request).</p>	<p>Members of the public requesting access to the data an organisation holds on them.</p>	<p>Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.</p>	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure</p>
<p>Optional – Data subject Address (this is to assist the receiving organisation in identifying the individual, satisfying the SAR request and in verifying identity)</p>	<p>Members of the public requesting access to the data an organisation holds on them.</p>	<p>Organisations data subject submits request to Customer (copy of their request)</p>	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time</p>

		Data processors as listed above.	Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.	<p>personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days.</p>
Optional – Data subject proof of ID and proof of address documents	Members of the public requesting access to the data an organisation holds on them.	Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control</p>

				purposes, for no more than 61 days.
Name and email address	Any third party submitting a request on behalf of a data subject.	Organisations who receive the request, 3 rd party requesters, Data processors as listed above.	Yes If yes, list the countries the data will be transferred to: Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.	Other (please specify time period below) If selecting other, please specify the length of time personal data will be retained: The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure. Data may be retained by Twilio for quality control purposes, for no more than 61 days.
Optional – evidence that someone has permission to make 3 rd party request, this could be a letter of consent, power of attorney, birth certificate or adoption certificate	Any third party submitting a request on behalf of a data subject and the data subject.	Organisations who receive the request, 3 rd party requesters, Data processors as listed above.	Yes If yes, list the countries the data will be transferred to: Data may be processed by Twilio and its sub-processor	Other (please specify time period below) If selecting other, please specify the length of time

			Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.	<p>personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days.</p>
Email address of the receiving organisation, which could be an identifiable individual	Named individuals at recipient organisation, identifiable by e-mail address	Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control</p>

				<p>purposes, for no more than 61 days.</p> <p>(Email validation requests are not stored.)</p>
<p>An individual making a request could provide personal data which forms part of Special Category or Criminal Offence data</p>	<p>Members of the public requesting access to the data an organisation holds on them.</p>	<p>Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.</p>	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days</p>

<p>Personal data could be included in the “details of the personal information being requested” – although this is not requested</p>	<p>Members of the public requesting access to the data an organisation holds on them.</p>	<p>Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.</p>	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it can recover and resend the request in event of service loss or failure.</p> <p>Data may be retained by Twilio for quality control purposes, for no more than 61 days.</p>
<p>Individuals in providing a date range for their enquiry could enter personal data i.e. dates of a prison sentence</p>	<p>Members of the public requesting access to the data an organisation holds on them.</p>	<p>Organisations data subject submits request to Customer (copy of their request) Data processors as listed above.</p>	<p>Yes</p> <p>If yes, list the countries the data will be transferred to:</p> <p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails</p>	<p>Other (please specify time period below)</p> <p>If selecting other, please specify the length of time personal data will be retained:</p> <p>The ICO will hold the SAR request for 14 days, so it</p>

			worldwide as may be necessary.	can recover and resend the request in event of service loss or failure. Data may be retained by Twilio for quality control purposes, for no more than 61 days.
--	--	--	--------------------------------	---

1.4 Lawful basis for processing

Guidance notes:

- To process personal data, you **must** have a lawful basis. Select a lawful basis for processing the personal data in your inventory from the drop-down lists below.

Guidance Links: [Lawful basis for processing](#) & [Lawful basis interactive guidance tool](#)

First, select a lawful basis from Article 6 of the UK GDPR.

Article 6(1)(e) - public task

If more than one lawful basis applies to your processing, please list any additional basis here:

Guidance notes:

- If your personal data inventory includes any **special category data**, you **must** identify an additional condition for processing from Article 9 of the UK GDPR.

Guidance link: [Special category data](#)

Next, if applicable, select an additional condition for processing from Article 9 of the UK GDPR:

Article 9(2)(g) - reasons of substantial public interest

If you have selected conditions (b), (h), (i) or (j) above, you also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018. Please select from the following:

Choose an item.

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of the conditions set out in Part 2 of Schedule 1 of the DPA 2018. Please select from the following:

6. Statutory and government purposes

Guidance notes:

- If you are processing **criminal offence data**, you **must** meet one of the 28 conditions for processing criminal offence data set out in paragraphs 1 to 37 Schedule 1 of the DPA 2018.

Guidance Link: [Criminal offence data](#)

Finally, if applicable select an additional condition for processing any criminal offence data:

6. Statutory and government purposes

1.5 Necessity and proportionality

Guidance note:

- You **must** assess whether your plans to process personal data are both necessary and proportionate to you achieving your purpose. You should explain why this is the case below.
- You **must** take steps to minimise the personal data you process; processing only what is adequate, relevant and necessary.
- You **should** think about any personal data you can remove without affecting your objective.
- You **should** consider if there's any opportunity to anonymise or pseudonymise the data you're using.

The SAR digital web service is entirely voluntary and designed to assist both individuals and organisations. Individuals can make SAR requests using alternative methods i.e. letter, e-mail etc if they chose to do so – the use of this service is an option for their convenience.

In using the service the mandatory fields are name, e-mail address (customer), email address (organisation), details of personal data being requested and a date range for the period of coverage being requested.

Research has shown that including these details:

- Reduces the time organisations will spend producing the SAR – therefore giving a better service to the requestors
- Reduce enquiries and complaints to the ICO
- Provide individuals with an increased chance of obtaining what they need in a more timely manner

The data we are requesting is the minimum required to be able to deliver this improved service and the likelihood of sensitive data being entered is low.

The project seeks to further the Commissioners tasks in Article 57 of the UK GDPR. Specifically:

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

And;

(d) promote the awareness of controllers and processors of their obligations under this Regulation

Update 11/10/2023

Metrics on use of the tool so far indicate that approximately 4% of SARs submitted through the service don't have a valid recipient email address. This means some SARs aren't received by the intended organisation as they fail/bounce back. To improve this we're introducing the instant email validation service provided by Data-8. The only data processed by Data-8 to provide this service is the recipient email address (which often doesn't contain any personal data) and we consider this additional processing a necessary and proportionate way of reducing the 4% of failed requests.

Update on 3/11/2023

Metrics indicate that the Data-8 integration will reduce the likelihood of request emails being non-deliverable from about 4% to about 1%. To reduce the manual effort required to check for non-deliverables and contact customers, we're introducing an automated email. The automation will use the same data processors as the existing service (Microsoft and Sendgrid). We consider this additional processing a necessary and proportionate way to provide important alert and advice to customers, negating the need for ICO staff to further process their data.

1.6 Consulting with stakeholders

Guidance notes:

- You **should** consult with relevant stakeholders both internally (for example Cyber Security, Legal Services, IT etc.) and externally to help you identify any risks to your data subjects.
- Briefly outline who you will be consulting with to inform your DPIA.

- Where appropriate you **should** seek the views of your data subjects, or their representatives, on your intended processing. Where this isn't possible, you should explain why below.

This project deliverable has been widely presented and demonstrated (in test form) to stakeholders across the business. These include, live services, ET members, Director of DP advise and complaints, and DDaT. In producing this solution, which will be released in Beta form, we have consulted with organisations in the preceding user research process, and we will be actively capturing feedback from individuals, testers, and organisations as part of the post Go Live assessment.

2. Personal data lifecycle

Guidance Note:

- You **must** provide a systematic description of your processing from the point that personal data is first collected through to its disposal.
- This **must** include the source of the data, how it is obtained, what technology is used to process it, who has access to it, where it is stored and how and when it is disposed of.
- If your plans involve the use of any new technology, for example a new piece of software, you **must** explain how this technology works and outline any 'privacy friendly' features that are available.
- If helpful you can use the headings provided below to help you construct your lifecycle. You can include a flow diagram if this helps your explanation.

Data source and collection:

Customer enters metadata, eg description, dates, type of data, to describe the personal data that the organisation holds about them.

Technology used for the processing:

The service will use existing technology that supports the ICO website to process the information. Key technologies are [REDACTED]

[REDACTED] The file upload feature uses the existing [REDACTED] service, with [REDACTED] providing anti-malware scanning. The email validation component uses a service provided by an existing supplier contracted with the ICO, Data-8. The automated alert and advice email for requests that are non-deliverable uses existing [REDACTED] technologies [REDACTED] and [REDACTED].

Storage location:

All locations are existing. Data collected by the website will be processed and stored in the [REDACTED], which uses [REDACTED] (DP and security documentation exists). Data processed by Sendgrid may be processed on Twilio's network and by its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary (DPIA, SOR and Transfer Risk Assessment existing). Data processed by Data-8 will be processed within [REDACTED] which uses [REDACTED]. The locations of storage and processing will not be changed as a result of this project.

Access controls:

Existing access controls are implemented across all relevant resources ([REDACTED]) using the principle of least privilege and will not be changed by the introduction of this service. [REDACTED] operates an [REDACTED] certified system that includes access controls based on the principle of least privilege. Examples: Access controls for [REDACTED] resources and [REDACTED] additionally require [REDACTED]. Access controls for [REDACTED] additionally require [REDACTED], and [REDACTED]. When processing non-deliverable notifications, [REDACTED] uses [REDACTED] to access [REDACTED].

Data sharing:

Data will be shared with the customer, and the organisation, at the email addresses supplied by the customer, for the purpose of providing the service. Data shared with Data-8 will be for the purpose of checking that the recipient email address is valid. Other data sharing for the purpose of delivering the website and digital services is existing and covered by existing DPIAs and SORs

(ICO website and Azure, Silktide analytics, Cloudflare, Sendgrid) and will not be changed by the introduction of this service.

Disposal:

Subject access requests made through the service, including any uploaded documents, will be retained for 14 days after which they will be deleted. Email validation requests to Data-8 are not stored by Data-8. Alert and advice emails for non-deliverable requests are subject to the same retention schedule for Sendgrid; they are processed in real-time and are not otherwise stored. Other retention and disposal schedules are existing and will not be changed by the introduction of this service.

3. Key UK GDPR principles and requirements

Guidance notes:

- Answering the questions in this section will help you comply with essential data protection requirements.
- You may identify specific actions that are needed and you should add these to your list of DPIA outcomes in section 6.0.

3.1 Purpose & Transparency

Guidance notes:

- In most cases you will need to communicate essential information about your data processing to your data subjects. A privacy notice is the most common way of doing this.
- You **must** review the existing [privacy notice](#) on the ICO website. If your data processing involves the personal data of ICO staff, review our [Staff Privacy Notice](#) on IRIS.

- You need to decide if our existing privacy notices sufficiently cover your plans. If not, you **must** get them updated or you **must** provide your data subjects with a separate, bespoke privacy notice.

Q1. How will you provide your data subjects with information about your data processing?

An update is required to our existing privacy notice/s. This required action has been added to the DPIA outcomes (see section 6.0).

Guidance notes:

- If you identified consent as your lawful basis for processing in section 1.4 you **must** maintain appropriate records of the data subjects consent.

Guidance Link: [Consent](#)

Q2. Are you satisfied you're maintaining appropriate records of data subjects' consent?

N/A - no processing based on data subjects consent

Guidance notes:

- If you identified legitimate interests as your lawful basis for processing in section 1.4 you **should** complete a Legitimate Interests Assessment (LIA). A template LIA is available [here](#).

Guidance Link: [How do we apply legitimate interests in practice?](#)

Q3. If legitimate interests is your lawful basis for processing have you completed a [legitimate interest assessment](#)?

N/A - no processing based on legitimate interests lawful basis

If applicable, please provide a link to your completed assessment.

3.2 Accuracy

Guidance notes:

- All reasonable steps should be taken to ensure personal data is kept accurate and up to date. Steps **must** be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

Q4. Are you satisfied the personal data you're processing is accurate?

Yes

Q5. How will you ensure the personal data remains accurate for the duration of your processing?

All data is provided by the data subject themselves, or their representative (eg family member, friend, solicitor) and the ICO do not amend, update, or review this information at any stage.

The introduction of the email validation check with Data-8 is intended to improve the likelihood of the recipient's email being valid but it remains the responsibility of the customer to enter a valid email address to send their request to.

3.3 Minimisation, Retention & Deletion

Guidance notes:

- You should only collect and hold the minimum amount of personal data you need to fulfil your purpose. Data should be retained for no longer than is needed for that purpose and then deleted without delay.

Q6. Have you done everything you can to minimise the personal data you're processing?

Yes

Q7. How will you ensure the personal data are deleted at the end of the retention period?

This is an established process whereby a retention job runs every day and deletes all records, including any uploaded documents, older than 14 days.

Q8. Will you need to update the ICO [retention and disposal schedule](#)?

Yes

3.4 Security: Confidentiality, integrity and availability

Guidance notes:

- Personal data **must** be processed in a way that ensures it is appropriately secure and protected from unauthorised access, accidental loss, destruction or damage.
- You **must** make sure access to the personal data is limited to the appropriate people and ensure you're confident the processing system being used is secure.

Guidance link: [Security](#)

Q9. Where will the personal data be stored and what measures will you put in place to maintain confidentiality, integrity and availability?

Storage will be in the existing website database. Storage for any uploaded files will use the existing [REDACTED] service within the website subscription. Both are restricted to authorised users and subject to role-based access controls. There are no proposals to change those controls or give access to any additional members of staff.

There are no new storage or web services being used as part of this solution and all existing technologies have been approved elsewhere and subject to their own contracts and DPIA coverage.

We use [REDACTED] to support our email infrastructure and the operation of these services. Any personal information shared with the ICO in the SAR service may be shared with Twilio and this can include the transfer of data to the USA. We have in place Standard Contractual Clauses to safeguard this transfer and data is retained by Twilio for no more than 61 days.

Q10. Have you confirmed there are appropriate access controls to keep the personal data secure?

Yes

Q11. Has the [cyber security team](#) completed a security assessment of your plans?

In progress

Q12. If yes what was the outcome of their assessment?

We are consulting with cyber and will review/implement their recommendations as part of the Go Live process

Q13. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

The Beta will be a soft launch. We have briefed and demonstrated the service to live services and will provide recordings for future reference. We are not introducing a new business service but have consulted with live services for awareness, should they receive any customer contact. The initial service will capture data from the requestor and pass it to the organisation without ICO intervention. Any queries or issues resulting from the Beta (failure or service loss) will be handled by the project team, this is the purpose of the 14 day retention period - we have the ability to support the process, should it be needed.

3.5 Accountability and governance

Guidance notes:

- The accountability principle makes us responsible for demonstrating our compliance with the UK GDPR. We do this by clearly assigning responsibilities for compliance tasks, and by maintaining relevant records relating to our processing activities and decision making.
- Your Information Asset Owner is the risk owner for any residual risk associated with your data processing and **must** sign off this DPIA.

Q14. Is your Information Asset Owner aware of your plans?

Yes

Q15. Will you need to update our article 30 record of processing activities?

Yes

Q16. If you are using a data processor, have you agreed, or will you be agreeing, a written contract with them?

Yes

3.6 Individual Rights

Guidance Note:

- UK GDPR provides a number of rights to data subjects when their personal data is being processed.
- As some rights are not absolute, and only apply in limited circumstances, we may have grounds to refuse a specific request from an individual data subject. But you **must** be sure your new service or process can facilitate the exercise of these rights and it should be technically feasible for us to action a request if required.

Guidance Link: [Individual rights](#)

Q17. Is there a means of providing the data subjects with access to the personal data being processed?

Yes

Q18. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

No

As all data is input by the data subject and sent immediately on submission to the controller the ICO can not edit this. However the data subject can use the service to submit to the controller any clarification, amendment etc.

Records retained by the ICO until our retention period expires will be an accurate reflection of data submitted by the data subject when using the SAR tool and is only retained for a limited period.

Q19. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes

Q20. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes

Q21. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes

Q22. Can we erase the personal data on receipt of a request from the data subject?

Yes

4. Risk assessment

Guidance Note:

- You **must** use the table below to identify and assess risks to individuals. You can add as many rows to the table as you need.
- **Remember:** we have an **Averse** risk appetite towards compliance risks (see our [Risk Management Policy and Appetite Statement](#) for more information).
- You **must** identify measures to reduce the level of risk where possible.
- In the risk description column, you can select from common risks to individuals in the drop-down list provided. Alternatively, you can enter your own risk descriptions if preferred.
- **The drop-down list is not exhaustive**, and you must identify and assess risks within the context of your planned processing.
- Mitigation measures can be existing, i.e. they're already in place and reduce the risk without any further action being needed. Or they're expected i.e. these are additional measures you intend to take before the data processing begins in order to further reduce risk.
- Use the risk scoring criteria in [Appendix 1](#) to score your risks. You **must** score both the impact (I) and probability (P). The expected risk score total is the result of I multiplied by P.
- When considering probability, you should score based on all your mitigation measures having been implemented in order to get an *expected* risk score.

Risk description	Response to Risk	Risk Mitigation	Expected Risk Score		
			Impact	Probability	Total
<i>Example: Access controls are not implemented correctly, and personal</i>	Choose an item.	<i>Existing mitigation: We have checked that the system we intend to procure allows us to</i>	3	1	3 - low

	<i>data is accessible to an unauthorised party.</i>		<i>set access permissions for different users.</i> <i><u>Expected mitigation:</u> We will appoint and train a system administrator who will be responsible for implementing access controls and monitoring access. The system administrator will also audit the system periodically to review access permissions.</i>			
1.	Risk 20: A customer entering their own e-mail address incorrectly could lead to an organisation sending the response back to an unintended recipient (information breach)	Tolerate: this risk is being accepted	This requires an incorrect e-mail address being entered twice by the customer, and the incorrect address being valid in its own right. We use 'check your details' and tell organisations that they are obliged to validate the requestor as part of the process – both of these should catch incorrect e-mail addresses	1	3	3 - low
2.	Risk 21: Cyber threat, ICO e-mails could be copied and used for phishing or as spoof e-mails by bad actors.	Tolerate: this risk is being accepted	We have accepted that this could happen today. We stress to organisations that they must validate the requestor. We will refer to cyber for further advise	1	4	4- low
3.	Choose an item.		Existing mitigation:	3	1	3 - low

	<p>A customer could enter the organisation email address incorrectly, resulting in non-delivery of a request or a request going to a third party</p>	<p>Treat: this risk is being reduced by management action such as implementing controls or tackling the cause</p> <p>Tolerate: the remaining residual risk (addresses where validity cannot be determined) is accepted.</p>	<p>A pattern validation control exists in the service, to ensure that email addresses conform to a known pattern, eg organisation@domain.com</p> <p>Expected mitigation: An 'instant email validation' service provided by Data-8 will help ensure that emails are additionally addressed to an address of a live mail server that accepts email to the full email address, and where responses are 'invalid' the customer will be unable to send their request.</p> <p>Residual risk (low likelihood): Where it's not possible to determine the validity of an email address, a requester will be able to submit their request. Email bounces will be monitored and an automated service will alert and advise customers.</p>			
4.	<p>A 3rd party could try and access a data subjects information unlawfully by making a inauthentic 3rd party request.</p>	<p>Transfer: this risk is being passed on to someone else</p>	<p>Existing mitigation: We have made it clear in the correspondence with organisations that we have not validated that the 3rd</p>	3	1	3 - low

			<p>party has the right to make a request on behalf of the data subject and they must follow their own procedures for validating this.</p> <p>We have provided the functionality for people to provide evidence of their right to act on someone else's behalf.</p>			
--	--	--	--	--	--	--

5. Consult the DPO

Guidance Note:

- Once you have completed all of the sections above you **must** submit your DPIA for consideration by the DPIA Forum who will provide you with recommendations on behalf of our Data Protection Officer (DPO). The process to follow is [here](#).
- Any recommendations from the DPOs team will be recorded below and your DPIA will then be returned to you. You **must** then record your response to each recommendation, and then proceed with completing the rest of this template.

	Recommendation	Date and project stage	Project Team Response
1.	You have listed Sendgrid as a data processor in section 1.1 but not identified other data processors associated with the website. These are however mentioned elsewhere in your assessment (Microsoft, Cloudflare etc.). Some clarification is required about the role of any data processors involved here to ensure the scope of this DPIA is clearly defined. Your response in section 3 to Q16 indicates no data processors are involved, so you need to clarify this contradiction. Suggest discussing when IM&C	07/07/2023	<p>Accept</p> <p>Any comments: Q16 has been updated along with section 1.1.</p> <p>The SAR online solution is using existing website infrastructure, currently in use and covered by DPIA's and security arrangements elsewhere.</p> <p>If rejecting DPO recommendations explain why:</p>

	Service and Project Team meet on 17/7/23.		
2.	<p>There appears to be additional categories of personal data being processed that aren't included in your data inventory at 1.3. You should also include:</p> <ul style="list-style-type: none"> Name and contact details of the controller. Names can be expected as part of the email address input by requester and/or within the body of the request. E.g. My medical record held by Dr C" You also need to include the personal data individuals will include within the body of the request. For example I've been receiving treatment for cancer by Doctor C and want to request a copy of my medical record. Or I was a prisoner at HMP serving 5 years for robbery and want a copy of my file. You should expect to receive both special category data and criminal offence data via this tool. You need to identify additional 	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>Data of receiving individual at the organisation has been added to section 1.3.</p> <p>Section 1.4 Lawful basis has been updated and updated privacy policy need made in section 6.</p> <p>If rejecting DPO recommendations explain why:</p>

	lawful basis' for processing these data categories, and consider any risks resulting from this processing. Suggest discussing when IM&C Service and Project Team meet on 17/7/23.		
3.	As far as we're aware there isn't any intention to have age verification on the ICO website to restrict access the SAR generator. We recommend you work on the assumption that the SAR tool could therefore be used by children to make access requests, and the ICO may therefore process childrens data as a result. Consideration should be given to ICO guidance on processing the data of children and you need to factor this into your plans. Suggest discussing when IM&C Service and Project Team meet on 17/7/23.	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>Children have a right to submit a SAR on their own behalf and therefore we would not prevent a child from using this service - however, we think it is unlikely it will be used by many children. Our lawful basis for processing children's data remains the same - public task - as it is related to our need to support people (incl. children) to exercise their rights. Our style guide (which the tool is following) ensures we use language that is plain and accessible and should be readable by someone with a key stage 2 reading age. This is the same for our privacy notice - it should be accessible and readable by anyone so we shouldn't need a special "children's" PN. The processing is unlikely to result in high risk to children's rights and freedoms. We are not covered by the age appropriate design code. We will not be testing the product with children the level of data processing we would have to do to recruit children for testing and then test with them is disproportionate to the risks to children using the service. However, all our online services are designed to accessible and usable by anyone with access to a computer or mobile device.</p>

			If rejecting DPO recommendations explain why:
4.	We recommend removing the sentence " <i>Organisation receiving the request, who already hold the data subjects data</i> " from your data inventory as this isn't always going to be true and shouldn't be assumed. Individuals will often make speculative access requests to organisations who they suspect might hold data about them, but they don't. It is also possible the requester will include additional personal data previously not processed by the organisation within their access request. You should consider if removing this assumption presents any new risks to your data subjects.	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>Updated section 1.3 to reflect that an organisation approached may not actually hold individuals data, and included data processors as a recipient.</p> <p>We do not think that this presents any new risk.</p> <p>If rejecting DPO recommendations explain why:</p>
5.	Section 1.5 – This is currently very limited and some further justification is required here to support the public task basis for processing this data, and satisfy necessity and proportionality requirements. Some of what you've mentioned in 1.2 can be expanded upon. For example consider justifications such as reducing volume of complaints to ICO,	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>Sections 1.3 and 1.5 have been updated.</p> <p>If rejecting DPO recommendations explain why:</p>

	<p>promoting individuals rights and helping them to exercise these, educating controllers on their responsibilities and reducing burdens on business' from poorly formulated SARs.</p> <p>You should also link back to the categories of data being processed and consider opportunities, if any, to minimise the data processed and still achieve your purpose.</p> <p>It was also noted that the statement "<i>the only mandatory fields are name and e-mail address....all other information on the web service is optional</i>" might not be accurate, as a number of other elements of the tool currently indicate via * they are mandatory. Please double check this and update the DPIA accordingly.</p> <p>Suggest discussing when IM&C Service and Project Team meet on 17/7/23.</p>		
6.	<p>If you haven't already, we'd recommend you consider the scenario where an individual uses the tool to submit an access request on behalf of somebody else. It needs to be made clear to the</p>	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>The online solution accommodates 'on behalf of' requests and the guidance sent to an organisation makes clear</p>


	<p>controller receiving the request that the ICO has taken no steps to verify authorisation to act, and they should do so.</p> <p>Similarly this will presumably be the case for regular requests, we'll be asking the controller to take steps to verify the requesters identity?</p> <p>There needs to generally be more explanation in this DPIA about what information will be provided to both data subjects using the tool and controllers receiving the request as a means of mitigating risks. Suggest discussing when IM&C Service and Project Team meet on 17/7/23.</p>		<p>that the ICO has not validated the request in any way, and that they are required to carry out their normal validation checks. In the email issued to the Organisation it clearly states, "You must be satisfied that you know the identity of the requestor, and that the data you hold relates to them. You may need to contact the requestor to check their identity."</p> <p>@Steve We are actually updating the wording to include something along the lines of "The ICO has forwarded this request on behalf of the requestor and has not taken steps to validate their identity" but want to get Hannah's input on that when she returns to work on 24/07.</p> <p>If rejecting DPO recommendations explain why:</p>
7.	<p>Personal data lifecycle / Response to Q9 in section 3 - it's not completely clear where personal data will be stored and there is indication copies may be held in multiple locations. It's important there is developed understanding of all places this data might be duplicated so the same retention rules can be applied. Without this there is a risk we retain data longer than required (14 days) and risk misinforming data subjects.</p>	07/07/2023	<p>Accept</p> <p>Any comments: Section 3 Q9 has been updated, as there are no new web services being introduced we are utilising existing time-served retention practices.</p> <p>@Steve I have clarified that Sendgrid will store minimal random content samples for 61 days, as is the case with our other online web form services – such as making a complaint or data protection fee. The following extract is taken from our current website privacy notice, so am proposing to include it in S3. Q9:</p>

			<p>“We use Twilio Sendgrid to support our email infrastructure and the operation of these services. Any personal information you share with us may be shared with Twilio and this can include the transfer of data to the USA. We have in place Standard Contractual Clauses to safeguard this transfer and data is retained by Twilio for no more than 61 days”.</p> <p>If rejecting DPO recommendations explain why:</p>
8.	<p>Access Controls –</p> <p>Access is described as limited to authorised users: website editors in comms, Tony Francis, Greer Schick and Hannah Smith in DDat. Please expand on how these accounts are managed. As per recommendation 7 if data is being held in multiple locations you should consider whether access to this data is actually wider than this pool of individuals and consider any risks.</p>	07/07/2023	<p>Accept</p> <p>Any comments: We are not introducing any new technologies and will continue with existing access practices used elsewhere, and approved, in the the business.</p> <p>If rejecting DPO recommendations explain why:</p>
9.	<p>Section 3</p> <p>Q2. - We’re unable to identify any data processing that relies on an individuals consent. Your response here should be N/A so it has been changed.</p>	07/07/2023	<p>Accept</p> <p>Any comments:</p> <p>If rejecting DPO recommendations explain why:</p>

	<p>Q8. – an update to the retention schedule will be required and response should be Yes so this has been changed. Action added to section 6.</p> <p>Q15. - An update to the ROPA will be needed. Response changed to Yes and added as an action in section 6.</p> <p>Q16. - See recommendation 1, clarification required on data processors.</p> <p>Q18, 19 & 20. – clarification required as to why these questions have been answered no as these are fundamental GDPR rights. Suggest discussing when IM&C Service and Project Team meet on 17/7/23.</p>		<p>The part that the ICO plays in the process is to forward the SAR request to external organisations. These questions have been answered on the basis that once we have delivered the mail we cannot then retrieve it, or amend it with the organisation is question. We should review these q's and our understanding of whats being asked.</p> <p>SJ 18/07/2023 – explanation for no response added to Q18. Q19 and Q20 reviewed and response changed to Yes.</p>
<p>10.</p>	<p>Risk Assessment – generally the risk assessment is very limited and will need to be reconsidered once the above recommendations have been addressed.</p>	<p>07/07/2023</p>	<p>Reject</p> <p>Any comments:</p> <p>If rejecting DPO recommendations explain why:</p>

	<p>A few additional risks (not exclusive list) we suggest you consider are:</p> <ul style="list-style-type: none"> • 1. the risk of the SAR tool failing, and an individual being unable to exercise rights. E.g. they think they've made a SAR but it's not been submitted correctly. Consider what controls are in place to alert us to send failures, bounce backs etc. and how do we intend to alert individuals if an email fails. • 2. Security controls are inadequate for protecting personal data resulting in a loss of confidentiality, integrity, availability. • 3. Risk of an individual sending their SAR request to wrong org – what validation measures / warnings are in place to prevent this. • 4. Individuals are unable to exercise their rights in relation to our processing (unless responses to Q18, 19 & 20 change). 		<p>The project has a formal Risk register which is fluid and will be signed off by the project sponsor, and any caveats completed before Go live.</p> <p>All the risks mentioned opposite are listed on the register, with the exception of:</p> <p>4. See above comments in point 9 ref these q's</p> <p>5. This has been addressed in point 3 above</p> <p>6. Addressed in point 7 above</p> <p>Key DPIA risks in project risk register include:</p> <p>7. In creating a tool, with contact data provided by the ICO, with an inferred responsibility for accuracy and delivery to an organisation, we risk legal challenge in the event of an error. If we direct a request to an inaccurate address, this could lead to the disclosure of personal data to a 3rd party.</p> <p>15. Due to the generator tool capturing data from requestors completing a SAR request, we are processing (potentially sensitive) person information, which could run risks to individuals if redirected or used incorrectly.</p> <p>16. The MMP solution tool hosts the routing of SAR requests via e-mail to the intended recipient. The ICO could become responsible for any delay in delivering the SAR request, as any 'bounce back' failure messages, from organisations, are not sent back to the originator - in the</p>
--	---	--	--

	<ul style="list-style-type: none"> • 5. Lack of age verification and risks associated with processing childrens data. • 6. Data retained for longer than is necessary 		<p>event of an incorrect e-mail being entered by the customer.</p> <p>19. The organisation receiving the request via the tool doesn't recognise it as a SAR or doesn't trust that it's legitimate, leading to the customer not receiving a response.</p> <p>20. The customer entering an incorrect email address as their own email address may lead to the organisation sending the response to an email address that doesn't exist, or sending it to the wrong recipient (information breach).</p> <p>21. Cyber Threat, partially linked to Risk 20. In sending ICO branded e-mails to requestors and organisations, as part of our intermediary role for SAR requests, There is a risk that these will be copied by bad actors and issued as part of phishing campaigns, spoof e-mails or other purposes to illegally capture or intercept personal data. Does an ICO branded SAR request being received by an organisation give the impression that the ICO have validated the requestor? Could this assumption lead to some organisations releasing personal data without carrying out security validations when receiving these requests?</p> <p>23. An individual could add personal special category data or criminal record data to the online solution. This could be a risk to individuals if redirected or used incorrectly (related to 15)</p>
--	---	--	---

			<p>Attached is a link to project risk register with risk scores and mitigations in place for each of these risks –</p> <p> Project%20RAID%20og%20-%20SAR%20</p>
--	--	--	--

6. Integrate the DPIA outcomes

Guidance Note:

- Completing sections 1 to 5 of your DPIA will have helped you identify a number of key actions that you now **must** take to meet UK GDPR requirements and minimise risks to your data subjects. For example, you may now need to draft a privacy notice for your data subjects; or you could have risk mitigations that you need to go and implement.
- You **should** also consider whether any additional actions are required as a result of any recommendations you received from the DPOs team.
- Use the table below to list the actions you need to take and track your progress with implementation. Most actions will typically need to be completed **before** you can start your processing.

Action	Date for completion	Responsibility for Action	Completed Date
Review/update of privacy policy	14 th July 23	SAT Tool project team	01/08/2023 - SJ
Review of cyber feedback	14 th July 23	Greer Schick/Graham Rumens	31/7/23 - GS
Update retention Schedule	ASAP	Greer Schick/Graham Rumens/ IM&C Service	07/08/2023 - SJ
Update ROPA	ASAP	Greer Schick/Graham Rumens/ IM&C Service	07/08/2023 - SJ

7. Expected residual risk and sign off by the IAO

Guidance note:

- Summarise the expected residual risk below for the benefit of your IAO. This is any remaining risk **after** you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank.
- If the expected residual risk remains high (i.e. red on the traffic light scoring in the Appendix) then you **must** consult the ICO as the regulator by following the process used by external organisations.

7.1 IAO sign off

Guidance Note:

- Your IAO owns the risks associated with your processing and they have final sign off on your plans. You **must** get your IAO to review the expected residual risk and confirm their acceptance of this risk before you proceed.
- Once your DPIA has been signed off it is complete. You should review it periodically or when there are any changes to your data processing.

IAO (name and role)	Date of sign off
Suzanne Gordon, Director of Public Advice and DP Complaints	19 July 2023
Suzanne Gordon, Director of Public Advice and DP Complaints	19 October 2023
Suzanne Gordon, Director of Public Advice and DP Complaints	21 November 2023
Suzanne Gordon, Director of Public Advice and DP Complaints	7 December 2023
Suzanne Gordon, Director of Public Advice and DP Complaints	19 January 2024

8. DPIA change history

Guidance note:

- You should track all significant changes to your DPIA by updating the table below.

Version	Date	Author	Change description
V0.1	30/6/23	Andy Grocott	First Draft
V0.1	4 th July 23	Graham Rumens	Draft and form completion
V0.1	07/07/2023	Steven Johnston	DPIA Forum Recommendations added to section 5. Actions updated in section 6.
V0.1	18/07/2023	Steven Johnston	Update to 1.5, 3.0 (Q18,19 & 20) made to support project team.
V1.0	19/07/2023	Suzanne Gordon	IAO Sign Off and first release
V1.1	07/08/2023	Steven Johnston	Update to section 6 – actions completed.
V1.2	14/9/23	Graham Rumens	Added optional capture of address data to Personal Data Inventory section 1.3
V1.2	19/9/23	Greer Schick	Added description of file upload functionality. Updated section 1.3 to reflect section 5 recommendation 4. Updated section 1.3 to clarify overseas data transfer due to use of Sendgrid.
V1.3	11/10/23	Greer Schick	Updated to reflect integration with Data-8 instant email validation integration.
V2.0	19/10/23	Suzanne Gordon	IAO Sign Off for addition of Data-8 email validation feature
V2.1	3/11/23	Greer Schick	Updated to reflect addition of automated alert and advice emails for non-deliverable emails
V3.0	21/11/23	Suzanne Gordon	IAO Sign Off for addition of automated alert and advice emails feature
V3.1	22/11/23	Greer Schick	Updated to Section 1.2 and Section 2 to reflect addition of anti-malware scanning feature on uploaded documents.
V3.2	7/12/23	Suzanne Gordon	IAO Sign Off for addition of anti-malware scanning feature.
V3.3	18/01/2024	Hannah Smith	Updates to 1.2, 1.3, Section 3 and Section 4 to account for iteration of service to improve SARs by third parties.

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (e.g. does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability and is represented by a RAG rating.

Probability \ Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted, and immediate action is required to reduce, avoid or transfer the risk.

SAR Tool Project



Show & Tell – 26 September 2023

Purpose of a show and tell

1. Opportunity for the Scrum Team to showcase the work they have been doing.
2. Opportunity for stakeholders to ask questions and provide feedback on the discovery work of the Scrum Team up until the end of March 2023.
3. Communication - encourages transparency and lets teams we are working with know what we are up to and keeps teams connected.

It is not an opportunity to discuss solutions and it is not a Project Board.



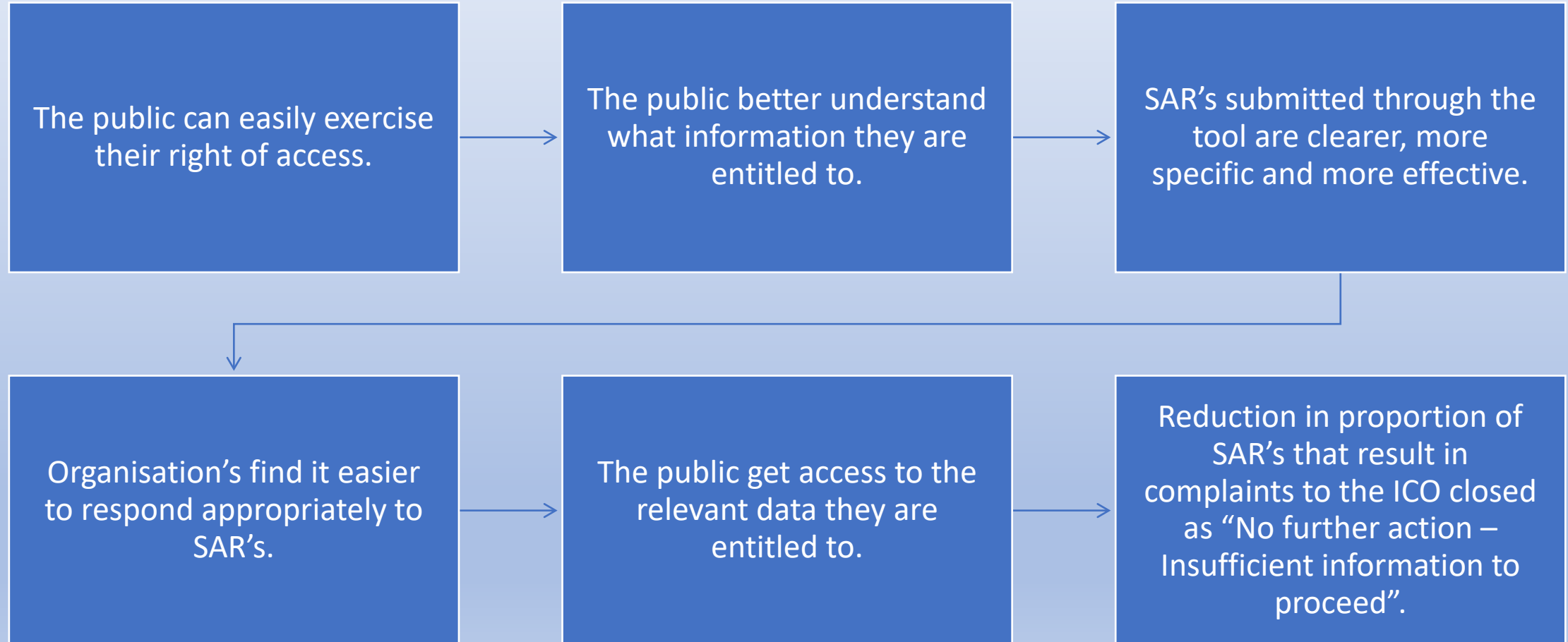


ICO25 Project mandate for SAR

Why are we doing it? How does it fit with our strategic objectives?

Individuals have an important legal right to access information held on them by businesses, through making SARs. But we believe that SARs going in to businesses are often formulated badly, meaning that requests are unclear or unnecessarily wide in scope. This slows down the process of the individual accessing the information they need, and gives businesses an extra administrative burden of trying to understand and meet the request. We think this is because individuals don't understand how to make a request in the best way, which may stop individuals exercising their right to make a request. The aim of this work is to help individuals understand their rights and how best to make an SAR, thereby supporting individuals, reducing the burden of poorly formulated SARs on businesses, and reducing complaints to the ICO.

SAR Project objectives



Sprint 12 Objectives



Manage and Monitor MMP service in Production



Raise change request and draft Data8 Contract variation notice



Manage bounce backs and refine bounce backs solution design



Develop and test solution for email validation



Develop mock ups for user Identity verification



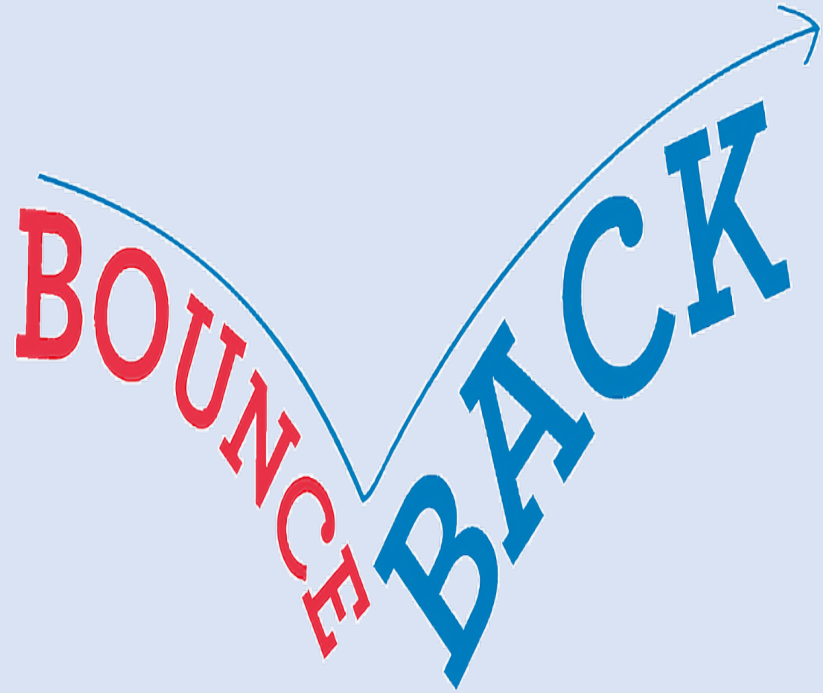
Develop and test template to support Welsh language service



Manage and monitoring service in Production

- **3281** submissions received through the service since it was launched on 02 August
- Time to complete the service remains constant at around 3 minutes 06 seconds and completion rate is steady at 29%.
- User satisfaction remains high with survey questions on satisfaction, usability and clarity all scoring between 4.26 and 4.84 out of 5.
- Users are expressing an understanding of their rights and the law.
- Organisations overall satisfaction is constant at 3.15 and understanding of what is being requested of them has climbed slightly to 3.79
- Continue to manually manage bounce backs, with 180 bounce backs processed to date.

Bounce backs



- 180 bounce backs to date (5%).
- Being managed by Project and PADPCS, but resource intensive.
- Analysis of bounce backs shows two thirds are “invalid” and will be resolved with Data8 email validation solution.
- Remainder (1.8% of submissions) will be “bounced back” to user in new solution being refined.

Email validation (as-is)

Pattern validation

Organisation email address *

Usually found in the organisation's privacy notice

Enter an email address in the correct format, like name@example.com

helpdeskatbarclays.co.uk

Incorrect, and not allowed

- ✓ Checks that address conform to standard pattern
- × Doesn't check that the domain exists
- × Doesn't check that the domain is receiving emails

Organisation email address *

Usually found in the organisation's privacy notice

helpdesk@barclays.co.uk

Incorrect, but
allowed

Email validation (to be)

Add: MX, Server, and Address validation

Organisation email address *

Usually found in the organisation's privacy notice

The email address is not valid. Check the organisation's website and try again

helpdesk@barclays.co.uk

Incorrect, and not allowed

- ✓ Checks that address conform to standard pattern
- ✓ Check the domain exists and is set up to receive emails
- ✓ Checks that at least one of the advertised mail servers is live
- ✓ Validates that the mail server accepts mail for the full email address

Add: Suggestions

Organisation email address *

Usually found in the organisation's privacy notice

The email address is not valid. Use greer_schick@hotmail.com instead?

greer_schick@hotmail.com

Incorrect, suggestion given



Email validation improvement (but not a silver bullet)

- ✓ Checks that address conform to standard pattern
- ✓ Check the domain exists and is set up to receive emails
- ✓ Checks that at least one of the advertised mail servers is live
- ✓ Validates that the mail server accepts mail for the full email address

Responses

Inconclusive }

CatchAll } customer will be allowed to continue

GreyListed }

Identity document upload

Refresher

- Analysed survey feedback from orgs
 - Many orgs didn't trust the request until they had contacted the requester for ID.
 - Lack of IDs was one of the top five reasons for orgs being unsatisfied with the service.
 - It was also one of the most common reasons for orgs saying the receiving SARs via the service was the same or sometimes harder to action than usual SARs.
 - Over 40% of people said their next steps were to validate ID*
- Desk based research
 - Looked at organisations who said it was the same or harder to action to see how they currently validate ID
 - Held a workshop to decide the design features and discuss risks and opportunities.



Identity document upload

This sprint:

- Created mock up: [Make a subject access request | ICO](#)



Identity document upload

This sprint:

- Created mock up: [Make a subject access request | ICO](#)
- Reviewed as a team
- Determined success measures*

Next sprint (and one after):

- Adjust security settings



Plan for Sprint 13

- **Welsh language service:** build service, update EQIA, go live
- **Email validation:** Complete build and testing, finalise CVN, update DPIA, SoR
- Iterative development: Go live for **date field validation fix**
- **Data dashboard:** gather requirements
- **ID documents upload:** refine user journey to incl virus scanning

Questions





Show & Tell Presentation End

SAR Tool Project



Show & Tell – 24 October 2023

Purpose of a show and tell

1. Opportunity for the Scrum Team to showcase the work they have been doing.
2. Opportunity for stakeholders to ask questions and provide feedback on the discovery work of the Scrum Team up until the end of March 2023.
3. Communication - encourages transparency and lets teams we are working with know what we are up to and keeps teams connected.

It is not an opportunity to discuss solutions and it is not a Project Board.



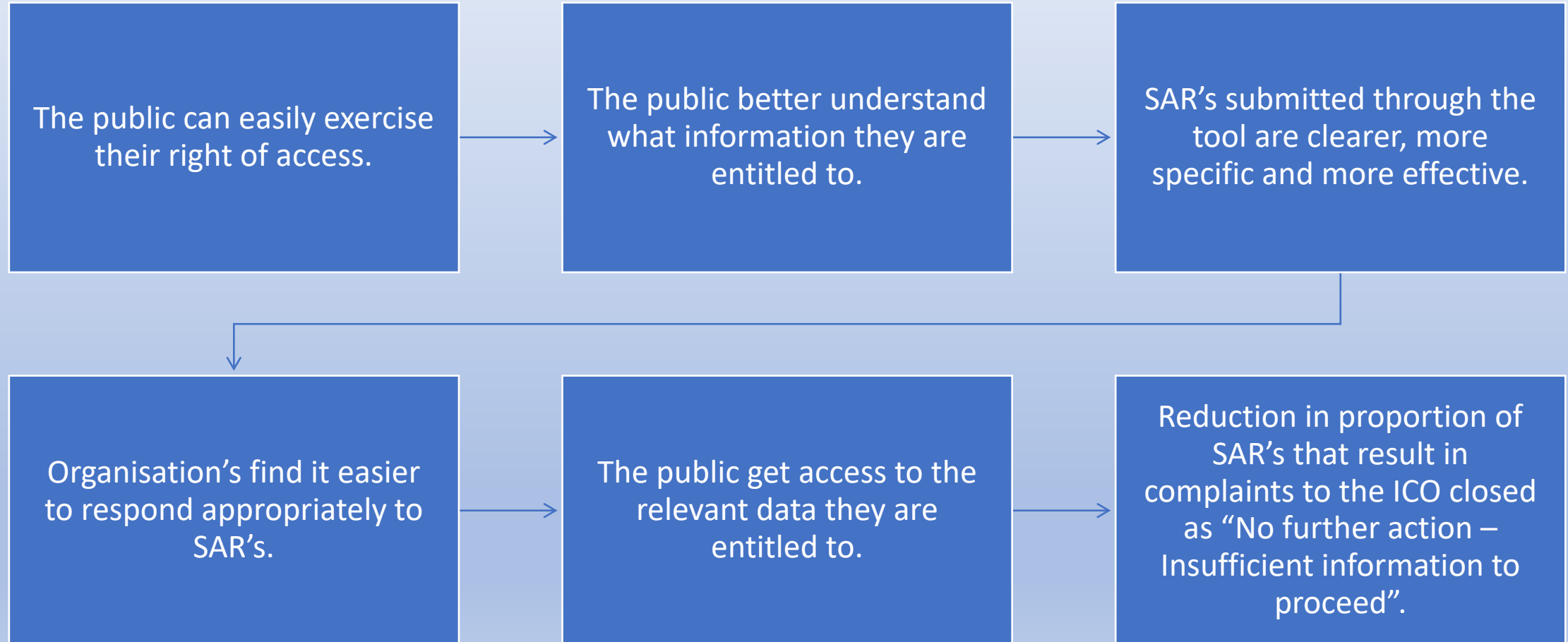


ICO25 Project mandate for SAR

Why are we doing it? How does it fit with our strategic objectives?

Individuals have an important legal right to access information held on them by businesses, through making SARs. But we believe that SARs going in to businesses are often formulated badly, meaning that requests are unclear or unnecessarily wide in scope. This slows down the process of the individual accessing the information they need, and gives businesses an extra administrative burden of trying to understand and meet the request. We think this is because individuals don't understand how to make a request in the best way, which may stop individuals exercising their right to make a request. The aim of this work is to help individuals understand their rights and how best to make an SAR, thereby supporting individuals, reducing the burden of poorly formulated SARs on businesses, and reducing complaints to the ICO.

SAR Project objectives



Focus of Sprints 13 & 14



Manage and Monitor MMP service in Production



Deliver Welsh version of service into Production



Refine and test solution for email validation



Draft updated guidance for users



Refine process for identity verification of users



Define and develop a process allowing for SAR requests to be made on behalf of another user



Manage and monitoring service in Production

- 5411 submissions received through the service since it was launched on 02 August
- Time to complete the service stands at around 3 minutes 49 seconds and completion rate is slightly up to 30%.
- User satisfaction remains high with survey questions on satisfaction, usability and clarity all scoring between 4.17 and 4.79 out of 5.
- Users are expressing an understanding of their rights and the law with scores increasing to 83.
- Organisations overall satisfaction is constant at 3.04 and understanding of what is being requested of them levelled off at 3.77

Welsh language version

The screenshot shows the Welsh language version of the ICO website. The header features the ICO logo and the tagline "Mae'r ICO yn bodoli i'ch grymuso chi drwy gyfrwng gwybodaeth." Below the header is a navigation menu with options: "Hafan", "I'r cyhoedd", "I sefydliadau", "Gwneud cwyn", "Camau rydym wedi'u cymryd", and "Am yr ICO". The main content area is titled "Gwnewch eich cais testun am weld gwybodaeth" (Make your text request to see information) and includes a "Rhannu" (Share) button. Under the heading "Am y sefydliad" (About the organization), there are two sections: "Enw'r sefydliad" (Organization name) with a text input field and "Cyfeiriad ebost y sefydliad" (Organization email address) with a text input field. Both sections include instructions and a "Rhowch" (Provide) link.

ico.
Swyddfa'r Comisiynydd Gwybodaeth

Mae'r ICO yn bodoli i'ch grymuso chi drwy gyfrwng gwybodaeth.

Hafan I'r cyhoedd I sefydliadau Gwneud cwyn Camau rydym wedi'u cymryd Am yr ICO

I'r cyhoedd / Gwneud cais testun am weld gwybodaeth / Subject access request service CY

Gwnewch eich cais testun am weld gwybodaeth

Rhannu 

Am y sefydliad

Enw'r sefydliad
Y sefydliad rydych chi'n gwneud eich cais iddo, e.e. ABC Cyf
[Rhowch enw'r sefydliad](#)

Cyfeiriad ebost y sefydliad
Sydd i'w gael fel arfer yn hysbysiad preifatrwydd y sefydliad
[Rhowch gyfeiriad ebost y sefydliad](#)

Welsh service now live to the public

Email validation



Aim: Make it easier for customers to enter a correct organisation email, reduce non-deliverables

- DPIA completed
- SoR completed
- This feature has been deployed to Production environment
- Not yet live to the public due to delays with contract variation

Organisation email address

Usually found in the organisation's privacy notice

Enter an email address in the correct format, like name@example.com

firstname.lastname.company.com

Guidance for users



Aim: Improve users' understanding of the process before, during and after a request.

Actions:

- Redrafted guidance and mocked up new structure
- Consulted with PADPCS
- Next steps: GGB

User identity verification

**IDENTITY
VERIFICATION**



Aim: Provide all the information an organisation need so that it is easier and quicker for them to action the request.

Actions:

- Desk based research
- Refinement
- Mock ups

- Next steps: Document upload virus checker

3rd party requests



Third
Party
Solution

Aim: Make the service as easy to use for third party requesters (and orgs receiving those requests) as 1st party requesters

Actions:

- Desk based research
- Refinement
- Mock ups
- Next steps: Document upload virus checker

Plan for Sprint 15

- **Email validation:** Get CVN signed off by Commercial Legal and deliver solution into Production for both English and Welsh versions
- **Comms:** Get comms to organisations signed off, arrange for inclusion in next newsletter and test pro-active email to all organisations using one sector to pilot.
- **Bouncebacks / non-deliverables:** Continue to develop automated solution for receiving, sorting and sending alert and advice emails to customers.
- **Data dashboard:** submit request to TDA for approval; develop and test solution.
- **ID documents upload:** Further refine virus checking solution
- **User Research:** Issuing follow up surveys to service users
- **3rd Party Requests:** Develop and test solution

Questions



Risk:
retention
and excess
data

Success: requester is able to upload documents
The requester can upload documents to the SAR service
The requester can upload documents to the SAR service
The requester can upload documents to the SAR service
The requester can upload documents to the SAR service

Quality assurance

As an organisation receiving a SAR via the ICO's service, I want a form of ID and a proof of address attached to the email when it arrives in my inbox so that I can quickly verify the ID and action the SAR



As a requester I want to be able to provide proof of ID and address easily so that doing so does not negatively impact my experience using the SAR service



As a requester I want to be able to take photos of my ID and proof of address whilst using the service so that it is quicker and automatically uploads it for me

As a requester with no proof of address and/or photo ID or who is unable to upload documents, I want to be able to use the ICO's SAR service so that I am not digitally excluded



As the ICO, we want it to be clear that asking for ID in the service is to help orgs and requesters and is not a reflection on our policy position so that people continue follow their own processes and we do not increase the number of complaints to us about ID verification



Upload options at
bottom, non-
mandatory.

Upload options and
about me section moved
to top of form

Make uploads mandatory
unless someone specifies
that they are unable to
provide them

Verification

As a medium sized LA **validating ID** can be time consuming because requests dont come from email we can validate or with ID attached (M)

As a bank, we have a challenge with **verifying the identity** of a requestor [when requests don't arrive via our portal or phone] -- it takes time and can frustrate the customer (H)

As a small GP surgery, it is harder to **validate ID** where a person doesn't have photo ID (eg refugees) so we use other information such as last prescription (L)

As a medium sized LA, **third party requests from parents** and family members can make it complex and time consuming to respond to a request as we have to ensure they have the legal right to make the request (M)

As a very small LA, I struggle to get people to **provide me with their ID** for validation as they don't want to send it to me - i need a way for them to upload it (M)

As a large government organisation, if requests don't come via the portal we often have to go back to get **validation of ID** (L)

As a bank, we will **respond to requests that are probably vexatious** because it can be easier and less time consuming that the complaint we may get from the requester (L)