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	Draft
Version Number	v0.1
Release Date	
Approver (if applicable)	
Review Date	
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:	Director of Public Advice and DP Complaints
Controller(s):	ICO
Data processor(s):	Sendgrid, Cloudflare, Microsoft (existing technologies currently in use)

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 competed the service (link to staging copy attached - **https://staging.ico.org.uk/for-the-public/make-a-subject-access-request/)** 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 Orgnaisation email address the user specified in the service, again with guidance explaining the organisations responsibilities in handling the SAR.

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, and data processors as listed above.	No If yes, list the countries the data will be transferred to:	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. The Organisation receiving the request, who may already hold the data subjects data, will have their own retention schedule.
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 ornaisation holds on them.	Organisations data subject submits request to, and data processors as listed above.	No If yes, list the countries the data will be transferred to:	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. The Organisation receiving the request, who may already hold the data subjects data, will have their own retention schedule.

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).	Members of the public requesting access to the data an ornaisation holds on them.	Organisations data subject submits request to, and data processors as listed above.	No If yes, list the countries the data will be transferred to:	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. The Organisation receiving the request, who may already hold the data subjects data, will have their own retention schedule.
Contact details (contained within the e-mail address) of an identifiable indivdual at the receiving organisation	Named individuals at recipient organisation, identifiable by e-mail address format	Organisations data subject submits request to, and data processors as listed above.	No	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. The Organisation receiving the request, who may already hold the data subjects data,

				will have their own retention schedule.
An individual making a request could provide personal data which forms part of Special Category or Criminal Offence data	Members of the public requesting access to the data an organisation holds on them.	Organisations data subject submits request to, and data processors as listed above.	No	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. The Organisation receiving the request, who may already hold the data subjects data, will have their own retention schedule.
Personal data could be included in the "details of the personal information being requested" – although this is not requested	Members of the public requesting access to the data an organisation holds on them.	Organisations data subject submits request to, and data processors as listed above.	No	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. The Organisation receiving the request, who may already hold the data subjects data, will have their own retention schedule.

Individuals in providing a date range for their enquiry could enter personal data i.e. dates of a prison sentence	Members of the public requesting access to the data an organisation holds on them.	Organisations data subject submits request to, and data processors as listed above.	No	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. The Organisation receiving the request, who may already hold the data subjects data, will have their own retention schedule.

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 convienience.

In using the service the mandatory fields are name, e-mail address, details of personal data being requested and a date range for the period of coverage being requested. In the examples of data that should be entered in 'details of data being requested' we show that we are looking for meta data and not personal details.

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

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 aseessment.

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 Cloudflare WAF and DDoS mitigation service, Azure app service, Umbraco web application, Azure SQL database, and Sendgrid SMTP email relay. There will be no new technology introduced for this project.

Storage location:
All locations are existing. Data collected by the website will be processed and stored in the ICO's Digital Services subscription, which uses Microsoft Azure UK South and UK West data centres (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). 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 (Umbraco Content Management System, Azure resources, Sendgrid) using the principle of least privilege and will not be changed by the introduction of this service. Examples: Access controls for Azure resources and Sendgrid additionally require

multi-factor authentication. Access controls for Umbraco additionally require username and password, and installation of site-to-site VPN with certificates.

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. 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 will be retained for 14 days after which they will be deleted. 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, the ICO do not amend, update, or review this information at any stage.

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 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. This is restricted to authorised users and subject to rules 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 Twilio Sendgrid 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
Example: *Access controls are not implemented correctly, and personal*	Choose an item.	*Existing mitigation: We have checked that the system we intend to procure allows us to*	3	1	3 - low

data is accessible to an unauthorised party.			*set access permissions for different users.* *<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.*			
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 you 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 orgnaisations that they must validate the requestor. We will refer to cyber for further advise	**1**	**4**	**4- low**

3.	**Choose an item.**	**Choose an item.**	Existing mitigation: Expected mitigation:	**Choose an item.**	**Choose an item.**	**Choose an item.**
4.	**Choose an item.**	**Choose an item.**	Existing mitigation: Expected mitigation:	**Choose an item.**	**Choose an item.**	**Choose an item.**
5.	**Choose an item.**	**Choose an item.**	Existing mitigation: Expected mitigation:	**Choose an item.**	**Choose an item.**	**Choose an item.**

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	**Accept** Any comments: Q16 has been updated along with section 1.1. The SAR online solution is using existing website infrastructure, currently in use and covered by DPIA's and security arrangements elsewhere. If rejecting DPO recommendations explain why:

	Service and Project Team meet on 17/7/23.		
2.	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: • 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 catgegory data and criminal offence data via this tool. You need to identify additional	07/07/2023	**Accept** Any comments: Data of receiving individual at the organisation has been added to section 1.3. Section 1.4 Lawful basis has been updated and updated privacy policy need made in section 6. If rejecting DPO recommendations explain why:

	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	**Accept** Any comments: 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.

			If rejecting DPO recommendations explain why:
4.	We recommend removing the sentence *"Organisation receiving the request, who already hold the data subjects data"* 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	**Accept** Any comments: Updated section 1.3 to reflect that an organisation approached may not actually hold individuals data, and included data processors as a recipient. We do not think that this presents any new risk. If rejecting DPO recommendations explain why:
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	**Accept** Any comments: Sections 1.3 and 1.5 have been updated. If rejecting DPO recommendations explain why:

	promoting individuals rights and helping them to exercise these, educating controllers on their responsibilities and reducing burdens on business' from poorly formulated SARs. 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. It was also noted that the statement "*the only mandatory fields are name and e-mail address….all other information on the web service is optional"* 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. Suggest discussing when IM&C Service and Project Team meet on 17/7/23.		
6.	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	07/07/2023	**Accept** Any comments: The online solution accommodates 'on behalf of' requests and the guidance sent to an organisation makes clear

	controller receiving the request that the ICO has taken no steps to verify authorisation to act, and they should do so. Similarly this will presumably be the case for regular requests, we'll be asking the controller to take steps to verify the requesters identity? 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.		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.**" @Steve We are actually updating the wording to include something along the lines of "**The ICO has forwarded this request on behalf of the requester 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. If rejecting DPO recommendations explain why:
7.	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.	07/07/2023	**Accept** Any comments: Section 3 Q9 has been updated, as there are no new web services being introduced we are utilising exisiting time-served retention practices. @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:

			"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". If rejecting DPO recommendations explain why:
8.	Access Controls – 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.	07/07/2023	**Accept** Any comments: We are not introducing any new technologies and will continue with existing access practices used elsewhere, and approved, in the the business. If rejecting DPO recommendations explain why:
9.	**Section 3** 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.	07/07/2023	**Accept** Any comments: If rejecting DPO recommendations explain why:

	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. Q15. - An update to the ROPA will be needed. Response changed to Yes and added as an action in section 6. Q16. - See recommendation 1, clarification required on data processors. 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.		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 retirieve it, or amend it with the organisation is question. We should review these q's and our understanding of whats being asked. SJ 18/07/2023 – explanation for no response added to Q18. Q19 and Q20 reviewed and response changed to Yes.
10.	Risk Assessment – generally the risk assessment is very limited and will need to be reconsidered once the above recommendations have been addressed.	07/07/2023	**Reject** Any comments: If rejecting DPO recommendations explain why:

	A few additional risks (not exclusive list) we suggest you consider are: • 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).		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. All the risks mentioned opposite are listed on the register, with the exception of: 4. See above comments in point 9 ref these q's 5. This has been addressed in point 3 above 6. Addressed in point 7 above Key DPIA risks in project risk register include: 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. 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. 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 orginator - in the

	• 5. Lack of age verification and risks associated with processing childrens data. • 6. Data retained for longer than is necessary		event of an incorrect e-mail being entered by the customer. 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. 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). 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? 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)

			Attached is a link to project risk register with risk scores and mitigations in place for each of these risks –  Project%20RAID%20Log%20-%20SAR%20T

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	14th July 23	SAT Tool project team	01/08/2023 – SJ
Review of cyber feedback	14th July 23	Greer Schick/Graham Rumens	
Update retention Schedule		Greer Schick/Graham Rumens/ IM&C Service	07/08/2023 - SJ
Update ROPA		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

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	4th 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.
V0.1	07/08/2023	Steven Johnston	Update to section 6 – actions completed.

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.