Data Protection Impact Assessment (DPIA) – PACE Fertility and Menstruation Apps. Understanding the user experience of fertility and menstruation apps

Document Name	Data Protection Impact Assessment – PACE Fertility and Menstruation Apps. Understanding the user experience of fertility and menstruation apps
Author/Owner (name and job title)	Melanie Carter, Project Manager
Department/Team	PMO/PACE
Document Status	Published
Version Number	V1.0
Release Date	4/09/2023
Approver (if applicable)	Pritheeva Rasaratnam, Director of Regulatory Risk & Supervision
Review Date	4/09/2024
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:	PACE 3: Fertility and Menstruation (Period) Apps
Project Manager:	Melanie Carter, Project Manager
Information Asset Owner:	Pritheeva Rasaratnam, Director of Regulatory Risk and Supervision
Controller(s):	Information Commissioner's Office
Data processor(s):	As we will be using the ICO website for this survey data may be processed by any of our current Data Processers who provide services to us that help the ICO website function. These are detailed in our existing privacy notice. But these existing services and any personal data they process to function will not be specifically considered as part of this assessment. https://ico.org.uk/global/privacy-notice/visitors-to-our-website/

	How you can contact us | ICO

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.

This DPIA is intended to consider the processing of data associated with the publication of a survey on the ICO website. This survey is available to all members of the public.

One of the ICO25 enduring objectives is to safeguard and empower people. To achieve this we've acknowledged that we need to do more to understand the views and concerns of the diverse UK population. Part of this is ensuring that the views of the public are an important evidence source for projects that we undertake at the ICO, including our projects led by PACE teams.

PACE 3 Fertility and Menstruation Apps project problem statement is: There are concerns that fertility and period tracking apps may be misusing the data of its users in a way which causes harm.

An objective of the PACE 3 Fertility and Menstruation Apps project is to receive feedback from users on their positive and negative experiences using the Apps and to obtain insights of user experience which increase our understanding of experienced harm.

Therefore we seek to create a dedicated survey page on the ICO website and invite users of fertility and menstruation apps (also referred to as period apps for our purposes) to answer questions on whether they have concerns about the use of their data by these apps and whether they have had any particularly positive or negative experiences about the use of their personal data by fertility tracking apps.

The survey will be a small number of questions, a mix of free text and multiple choice.

We plan to keep this survey open for up to one month. The insights from this research will be used by the PACE team exploring how users experience the relevant apps and the potential harms of these apps to the UK public.

We will create a specific survey page to ask the agreed question(s) and capture responses. The format will look similar to this Speaker request form | ICO.

Once app users have answered the questions and submitted their experiences, they will be taken to a page which thanks them for their time.

The team aims to create clear messaging which explains that this is an information gathering exercise. We don't intend to follow up on all responses. But the team may reach out for more information in some cases.

We also will outline that this is not a route for users to make a complaint to the ICO. If users wish to make a complaint then they should go through our existing recommended channels.

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
• Name (optional) • Email address (optional) • Age (optional) There is an option to submit a response to the survey anonymously.	Members of the public. Users of fertility and menstruation tracking apps.	Information Commissioners Office, Twilio Sendgrid	Yes If yes, list the countries the data will be transferred to: Data will be collected through a form on the ICO	< 1 year (please specify time period below) As per Privacy Policy, "we will retain consultation and survey response information until our work

			website. We use Twilio Sendgrid to support our email infrastructure and the operation of these services. Any personal information shared 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.	on the subject matter of the consultation is complete". For this particular consultation, responses will be reviewed when the survey closes (after approx. 1 month). Where a response does not require follow up, name and email addresses will be deleted. Where a response does require follow up we anticipate we will retain the data for up to 12 months.
Participant's views and opinions	Members of the public. Users of fertility and menstruation tracking apps.	Information Commissioners Office, Twilio Sendgrid	Yes If yes, list the countries the data will be transferred to: Data will be collected through a form on the ICO website. We use Twilio Sendgrid to support our email infrastructure and the operation of these services. Any personal information	< 1 year (please specify time period below) As per Privacy Policy, "we will retain consultation and survey response information until our work on the subject matter of the consultation is complete".

			shared 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.	For this particular consultation, we anticipate we will retain the data for up to 12 months.
Health data, including but potentially not limited to, fertility status, menstrual cycle, historic and/or current pregnancy. Participants will not be asked directly for this data but given the subject matter of the research it's reasonably foreseeable that they may well voluntarily provide it in the course of discussions.	Members of the public. Users of fertility and menstruation tracking apps.	Information Commissioners Office, Twilio Sendgrid	Yes If yes, list the countries the data will be transferred to: Data will be collected through a form on the ICO website. We use Twilio Sendgrid to support our email infrastructure and the operation of these services. Any personal information shared 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	< 1 year (please specify time period below) As per Privacy Policy, "we will retain consultation and survey response information until our work on the subject matter of the consultation is complete". For this particular consultation, we anticipate we will retain the data for up to 12 months.

			transfer and data is retained by Twilio for no more than 61 days.	
Data concerning sexual orientation. Participants will not be asked directly for this data but given the subject matter of the research it's reasonably foreseeable that they may well voluntarily provide it in the course of discussions.	Members of the public. Users of fertility and menstruation tracking apps.	Information Commissioners Office, Twilio Sendgrid	Yes If yes, list the countries the data will be transferred to: Data will be collected through a form on the ICO website. We use Twilio Sendgrid to support our email infrastructure and the operation of these services. Any personal information shared 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.	< 1 year (please specify time period below) As per Privacy Policy, "we will retain consultation and survey response information until our work on the subject matter of the consultation is complete". For this particular consultation, we anticipate we will retain the data for up to 12 months.

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:

NA

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:

N/A - no criminal offence data being processed

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.

This research forms part of a wider PACE project which is looking to understand whether fertility and menstruation apps may be misusing the data of its users in a way that causes harm.

We also want to capture areas of good practice in terms of fertility and menstruation apps' use of data.

Under the UK GDPR, the Information Commissioner has a number of tasks, including Article 57(1)(a) to monitor and enforce the application of the regulation, Article 57(1)(b) to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing, Article 57(1)(d) to promote the awareness of controllers and processors of their obligations under this Regulation, and Article 57(1)(i) to monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices.

The research will look to support the Commissioners decision making on appropriate regulatory action in this sector.

Wider project objectives are:

- 1. Understand how apps use data; identify any Data Protection non-compliance; and capture areas of Data Protection good practice

- 2. Identify any harms (or risk of harms) potentially arising from Data Protection non-compliance and establish if there are causal links or potential causal links

- 3. Recommend action that ICO should take to minimise harms or promote good practice in the sector.

We are commissioning research to support our understanding of points 1 and 2. We feel that to answer these objectives we need to engage directly with users of fertility and menstruation (period) apps. This will inform our understanding of how people experience these apps as part of their daily lives and if they have any particularly positive/negative experiences relating to the use of their data by fertility and menstruation (period) apps.

In order to inform the Information Commissioner under the Article 57(1) tasks already mentioned above, we feel it is necessary to engage with users of apps and ask for their first hand experiences and to be able to communicate and follow up with respondents, where they chose to provide contact information. Respondants will have the option to submit a response anonymously.

The reason we include the option to provide name and email address is so that ICO can follow up with respondents for further information if required, if the response is particularly relevant to this enquiry. Instances where ICO may follow up with a recipient include:

- To ask for more details
- To ask for permission to use their response as part of a case study
- To direct the respondent to our complaints department if it seems they are making a complaint (although we will set out on the web page that this is a research piece and complaints should be made through usual channels)

We have worded the question(s) asked in the survey so they specifically reference experiences 'regarding the use of personal data'. Due to the fundamental nature of the personal data that users provide to these apps it's expected that information about participants health and possibly other personal information will be disclosed.

Our view is that the amount of personal information participants will voluntarily provide in this case is necessary and proportionate to achieve the objectives of this research, to understand, first hand, users' experience of using fertility and menstruation apps and the 'real world' benefits or harms.

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.

The project manager had an initial meeting with Information Management Team Manager to run through the 'Screening assessment - do I need to do a DPIA?' form. I was advised a full DPIA would be appropriate in this case.

Corporate Comms, HPI were consulted about the question(s) that we intend to ask. Corporate Comms recommended the chosen survey method.

Policy legal consulted with regards to clarifying the purpose of the survey in our external messaging and managing expectations of those wanting to participate.

All sections of the DPIA will be completed, ensuring consideration is given to the data flow, security, retention and risks.

The ICO DPO, through the DPIA Forum, will also be consulted.

There will not be any consultation with the data subjects. We will not know who the data subjects until they respond to our survey.

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:

The survey will be posted as a web page on the ICO website. Data will be collected through the ICO website, directly from people submitting responses.

The survey is optional. Inputting name and email address is optional.

Technology used for the processing:

ICO website and its existing technologies. Specifically Twilio Sendgrid is used to support our email infrastructure, and this includes forms submitted through the website like this survey.

Detail on Twilio Sendgrid is available under existing info under the 'Submitting a form through our website' heading within the 'How you can contact us' section of the PN. How you can contact us | ICO

"**Submitting a form through our website**

Our website allows you to submit forms to us, for example, when making a complaint or paying the data protection fee. 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."

Storage location:

Stored in ICO website back end for 2 weeks.

When the forms are completed and submitted through the ICO website, we will use the 'Send as email' workflow, and responses will be auto-emailed to a dedicated inbox. This mailbox will be set up to allow the project team to review them.

Responses will be further collated into an Excel sheet and stored in a restricted access folder in an existing SharePoint online site. The ICO will store all outputs in the ICO SharePoint folder, where access to the data will be restricted to a need-to-know basis, based on business needs.

Access controls / data sharing

Access to ICO website back end: internally, information submitted through ICO website survey will be accessible by the ICO website team and the web development team in DDAT.

Dedicated Outlook inbox: small number of nominated colleagues will have access to this inbox to process responses. We expect emails will be deleted once reviewed and information transferred to SharePoint online library. In any case, the inbox will have a 12 month deletion rule.

SharePoint online folder: All outputs will be stored in a restricted access folder on the ICO SharePoint site, where access to the data will be restricted to a need-to-know basis, based on business needs. We forsee that this access will be restricted to the ICO project team. Any information relating to this research will be reviewed and, if necessary, destroyed by the relevant department when the retention period expires.

Disposal:

ICO website: ICO comms team will set the retention policy for ICO website, typically CMA keeps a copy of survey responses for two weeks. After two weeks they will be auto-deleted.

Dedicated inbox and excel sheet: in accordance with Privacy Notice, Responding to our consultation requests and surveys | ICO , we will retain consultation and survey response information until our work on the subject matter of the consultation is complete (see 1.3 for further details). At the end of this PACE project, all responses in the dedicated email inbox and excel sheet will be deleted and the inbox shut down and we expect this to be within 12 months.

The final output of the research, which will contain anonymised views and opinions will be reviewed after 6 years in line with the ICO's Retention and Disposal policy (Annex B, point 11.1).

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?

The existing privacy notice already covers my planned processing.

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?

Personal data will be submitted directly by the data subject when they fill out the survey. We will assume that data submitted is accurate.

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?

There is an existing project closure checklist for PACE projects and we intend to add an action to dispose of data to this as a checklist item, so it isn't missed.

Captured as part of ICO's retention and disposal policy. All information will be reviewed after 6 years.

Calendar reminders (HPI and Comms).

Q8. Will you need to update the ICO retention and disposal schedule?

No

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?

Please see information on data storage, access controls and data sharing in section 2 above.

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?

No

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

N/A – as this is a survey run through existing technology on the ICO website security assessment was not required.

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.

Don't anticipate a requirement for any new training or policies.

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?

No

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

N/A no new data processors involved.

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?

Yes

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*	Choose an item.	*Existing mitigation: We have checked that the system we intend to procure allows us to*	3	1	3 - low

personal 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.	**Access controls are not implemented correctly and personal data is accessible to an unauthorised third party**	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	Existing mitigation: Secure SharePoint site already set up. Expected mitigation: Dedicated inbox for survey responses with appropriate access controls.	**3**	**1**	**3 - low**
2.	**Personal data is retained for longer than is necessary by us**	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	Expected mitigation: See section 1.3, 2.0 and section 3 Q7 for how we will ensure data is deleted at the right time.	**3**	**2**	**6 - medium**

3.	**Unintended collection of additional personal data.**	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	Existing mitigation: As part of the DPIA process we have considered what data we can reasonably foresee survey respondents may provide, these are included in section 1.3. Expected mitigation: Any Personal Data (PD) that is collected that hasn't been included in section 1.3 will also be processed, stored and deleted in line with other PD as part of the project. If any PD is disclosed that we had not accounted for then we will update the DPIA and consider any implications before going into the next phase of the project. Participants will be informed of their rights to have any data rectified or deleted after submission of their response, should they wish.	**3**	**1**	**3 - low**

4.	**Data is transferred overseas to a country without equivalent data protection laws**	Tolerate: this risk is being accepted	Existing mitigation: SCC's in place for use of Twilio Sendgrid. Transfer risk assessment completed.	**3**	**1**	**3 - low**
5.	**Personal data is further processed in a way that is incompatible with the initial purpose and is not within the expectations of the data subjects**	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	Existing mitigation: We have provided privacy information that sets a clear purpose. Expected mitigation: If there is any desire to use data for new purposes outside of the scope of this DPIA then we will revisit and update the DPIA.	**3**	**1**	**3 - low**

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.	**DPIA section:** 2.0 Data Lifecycle **Recommendation:** There is reference to some data storage being in a SharePoint Online site. It would be helpful to clarify whether you're intending to set up a new SharePoint Online site (this is a site in the cloud version of SharePoint) or whether you're actually intending to save data to an existing site in SharePoint EDRM (our on premise version of SharePoint). This is just so there is absolute clarity on the storage location for this data. **Action:** Update DPIA to clarify.	Planning 31/08/2023	**Accept** Any comments: **The project operates an existing SharePoint online (cloud version) site.** **A restricted access folder was created, within this site, to store the data.** If rejecting DPO recommendations explain why:

2.	**DPIA section:** 2.0 Data Lifecycle **Recommendation:** If the ICO comms team will set the retention policy for data stored in the ICO website (CMA) we'd recommend you're specific about what you want them to set. Suggest just removing the word "typically" from here: "typically CMA keeps a copy of survey responses for two weeks. After two weeks they will be auto-deleted." And you then communicate your specific retention requirements to the Communications Team to ensure auto deletion rules are established and data isn't retained longer than is necessary. **Action:** Update DPIA and ensure automated deletion enrolled.	Planning 31/08/2023	**Accept** Any comments: **DPIA updated and comms team notified** If rejecting DPO recommendations explain why:
3.	**DPIA section:** 3.0 Q7 **Recommendation:** On review there was some confusion about what this mitigation action is: "Add as a checklist item in PACE project Operation (closure) phase."	Planning 31/08/2023	**Accept** Any comments: **DPIA amended** If rejecting DPO recommendations explain why:

	The assumption is there is an existing project closure checklist for PACE projects and you intend to add an action to dispose of data to this so it isn't missed? This paragraph may just benefit from some rewording to add context.		

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
Establish dedicated inbox for survey responses with 12 month deletion rule and appropriate access controls.	Start of research	Project Manager	31/08
Calendar reminders (HPI and Comms) for data deletion.	Survey Closure	Project Manager	

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.

The expected residual risk has been assessed as low and can be routinely accepted.

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**
Pritheeva Rasaratnam, Director of Regulatory Risk & Supervision	4 September 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	16/08	Melanie Carter (MC)	First Draft
V0.1	23/08	MC	Comms team input added
V0.1	31/08/2023	Steven Johnston, IMC Service Manager	DPO recommendations added to 5.0. Actions added to 6.0.
V1.0	04/09/2023	Pritheeva Rasaratnam, Director of Regulatory Risk & Supervision	Sign off and first release.

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.