Data Protection Impact Assessment (DPIA) – Understanding the user experience of fertility and menstruation apps

Document Name	Data Protection Impact Assessment – Understanding the user experience of fertility and menstruation apps.
Author/Owner (name and job title)	Damian Hamill – Senior Research Officer/ Helen Conlon – Market Research Manager
Department/Team	Research and Insight
Document Status	Published
Version Number	v1.0
Release Date	04/09/2023
Approver (if applicable)	Pritheeva Rasaratnam, Director of Regulatory Risk & Supervision
Review Date	04/09/2023
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:	Understanding the user experience of fertility and menstruation apps.
Project Manager:	PACE team
Information Asset Owner:	Pritheeva Rasaratnam - Director of Regulatory Risk and Supervision
Controller(s):	Information Commissioner's Office IFF Research (IFF)
Data processor(s):	Processor: Mojo Fieldwork, who are a recruitment provider and data processor under contract with IFF Research.

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.

One of the ICO25 enduring objectives is to safeguard and empower people and 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.

Therefore we are looking to commission an external research provider to support us with a research project that will explore the user experience of fertility and menstruation apps. The insights from this research will be used by the PACE team exploring the potential harms of these apps to the UK public.

We are asking a supplier to explore with members of the public areas such as:

- Overall views on fertility and menstruation apps, including why people use them, how they chose which app to use and how they use these apps on a regular basis
- Benefits and concerns about using fertility and menstruation apps
- Unprompted and prompted awareness of data protection concerns relating to the use of fertility and menstruation apps.
- The amount of data that users input into their fertility and menstruation apps from sign up to during use.
- Users approach to entering data into fertility and menstruation apps. For example, are they keen to provide as much information as possible, why? Do they only input data in required fields?
- Users understanding of what their personal data is used for when they enter it into fertility and menstruation apps.
- Users reactions to finding out what could happen to the data they enter into fertility and menstruation apps.
- Knowledge of privacy policies and their approach to this when signing up for the fertility and menstruation app.

This project will involve recruiting 26 participants to take part in either a 1:1 interview or a focus group. In total there will be approx. 10 interviews and approx. 2 focus groups, all of which will be conducted online via Zoom or Teams. All participants will be aged 16 or over.

All interviews and focus groups will be conducted by trained researchers from IFF Research (IFF).

In their role as the recruitment partner in this project, Mojo Fieldwork (MF) will initiate the initial contact with prospective participants and ask them a number of questions based on our screening questionnaire.

The purpose of these questions is to ensure that we obtain a diverse and representative sample of individuals to partake in the research. A sample of research participants meeting our criteria will then be selected to participate in the subsequent interviews and focus groups led by IFF.

Those who are screened for suitability but not selected to partake in the focus groups are described below as 'non-participants', whilst those who are

screened and selected to partake in the research are described as 'research participants'. Non participants may not end up being asked for all of the personal data in 1.3 below as Mojo Fieldwork will stop the interview as soon as they identify them as being unsuitable.

After the selection stage MF will share personal data of the research participants with IFF so they are clear of the characteristics of those recruited and so they do not need to ask these questions again and they have contact information to continue with the research process i.e. an email address to arrange a time for the interview / focus group.

All participants will be asked to consent to taking part in the research, at the recruitment phase but also again before beginning the interview or focus group. More details about how consent will be obtained and managed is found in section 1.4.

The ICO will receive only the anonymised views and opinions of participants as a report at the end of the research.

This research methodology is a well-established and well used technique that allows organisations to gain a more detailed and holistic view of a topic. The team at IFF Research who we have commissioned for this work are all highly experienced in undertaking this type of research.

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
• Gender • Names • Age • Region lived in • Ethnicity • Socio-economic group • Lifestyle information	Research participants/ non participants	IFF Research and Mojo Fieldwork	No	< 1 year (please specify time period below) IFF Research will keep personal information of

• Email address • Telephone number • Use of fertility and menstruation apps				research participants for 6 months after the completion of the whole project. Mojo Fieldwork will keep personal information of research participants for 3 months after recruitment and delete personal information of non participants at the end of fieldwork. Consent forms will be kept for 6 months from end of research.
Participants' views and opinions	Research participants	IFF Research and the ICO	No	IFF Research will keep personal information of research participants for 6 months after the completion of the whole project. The final output of the research, which will contain only anonymised views and opinions, will be reviewed after 6 years.

				ICO: In line with the ICO's Retention and Disposal policy (Annex B, point 11.1) any information relating to this research will be reviewed after 6 years and, if necessary, destroyed by the relevant department.
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.	Research participants	IFF Research	No	IFF Research will keep personal information of research participants for 6 months after the completion of the whole project.
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	Research participants.	IFF Research	No	IFF Research will keep personal information of research participants for 6 months after the completion of the whole project.

voluntarily provide it in the course of discussions.				
Images and audio recordings	Research participants	IFF Research	No	IFF Research will keep personal information of research participants for 6 months after the completion of the whole project.

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

Article 6(1)(a) - consent

Consent of research participants is obtained at the following points throughout the project:

- Mojo Fieldwork will conduct a recruitment interview via telephone (following initial contact by email) to determine if someone is suitable for the research (i.e. meets our criteria). If someone is found to be suitable then verbal consent to participate in the project, their details to be recorded and shared with IFF Research is obtained. Written consent is also obtained (electronically). It will be up to IFF / Mojo to ensure that any verbal consent obtained is properly recorded and compliant with the requirement for valid consent under DP legislation (e.g. individuals must be made aware of their right to withdraw consent and provided with a simple method to do so if they wish).
- Participants will be asked to give verbal consent to participate at the start of each depth interview / focus group. Video recordings of the interviews/groups are saved to a project-specific folder on IFF's secure network which only the named project team are able to access (this original file is not moved from this file at any stage, other than when it is securely deleted). Permission rights to secure network folders are allocated by the Project Manager. All activity relating to the secure files (copying, amending etc.) is recorded on the Data Asset Register and this is monitored and reviewed regularly. Video recordings of the interviews/ groups will be used for analysis purposes only and will be deleted inline with all the other information gathered by IFF during this project.
- The privacy notice will be shared with participants when they are sent the confirmation email for their interview / focus group slot.
- Participants have the right to withdraw from the project at any point, during or after the fieldwork.

The record of verbal and written consent will be kept for six months after recruitment by Mojo Fieldwork and 6 months after completion of the project by IFF Research.

The supplier/processor will provide the participants with a copy of their Privacy Notice which must fully comply with the requirements of Article 13 of the UK GDPR. The privacy notice will be preapproved by the ICO prior to being used. As per the Market Research Soceity's code of conduct, participants have the right to withdraw from the research at any point. Should a participant wish to withdraw their consent, the supplier will delete all the participant's personal data securely and a deletion 'receipt' can be produced for the participant's own records.

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)(a) - explicit consent

The process for obtaining explicit consent for the processing of special category data will be obtained at the same time and through the same method as for the Article 6 consent.

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:

N/A

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:

N/A - no public interest processing

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.

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.

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

- 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 a more holistic view of the user experience so we have a thorough understanding of how people select, sign up and use these apps as part of their daily lives and their experiences of these apps. In addition we'd like to explore people's understanding and expectations of how their personal information is used by these apps.

In order to carry out this research in a manner that adequately informs the Information Commissioner's understanding of this area of processing it will be necessary for our supplier to process the names and contact information of participants to be able to communicate with them to carry out the research.

Age, ethnicity, gender, socio-economic status and region lived in are required to ensure that the research contains an adequate representative sample of users of these apps.

Obtaining research participants' views and opinions is the fundamental purpose of this research in order to inform the Information Commissioner under the Article 57(1) tasks already mentioned above.

Due to the fundamental nature of the personal data that users provide to these apps it's expected that information about participants health will also be discussed.

Our view is the amount of personal information participants will voluntarily provide in this case is necessary and proportionate to achieve the objectives of this research.

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.

A 'Screening assessment - do I need to do a DPIA?' was completed and shared with Information Management who advised a full DPIA would be appropriate in this case.

All sections of the DPIA will be completed, ensuring consideration is given to the data flow, security, retention and risks. We'll consult with our supplier to understand all the elements of their processing and that of their processor.

We have consulted with Cyber Security and are awaiting their views on security arrangements.

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

There will not be any consultation with the data subjects as this would not be appropriate or practical given the nature and breadth of the processing. We will however ensure they are appropriately informed of what and how their personal data will be used as part of the recruitment process.

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 ICO and IFF Research will both be controllers for the personal data processed but the data subjects primary contact initially for this project will be Mojo Fieldwork as they will make the initial contact with potential participants, followed by IFF Research who will be the primary contact after the recruitment stage for all research partcipants.

- MF will make contact with participants via an existing panel of potential research participants.
- Participants join the panel by completing a form on the recruiter's website, usually via word of mouth / recommendations, or in response to advertising on local social media groups. Panel members are asked for demographic and geographical information, and some general lifestyle information (e.g. if they drive). The panel database is stored locally by the individual recruiter, on a single computer (protected with a strong password and with antivirus installed) to which only that recruiter has access. People join the panel to register their interest in taking part in future research projects.
- Panel members' information is held indefinitely as they requested to join the panel initially. If they wish to withdraw they can send a message to the recruiter at any time. Their personal data would then be deleted within seven working days.
- Additional information gathered about non participants related to this project would be deleted at the end of fieldwork.
- Further data is then gathered by IFF from participants as part of the interviews / focus groups.

- Anonymised quotes, insights and case studies will then form the basis of a published report for the ICO.

Technology used for the processing:

- Personal information about research participants will be transferred to IFF Research from MF via IFF's Secure File Transfer process which comprise sophisticated encryption technologies and Extended Validation SSL to ensure the integrity of data. File transfer sessions are fully encrypted using a TLS certificate. The encryption standards used are fully compliant with AES-256.

- Findings from depth interviews will be written up into an Excel framework for analysis, this will contain demographic information (e.g. gender, age) but no identifiable personal information. The framework will be stored in a project-specific folder on IFF's encrypted file server located on a secure local network which only the named project team are able to access (this original file is not moved from this file at any stage, other than when it is securely deleted). Permission rights to secure network folders are allocated by the Project Manager. All activity relating to the secure files (copying, amending etc.) is recorded on the Data Asset Register and this is monitored and reviewed regularly.

- The ICO will store all outputs on the ICO SharePoint site where access to the data will be restricted to a need-to-know basis, based on business needs.

- No other systems or technology will be used to deliver the project.

Storage location and Access Controls:

Mojo Fieldwork:

Information gathered during recruitment will be stored on a strong password-protected computer with antivirus software, in the UK, to which only the recruiter has access.

IFF Research (this refers to personal information gathered at recruitment and in the interviews/ focus groups):

Client data at rest resides on a TPM 2.0 hardware encrypted hard disk utilising Microsoft Bitlocker at AES-256 plus Diffuser. Storage is hosted exclusively within the businesses own London office data centre. The data centre is contained within locked, access and environmentally controlled server room. Logical data storage is to fully encrypted storage volumes hosted upon redundant SAN units. All business data and systems are backed up daily, utilising a 3-2-1 backup strategy. Off-site backup is uploaded to Azure using AE256 encryption.

Personal data will be stored in a project-specific folder on IFF's secure network which only the named project team are able to access (this original file is not moved from this file at any stage, other than when it is securely deleted). Permission rights to secure network folders are allocated by the Project Manager. All activity relating to the secure files (copying, amending etc.) is recorded on the Data Asset Register and this is monitored and reviewed regularly. All activity relating to the secure files (copying, amending etc.) is recorded in their Access Rights Management software – object access events are kept for 6 months and are available for retrospective analysis.

Only authorised users can access IFF Research systems, Access to IFF systems is restricted to users with an approved Active Directory account. All users are required to have a 10-character complex password which must be changed every 30 days. A clear screen policy is in effect with automated locking and blanking of screens after 5 minutes. IFF also have an access rights policy that restricts access of sensitive data (including all personal data) on an authorised as needs basis. Privileged access is granted by IT administrative staff only. Restricted areas of the system are subject to an access control policy whereby project managers manage access on an as needed basis. A register is kept of who has been granted access rights to sensitive data.

IFF protect their systems through a package of sophisticated network security appliances (SonicWall NSA 4700) which offer DPI (Deep Packet Inspection) of data of all kinds coming into IFF Research Ltd. BitDefender anti-virus enterprise software is installed on desktops, laptops and servers. Virus Definition Files are checked every 15 minutes and updated when required.

ICO

All outputs will be stored 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.

Data sharing:

IFF Research:

Outputs will be transferred to the ICO by secure electronic transfer via a Secure File Transfer process with sophisticated encryption technologies and Extended Validation SSL to ensure the integrity of data. File transfer sessions are fully encrypted using TLS 1.2/1.3 certificates. The encryption standards we use are fully compliant with AES-256. Access to files is restricted to authorised recipients only, who receive an email with details of the download as well as a further identity verification check.

Mojo Fieldwork:

Participant information will be transferred to IFF Research by secure electronic transfer via a Secure File Transfer process with sophisticated encryption technologies and Extended Validation SSL to ensure the integrity of data. File

transfer sessions are fully encrypted using TLS 1.2/1.3 certificates. The encryption standards we use are fully compliant with AES-256. Access to files is restricted to authorised recipients only, who receive an email with details of the download as well as a further identity verification check.

Disposal:

IFF Research:

All personal data will be stored for a maximum of six months from the end of the project (including participant data collected during recruitment, transcripts from fieldwork and consent forms). Research outputs (final report), which do not contain any personal data, would typically be held indefinitely unless the client requests otherwise, in which case they will be securely deleted in line with the timeline requested.

Mojo Fieldwork:

Written consent forms are stored securely for a period of 6 months. All other information gathered at recruitment is stored securely for a period of 3 months.

ICO:

The ICO's retention and disposal policy (Annex B, point 11.1) outlines that information created in relation to research will be retained for 6 years from last action and then reviewed.

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?

A seperate bespoke privacy notice will be drafted and provided to the data subjects. This required action has been added to the DPIA outcomes (see section 6.0).

The supplier/processor will provide the participants with a copy of their Privacy Notice which must fully comply with the requirements of Article 13 of the UK GDPR. The privacy notice will be pre-approved by the ICO prior to being used.

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?

Yes

The recruiter (Mojo Fieldwork) will first obtain verbal consent to participate, followed by written consent (electronically). This is stored securely on a password protected laptop which only the Company Director has access to. Records of verbal and written consent are kept and stored securely for 6 months.

IFF Research will confirm consent verbally at the start of the depth interview or focus group. Video recordings of the interviews/groups are saved to a project-specific folder on IFF's secure file server which only the named project team are able to access (this original file is not moved from this file at any stage, other than when it is securely deleted). Permission rights to secure network folders are allocated by the Project Manager. All activity relating to the secure files (copying, amending etc.) is recorded on the Access Rights Manager software. Records of verbal consent will be kept for 6 months after completion of the project.

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?

The personal data likely to be collected by IFF Research will reflect an experience at a point in time and is unlikely to need updating or correction. If details about a participant do change over the course of the project then the supplier will update this with the participants consent.

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?

IFF Research – the retention schedule is outlined in 2.0 and information will be deleted six months after the completion of the project.

This is in line with the documented IFF disposal procedure (**A18_1_3 Data Retention and Disposal Procedure**)

IFF ensure data is deleted from their systems using the deletion tool SDELETE which meets data sanitisation standards outlined in 'DoD 5220.22-M'.; and provide confirmation in writing to the client that this has been done.

Mojo Fieldwork –Personal information belonging to a project is deleted up to three months after the project is completed except for the records of consent which are kept for six months.

ICO: We'll be following the guidance in the ICO's retention and disposal policy and all information will be reviewed after 6 years.

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?

Yes

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

Security opinion is "met". This reflects our view that the Supplier, IFF Research, has met all our minimum requirements. The Supplier assessment is now concluded, and the outcomes saved for our records.

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.

N/A

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 data processors involved

The ICO and IFF will both be controllers for the personal data. We will ensure that appropriate contracts are in place between the ICO and IFF. Mojo Fieldwork are an existing processor of IFF, and the ICO will have no direct contractual relationship with MF.

All third-party data processors have undergone IFF Research approved supplier process; the supplier agreement in place with these include data protection clauses. The contract between IFF Research and Mojo Fieldwork is here:

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 asses 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 set*	3	1	3 - low

personal data is accessible to an unauthorised party.			*access permissions for different users.* *Expected mitigation: 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	Tolerate: this risk is being accepted	Existing mitigation: Data storage shall be carried out on UK based servers in a secure ISO27001 environments. All PI held by both IFF Research and Mojo Fieldwork is held on secure servers and only approved staff have access to personal data for this project as outlined in section 2.	**3**	**2**	**6 - medium**

2.	Security controls are inadequate for protecting personal data resulting in a loss of confidentiality, integrity or availability.	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	Existing Mitigation: Section 2 outlines how IFF Research and Mojo Fieldwork will store and protect the personal information collected during this research. All PI will be stored on encrypted or password protected files with only relevant staff members having access to it. PI will be transferred between Mojo Fieldwork and IFF Research via a secure file transfer. Expected Mitigation: ICO Cyber Security service will carry out a supplier assessment. Any resulting recommendations or actions required will be followed up by project leads.	**3**	**2**	**6 - medium**
3	Unintended collection of additional personal data.	Treat: this risk is being reduced by management action such as implementing	As part of the DPIA process we have considered what data we can reasonably foresee the researchers may gather as part of the	**3**	**1**	**3 - low**

		controls or tackling the cause	interview and these are included in section 1.3. Any PI that is collected that hasn't been included in section 1.3 will also be processed, stored and deleted in line with other PI as part of the project. If any PI 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 interviews, should they wish – including reviewing relevant data after its conclusion.			
4	Mojo Fieldwork fail to process in accordance with instructions from IFF.	Tolerate: this risk is being accepted	Existing Mitigation: The data processing will be carried out in line with the contract between IFF Research and Mojo	**3**	**1**	**3 - low**

			Fieldwork. Mojo Fieldwork have undergone Ipsos UK's approved supplier process; the supplier agreement in place with includes data protection clauses.			
5	Participants come to harm during the research, e.g. becoming distressed when discussing the subject of the research.	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	All IFF researchers understand their obligation to protect respondents from harm and abide by the professional standards of the MRS to ensure no harm is caused by participating in research. They are trained to intervene and contact the relevant authorities if they believe the respondent to be at direct risk, or signposting to relevant services if the respondent has a need for official advice and support. When designing research involving sensitive subjects, care is taken to incorporate safeguarding considerations. These considerations inform the design of recruitment strategies, research materials and researcher	**3**	**1**	**3 - low**

			briefings - ensuring that not only do researchers conduct themselves in the proper manner to minimise potential personal and social harm, but they are prepared to respond to any allegations or clear signs of abuse, harm or exploitation having occurred.			
6	Participant does not feel comfortable taking part in the discussion.	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	Participants can withdraw from the process at any time, including on the day of the interview/ focus group – and afterwards should they wish for data to be deleted. Any PI collected up to that point will be deleted	**3**	**1**	**3 - low**
7	Participant unable to provide informed consent.	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	When recruiting, IFF Research and Mojo Fieldwork will ensure information and consent is provided in a format that complies with relevant equalities law, and specific accessibility needs as required (for example plain language versions for individuals with reading disabilities). IPSOS and ICO will also consider ways to verify that	**3**	**1**	**3 - Low**

			participants understand information provided.			

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.	The IFF privacy notice indicates they gather IP address and web browser data when individuals participate in their research. This needs to be clarified with IFF to see if they will gather this data as part of our research. If yes, these data categories should be added to your data inventory in 1.3.	Planning 16/08/2023	**Accept** Any comments: We have clarified with IFF that the references to IP address and web browser data in their privacy notice only apply to online surveys – so they will l not gather that data as part of this research. If rejecting DPO recommendations explain why:
2.	We understand images and audio recordings of participants will be collected and we recommend you also	Planning 16/08/2023	**Accept** Any comments: Added to 1.3

	add these as data categories in your data inventory at 1.3.		If rejecting DPO recommendations explain why:
3.	Mojo Fieldwork – We were unable to find a privacy notice on the website of Mojo Fieldwork so it's unclear what transparency information they provide to their existing panel of potential research participants. If you haven't already we would recommend you seek some assurances from IFF / Mojo to confirm that the personal data of panel members has been obtained lawfully and is processed in compliance with UK GDPR. We also noted data is all stored by MF on one laptop. We understand you're engagement with our Cyber Security team is in progress and, if you've not done so already, we'd advise you flag this to them so it's considered as part of their assessment.	Planning 16/08/2023	**Accept** Any comments: Mojo's privacy notice has now been added to their website. As a company Mojo Fieldwork only has a single member of staff so the data for all the recruits for this project would be stored on his password-protected business laptop. Cyber Security have concluded their assessment, saying 'Security opinion is "met". This reflects our view that the Supplier, IFF Research, has met all our minimum requirements.' If rejecting DPO recommendations explain why:
4.	We're not clear on the age range you're targeting with your research, and we understand you're still developing your screening questionnaire that will be used to identify suitable participants.	Planning 16/08/2023	**Accept** Any comments: Participants will be aged 16 or over and I have added this into section 1.2. If rejecting DPO recommendations explain why:

	We will just flag that you should consider whether you'll be seeking views from children (under 16). If you're not explicitly ruling this group out you should revisit this DPIA to consider any additional risks associated with using the personal data of children. If you don't intend to use any data related to children we'd advise just updating the DPIA at 1.2 to explicitly state this.		
5.	We'd recommend you remove the statement "ICO recommends that this is reviewed after 6 years in line with the ICO retention and disposal policy." in section 2. This isn't applicable to IFF as it is our own internal policy.	Planning 16/08/2023	**Accept** Any comments: Sentence has been removed. If rejecting DPO recommendations explain why:
6	We've updated your response to Q15 in section 3 from 'Not Sure' to 'No' as no update to our Record of Processing Activities is required.	Planning 16/08/2023	**Accept** Any comments: N/A If rejecting DPO recommendations explain why:

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
Privacy notice / consent forms to be provided to participants in advance of interviews / focus group sessions.	Before start of processing	Helen Conlon – Market Research Manager Melanie Carter – Project Manager	Ongoing
Update risk assessment once the outcome of the Cyber Security Assessment is received.	Before start of processing	Helen Conlon – Market Research Manager Melanie Carter – Project Manager	Cyber security assessment complete 17/08/2023. Security opinion is met.

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.

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	08/11/2023	Helen Conlon	First Draft
V0.1	17/08/2023	Steven Johnston	DPIA Forum recommendations added to section 5. Actions updated in section 6.
V0.1	01/09/2023	Melanie Carter	Responded to IAO comments and updated
V1.0	4/09/2023	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.