PG621944A Data Protection Impact Assessment – Early Help and Supporting Families National Insights data collection.

NAME OF PROJECT/ACTIVITY:	Early Help and Supporting Families National Insights data collection
DATE:	26th September 2023
NEXT REVIEW DATE:	8th January 2023

What kind of processing and data does this proposal involve?	
Who is the Lead/Manager/Senior Responsible Owner for the policy/ project/initiative?	[redacted], Deputy Director of Changing Futures and Supporting Families
Who is the Information Asset Owner?	*DfE (May 2024-)* *DLUHC (July 2023-May 2024) – Catherine Frances, Director General of Local Government, Resilience and Communities*
What is the controller/processor relationship	Since 2021, the Supporting Families has been jointly governed the Department for Levelling Up, Housing and Communities (DLUHC) and the Department for Education (DfE). The programme has two SROs, one in each department, who cross-departmentally determine the direction of the programme. Therefore, it is deemed appropriate that both DLUHC and DfE are given the status of data controller for this project. However, due to the planned Machinery of Government (MOG) change in May 2024, which will involve the DLUHC component of the Supporting Families team moving to DfE, DfE will become an independent data controller. Beyond May 2024, there will be no role for DLUHC. Additionally, all participating Local Authorities will hold the status of independent data controllers. They will provide data from their case management systems to IFF Research. IFF Research is the contracted supplier appointed by DLUHC to manage this data collection project. They are a data processor and will hold this status from July 2023 until March 2025, when the contract ends. This contract is currently between IFF Research and DLUHC but will be transferred to DfE in May 2024 as a result of the planned MOG change.

If there is a joint controller relationship, provide an explanation of how this was determined and the roles and responsibilities of each controller	Due an impending Machinery of Governance (MOG) transfer of policy responsibilities, which will see the "Supporting Families" policy area transfer from DLUHC to DfE, DLUHC and DfE will be interim joint data controllers for this collection until May 2024. Beyond May 2024, and the planned MOG change, DfE will be the only department with the status of data controller. DLUHC will no longer be a data controller and therefore all the roles and responsibilities highlighted as belonging to DLUCH will be transferred to DfE after the MOG change. Interim DLUHC Roles and Responsibilities: - Management of data processors (the contract with IFF Research) to ensure they are adhering to the data processing arrangements set out in Schedule 20 of this contract. - Issue the data sharing agreements to the 152 participating local authorities that set out their roles and responsibilities as independent data controllers. - Ensure the data is stored on the departmental SharePoint securely. - Manage access to the data within DLUCH and ensure everyone has adequate training/understanding of data sensitivity. - Oversee the dissemination of LA and National level reports produced by IFF Research. Joint Roles and Responsibilities: - Determine the purpose of processing and how personal data is processed by IFF Research. - Adhere to GDPR principles. - Determine what kinds of ad-hoc analysis on data will be required to inform commissioning decisions.
What personal data will be processed as part of the project/ policy/initiative?	The case level/family 'packet' of data, which includes the Family ID, contains personal and sensitive data relating to family needs (see Annex A for full break down of fields). The sensitive topics included in the case level collection includes the presence/absence of; - Childhood sexual exploitation, - Domestic abuse, - Criminal activity/conviction, - Poor mental health, - Drug and or/ alcohol abuse. This makes the processing "high risk" under UK GDPR. There will be no detail relating to the specifics of these issues recorded, only a drop down which will indicate the presence or absence of evidence of these issues. The data collected and processed will be pseudonymised at case/family level, therefore it constitutes personal data under UK GDPR. • The data will be provided by local authorities (LAs) from their own case management systems. This will be data collected from families and partners, to provide a holistic picture of all the issues faced by families supported in Early Help and/or Childrens Social Care (if the case is claimed under the Supporting Families payments by results process).

<table>
<tr><td></td><td>

The data will be submitted by LAs in a pseudonymised format using an LA family identifier (Family ID). Pairing the case level data with a family identifier is necessary to identify which problems are correlated with one another and associated with outcomes. Without this identifier it would also not be possible to track trends over time (problems, outcomes, re-referrals).
However, in the interest of data minimisation, the LA family identifier (Family ID) will be replaced by a new Family ID created by IFF before being shared back to DLUHC for government analytical use. This will minimise the sharing of personal data.

</td></tr>
<tr><td>How many individuals' data will be involved?</td><td>
This will be very large-scale processing. The number of individuals affected will depend on the number of individuals that are being worked with by Early Help services. From a small sample of local authorities who provided the approximate number of cases they have over a two-year period; we are estimating approximately 5,000 cases to be in each submission on average from each local authority. The national evaluation for Supporting Families found that the average size of a family on the programme was four. Therefore, for every data submission, we would expect an average of 20,000 individuals to be in scope per authority, and scaling that up to 152 upper tier authorities in England, that would put 3,040,000 individuals in scope.

<table>
<tr><td></td><td>5,000</td><td>The average number of cases in each submission</td></tr>
<tr><td>x</td><td>4</td><td>The average size of a family on the programme</td></tr>
<tr><td>x</td><td>152</td><td>The number of upper tier local authorities</td></tr>
<tr><td>=</td><td>3,040,000</td><td>The approximate number of individuals in scope for the data</td></tr>
</table>

The smallest submission we could expect to receive is 100 families. This estimate is based on the number of families our smallest LA works with each year (50).
The project is aiming to build up this dataset gradually, asking for local authorities to join the data collection when their systems are ready, so the aim is for all 152 upper tier local authorities in England to be sharing data.
</td></tr>
</table>

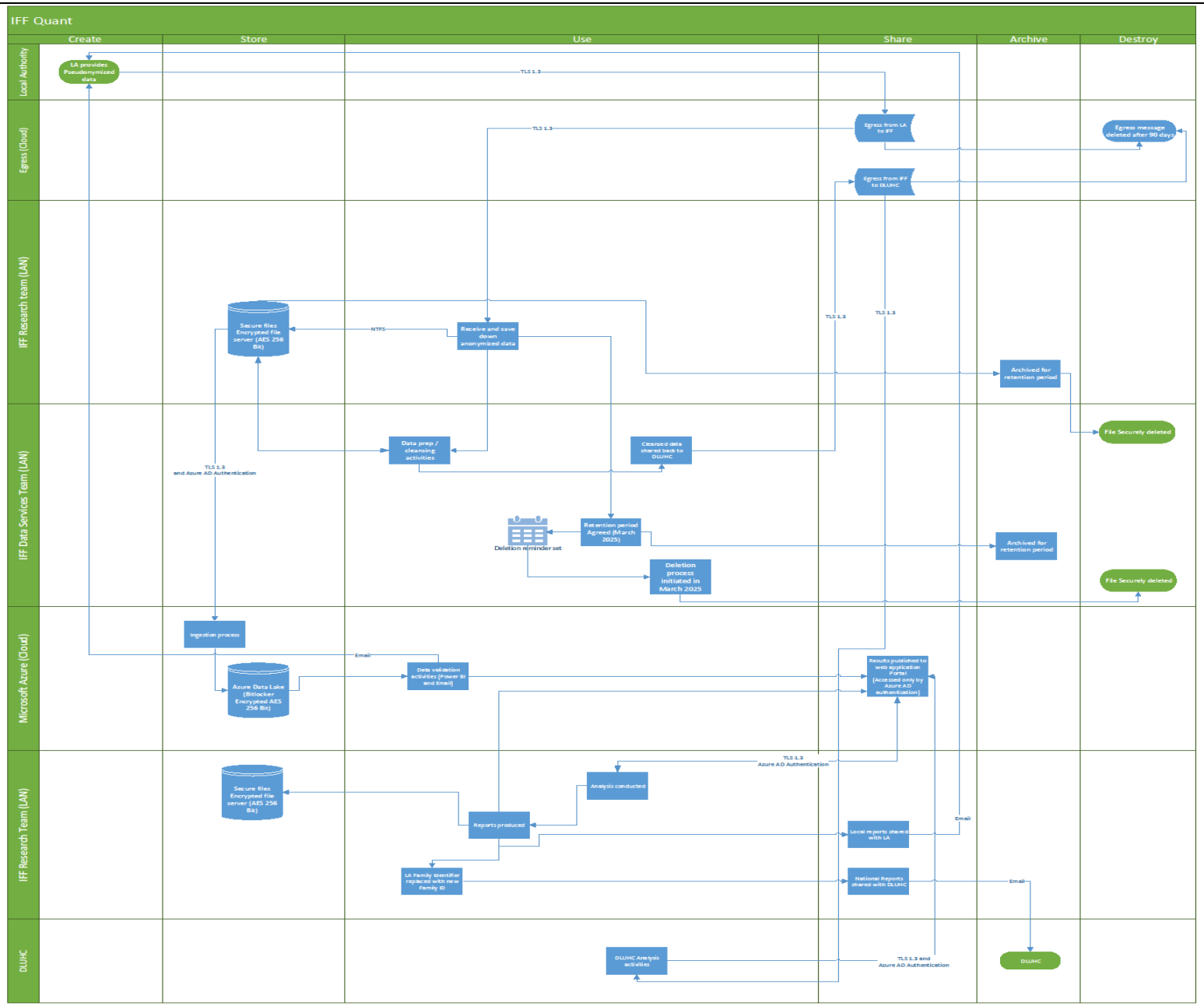
<table>
<tr>
<td>How much data will you be collecting?</td>
<td>
According to the 2022 Data Survey, we estimate to collect data from the following number of Local Authorities.
<table>
<tr><th></th><th>Estimated number of LAs per collection</th><th>Estimated number of cases per collection</th></tr>
<tr><td>July 2023</td><td>67</td><td>335,000</td></tr>
<tr><td>Feb 2024</td><td>110</td><td>550,000</td></tr>
<tr><td>July 2024</td><td>130</td><td>650,000</td></tr>
<tr><td>Feb 2025</td><td>135</td><td>675,000</td></tr>
<tr><td>July 2025</td><td>149</td><td>745,000</td></tr>
</table>
We will be collecting case level data on the fields found in Annex A.
</td>
</tr>
<tr>
<td>Describe the nature of the processing.</td>
<td>
The data will be collected by Lead Practitioners from their case work with families receiving support from Early Help and Childrens Social care service. There will be no new data collected from data subjects for the purpose of this collection, as all this data is already collected and stored in LA case management systems. Therefore, the data source will be LA case management systems. LAs will extract this data and share it with DLUHC’s contracted data processor IFF Research via Egress (a DLUHC approved secure file-sharing software).

IFF Research will download the data onto their on-premises secure encrypted file server. The data will be cleansed and output into IFF’s secure Web Portal accessible through Azure AD authentication. Storage of this data is in Azure Data Lakes using AES-256 encryption. The IFF Web Portal will be accessible to LAs to self-serve an view their own data visualisations on PowerBI. This will be a password protected secure log in using Microsoft 365.

IFF Research will act under DLUHC’s instruction to perform quality assurance analysis and statistical analysis (including frequency distributions, multivariate analysis, segmentation analysis and longitudinal regression). The processed data files will be provided back to DLUHC using Egress.
</td>
</tr>
</table>

	Once returned to DLUHC, the data will be stored on SharePoint which is DLUHC's main information management platform. In addition to the Supporting Families team in DLUHC, a restricted number of DfE analysts will have access to the SharePoint in order to perform data quality assurance and ad-hoc analysis to respond to requests from SLT/Ministers. All parties with access will be briefed on the sensitivity of the data. In the event of role change, any party with access to the cleansed data files will have access removed. The final data outputs will be the national and local level reports. These reports will only contain cohort level data. There will be no case-level, Family IDs or personal data within these reports. As a result, these can be shared by IFF Research to DLUHC via email. These emails will be marked Official-Sensitive when distributed. Additionally, all outputs will be marked as Official-Sensitive.
Does the project/policy/initiative involve the use of personal data we currently process, or will this be new data??	This data is already collected at the local level by LAs for Early Help and Children's Social Care services. This will be nationally collated for the first time. Collecting the data at a national level will help to provide a holistic picture of all the issues faced by families supported in Early Help and/or Childrens Social Care (if the case is claimed under the Supporting Families payments by results process).

Data Flow analysis –


IFF Quant
Create
Store
Use
Share
Archive
Destroy
Local Authority
Egress (Cloud)
IFF Research team (LAN)
IFF Data Services Team (LAN)
Microsoft Azure (Cloud)
IFF Research Team (LAN)
DLUHC
LA provides Pseudonymized data
TLS 1.3
Egress from LA to IFF
Egress from IFF to DLUHC
Egress message deleted after 90 days
Secure files Encrypted file server (AES 256 Bit)
NTFS
Receive and save down anonymized data
Archived for retention period
File Securely deleted
Data prep / cleansing activities
Cleansed data shared back to DLUHC
TLS 1.3 and Azure AD Authentication
Deletion reminder set
Retention period Agreed (March 2025)
Archived for retention period
Deletion process initiated in March 2025
File Securely deleted
Ingestion process
Email
Azure Data Lake (Bitlocker Encrypted AES 256 Bit)
Data validation activities (Power BI and Email)
Results published to web application Portal (Accessed only by Azure AD authentication)
TLS 1.3 Azure AD Authentication
Secure files Encrypted file server (AES 256 Bit)
Analysis conducted
Reports produced
Local reports shared with LA
Email
LA Family identifier replaced with new Family ID
National Reports shared with DLUHC
Email
DLUHC Analysis activities
TLS 1.3 and Azure AD Authentication
DLUHC

Requirement		Comments
Data Protection Impact Assessment UK - GDPR Article.35	Data Protection Impact Assessment (DPIA): • Has a DPIA screening process for the proposal/project/system been completed? • If yes – please attach the DPIA screening outcome.	1. Vulnerable persons processing 2. Special category data processing 3. Very large-scale processing
The Principles UK-GDPR Article.5 • Lawful • Purpose • Data minimisation • Accurate • Storage limitation • Integrity and confidentiality (security) • Accountability	Lawful: • What is the legal basis for processing the data? • Does this require the data to be processed, or simply allow it?	The processing is necessary for the interim joint controllers to perform a task in the public interest. In particular, to help further the understanding of needs identified for families within Early Help, identify the scale of re-referrals and be able to share insight on a national and local level to support the work in improving the lives of families. • UK GDPR Article 6(1)(e), "task in the public interest or official authority". The joint controllers are relying on respective Secretary of State common law powers (LUHC and Education) as the vires for this processing. • Data Protection Act 2018, Section 8(d) "exercise of a function of the Crown, a Minister of the Crown or a government department" • Article 9(2)(g) "substantial public interest". The joint controllers are relying on respective Secretary of State common law powers (LUHC and Education) as the vires for this processing. • Data Protection Act 2018, Part 2, Schedule 1 section 6 "exercise of a function of the Crown, a Minister of the Crown or a government department" This is because we need to understand how families with health conditions/mental health problems are accessing Early Help services, and the extent to which they are able to achieve successful outcomes. This will enable us to make more informed policy and

		commissioning decisions, and support those with health conditions (physical and mental). • The processing of criminal conviction data is justified as it is also deemed necessary for reasons of substantial public interest. This is because without this information, we would not be able to understand how offenders or historic offenders navigate the Early Help system, and the extent to which they are able to achieve successful outcomes. Without this special category data, we would not be able to make informed decisions about the commissioning of services tailored to the needs of offenders. • In accordance with the requirements of Part 2, Schedule 1, Part 4 of the Data Protection Act 2018, the Joint Controllers will have an 'appropriate policy document' as the required additional safeguard. The Local Authorities, as independent data controllers, will be utilising their own legal basis for processing. While we would expect LAs to take their own legal advice, the Department's view is that in the data sharing agreements that they might consider using Section 111 of the Local Government Act 1972 as a suitable statutory power.
	• What is the business use/purpose for processing the data?	The processing will achieve the purpose of allowing DLUHC and DfE to understand the issues and outcomes affecting families worked with by Early Help and Supporting Families, for the following purpose: • Processing the data in this way will help recognise which problems are correlated with one another, but also with outcomes. • By collecting and processing this data we will better understand the demographics of those families supported by Early Help. • This will help inform policy and commissioning decisions. In particular, the collection will provide essential inputs to future policy discussions on the shape of early help and children's social care and the response to the Care Review. • As the data set grows, there is also potential for causation and trends in risk to emerge over time. Insights from this research will also enable local authorities to resource and commission support more effectively and target specialist support at specific problems (thereby increasing the impact and value for money of existing programmes).

		• Asking local authorities to provide these data drives them to improve their use of data, helping to deliver our priority to 'increase data maturity, so that services are targeted at the communities that need them, and we can assess and prove impact'. • During the consultation both Sheffield City Council and Liverpool City Council reported that the actions of generating the test data for the pilot informed them of key changes that could be made to improve their current data and systems, such as identifying data gaps and helping to prioritise future system development. At the local and national level, these insights will lead to an improved service for individuals and families, and families receiving the right support at the right time.
	Data minimisation: • Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purpose. What assessment has been made to ensure the personal data is adequate, relevant, and limited to what is necessary in relation to the purpose?	This is large scale project which involves the processing of data relating to vulnerable individuals. We have considered the potential for alternative approaches, to minimise the amount of data processed. For example, a sampling method could be used to limit the number of families data processed. However, because Early Help data has not been collected on a national scale, we have no reference point to determine an appropriate sampling frame. This would risk us producing inaccurate pictures of outcomes to inform policy or decision-making and would not encourage LAs to include partnership data. For this collection, the only personal data collected is an extract from the wider LA record - the Family ID used by Local Authority case management systems. This is pseudonymised data, which would only be personally identifiable if matched back to Local Authority records (names, contact details, addresses etc). However, we are aware that there is a small "disclosure control" risk of there being a data breach in LA case management systems which would enable the Family ID to be matched to a specific family. One of the ways we are seeking to minimise this risk is by giving each case a further new Family ID once transferred to IFF Research. This will mean two layers of pseudonymisation are implemented, making the likelihood of someone being able to match the new Family ID back to personal identifying information more remote. The Family ID is still necessary to perform the analysis required for this collection. In particular to recognise and track rereferrals and understand the step-up and step-down journey of families between preventative Early Help and statutory services. We are therefore confident that we are collecting and processing the minimum possible amount of personal data in order to fulfil our purpose.

		While the Family ID is the only direct possible identifier, there is a chance that when combined the other data fields may result in family identification. For example, in a small local authority with a small number of Early Help cases, a family with a niche combination of issues may be identified. If there are only a handful of families with children with SEND, parent with criminal convictions and addiction problems in an LA there is a possibility that a family's identity could be inferred by someone who is familiar with them. Therefore, we are treating the entire data set as pseudonymised personal data. It is necessary to collect all these data fields on the issues and outcomes faced by families in order to capture the complexity of family need, and to remain consistent with the Supporting Families outcomes framework.
	Accurate: • How will the accuracy of the data be checked? • How will inaccurate data be corrected? • How will it be kept up to date? • What processes will be in place to manage requests for rectification?	Article 5(1)(d) states 'personal data shall be: (d) accurate and where necessary, kept up to date.' The personal data in this collection (Family ID) will be kept up to date by Local Authorities. Each submission will give them an opportunity to give an updated Family ID in the event of a family split (whereby a second Family ID is created). In the event there is an error in the Family ID/any other data field, this will be detected by the data validation reporting tool IFF Research have built into their online submission portal. After the initial collection window (approximately 3 weeks), there will be a 2-week data checking period. During this time, IFF will review the data validation reports for each LA submission and will raise any queries/errors identified in the data to rectify any errors. This process will occur on a rolling basis, following each collection.
	Storage Limitation: • How long will the data be kept? • Is the data covered by an existing retention and deletion schedule? • If not, will one be agreed with the Departmental Records Officer? • Will you be able to delete the data when you no longer need it? If you can't delete it, can you anonymise it partly or wholly? What processes will be in place to ensure the data is securely destroyed/deleted?	The data will stored by IFF Research for the duration of this project (until March 2025). This is needed in order to identify trends that emerge over time and successfully identify re-referrals over the two year collection period. Once the project ends (in March 2025), IFF Research will have three months to delete all case level data/personal data. Deletion certificates must be provided within this three month period to DLUHC/relevant LAs. IFF will ensure on-premises data is automatically deleted within this timeframe. This can be manually achieved on request. Azure based data retention can be customised according to the client preference. This data will be permanently removed once the services are shutdown. Until May 2024, DLUHC as a joint data controller will store the data on the departmental SharePoint. However, upon the planned MOG change to DfE, DfE will become the sole data controller. Therefore, the data will be deleted from DLUHC once it is no longer needed by the department (because the Supporting Families team has moved to DfE). After May 2024, DfE will become` the data controller. DfE will retain case level data for the remainder of the project (until March 2025). After March 2025, DfE may store aggregated data and data without Family IDs until 2023, but all personal/case level data must be deleted.

<table>
<tr>
<td></td>
<td></td>
<td>Summary table of deletion timetable for data by different parties:

<table>
<tr><td></td><td>IFF Research</td><td>DLUHC</td><td>DfE</td></tr>
<tr><td>Personal Data (Pseudonymised case level data)</td><td>March 2025 (project end).

IFF Research will have 3 months to delete all personal data and provide the contract holder (DfE) with deletion certificates.</td><td>May 2024 (Supporting Families programme moves to DfE).
DLUHC will cease to hold the status of data controller and will have no involvement beyond May 2024.</td><td>March 2025 (project end).</td></tr>
<tr><td>Non-personal Data (aggregated data/reports)</td><td>March 2025 (project end).

IFF Research will have no purpose for retaining aggregated data/reports beyond project end. They will therefore be instructed to delete this data.</td><td>May 2024 (Supporting Families programme moves to DfE).
DLUHC will cease to hold the status of data controller and will have no involvement beyond May 2024.</td><td>March 2030 (with annual review).

Reports and aggregated data may be stored by DfE until 2030 to help inform policy/commissioning decisions. This is appropriate as it is non-personal data.</td></tr>
</table>
</td>
</tr>
<tr>
<td></td>
<td>Secure:
• How will the data be secured and kept safe?</td>
<td>In DLUHC/DfE the data will be stored on SharePoint (Microsoft 365). This is a secure platform which will be accessible to a restricted group of individuals who will be briefed on the sensitivity of the data. The individuals granted access will be limited to several analysts in DfE and the Supporting Families team in DLUHC (until May 2024).</td>
</tr>
</table>

	Accountability • How will demonstrate responsibility for what you do with personal data? • What measures and records are in place or will be put in place to demonstrate your compliance?	Compliance: - In our quarterly review sessions with IFF Research we will monitor their adherence to the security and processing standards outlined in Schedules 9 and 11 (respectively) of the contracts with IFF Research. - The risks and mitigations set out in this DPIA will be recorded in the Supporting Families risk register and escalated using our RADAR log. Complaints process: - LAs will be able to contact us with any feedback/complaints through the families inbox (families.team@levellingup.gov.uk), regional meetings, area calls with regional leads and via Slack. - LAs will also be able to contact IFF Research using their shared area engagement inbox and through the regional liaison contacts. - Families will be able to raise concerns/complaints directly using the families inbox (same as above) which will be signposted on the privacy notice on GOV.UK. - Additionally, the Joint Controllers will be able to raise complaints to IFF Research, if their data processing does not been the standard required and set out in the contract.
Transparent **UK-GDPR Article.12, 13 & 14**	**Transparent / Duty to Inform:** • How will data subjects (e.g. customers, staff) be made aware of what is happening to their data? • Do individuals have an opportunity and/or right to decline to disclose or share their information?	Families that have an Early Help assessment, or an equivalent CSC assessment, have all been made aware that their data will be shared with the Supporting Families team for the purposes of programme evaluation. This is achieved by LA privacy notices which are held on their websites and explains the local processes for the withdrawal of consent. These privacy notices outline the UK General Data Protection Regulation rights of the data subject to: - Object and restrict further processing of your data, - Request your data to be rectified if it is inaccurate or incomplete, - Not be subject to automated decision-making including profiling, where applicable. Although, data subjects are already informed that data will be used for evaluation we will ask LAs to update these privacy notices (held on websites and provided by workers to families on request) to explain that this will be shared with the national team on a pseudo-anonymised basis for the purposes of this collection. • We previously did this for the National Impact Study evaluation, so there is precedent, and areas have taken part in a similar exercise before. • This is in line with the right to be informed set out in Article 12(1), and Articles 13 and 14 of the GDPR.

		DLUHC will also have a Privacy Notice on GOV.UK which covers the rights of the data subject as outlined above.
Subject Access UK- GDPR Article.15	Subject Access Requests: • Will the personal data be extracted and provided to the data subject through usual business processes? • If not how will subject access requests be managed?	As joint data controllers, DLUHC and DfE will have a process of responding to SARs. - Until May 2024, DLUHC will have responsibility for responding to SARs. - This responsibility will be transferred to DfE upon the planned MOG change. Process until May 2024: "To ask for personal information held about you by DLUHC, please contact the Knowledge and Information Access team using the contact details below. Knowledge & Information Access Team Department for Levelling Up, Housing and Communities 2nd floor NW, Fry Building 2 Marsham Street London SW1P 4DF United Kingdom or dataprotection@levellingup.gov.uk When you write to us to access your personal information you must provide the following: - confirmation of your identity: a copy of your passport, full driving license or birth certificate (please do not send original documents) - confirmation of name and address: a copy of your full driving license, a copy of a recent utility bill, bank or credit card statement, pension or child benefit book (or similar official document which shows your name and address) - if you are writing on behalf of someone else, a signed declaration from the person you are acting for indicating that they have asked you to make an application on their behalf If possible, you should also send:

		- details of all addresses you have used in previous correspondence with DLUHC, including email addresses (if applicable) so that we can search our systems - any information that might help us in locating the information in which you are interested (this might include details of any contacts you have had with DLUHC at any time, and details of why you think we will hold information about you) - Once we receive all the above information, DLUHC has one month within which to respond to your request. This may be extended by up to 2 months in complex cases. - DLUHC does not keep records of individuals as a matter of routine and if you have had no previous dealings with the department, it is unlikely that we will hold information about you. If, however, you have reason to believe that we do hold information about you, please indicate any contacts or dealings you have had with the department in the past, so that we can locate anything that is relevant." Process after May 2024: "To make a subject access request you can use the DfE contact form. Alternatively, subject access requests can be made in writing and be posted to: Data Protection Officer Department for Education (B2.28) 7 & 8 Wellington Place Wellington Street Leeds LS1 4AW
Data Transfers UK-GDPR Article.44 and 45	Data Transfers: • Will the data be held or transferred outside the UK? • If yes – where will it be held or transferred to? • Will the data be held or transferred inside the EEA? • Will the data be held or transferred outside the EEA? • If yes - where will it be held or transferred to?	The data will not be held or transferred outside the UK. The data will be processed and stored in Microsoft Azure centres in the UK regions.

	• If yes, what processes will be place to ensure it is adequately protected?	
Lawfulness UK-GDPR Article.6	Lawfulness: Which of the following conditions will apply to how the data is used? • Public Task - Fundamental to the performance of a government function?	The use of data in this way will be justified by the substantial public interest in protecting vulnerable children and families. This is in line with Article 6(1)(e) and Article 9(2)(g) of UK General Data Protection Regulation (GDPR). In order to rely on article 6(1)(e), article 6(3) requires there to be a separate legal basis laid down in law to justify the processing. DLUHC is relying on its SoS common law powers to justify this processing.
Special Categories of Personal Data UK-GDPR Article.9	Special Categories: • Will any of the data that will be processed include information about individuals': race, ethnicity, health, religion, sex life/orientation, political views, Trade Union membership, genetic or biometric data? • Which of the following options will be applied to that processing? • Substantial public interest?	Pseudonymised data will be collected on the following special category data fields: - 3.3 Child and/or parent/carer require support with learning disabilities, neurodiverse conditions and/or physical health needs that affect the family (e.g., long-standing health conditions requiring management, physical disabilities requiring adaptations) - 3.2 Adult needs support with their mental health. - 3.1 Baby/child needs support with their mental health. This is in substantial public interest as it will enable us to identify any specific issues facing these individuals/families. At a cohort level, information on gender identity, age and ethnicity will be collected but this is not at an individual level (see Annex B).
Criminal Convictions & Offenses UK-GDPR Article.10	Criminal Convictions: • Will the information include personal data about offences/convictions? • If yes, what information will be processed? why is this needed? • Do you have a legal reason to process it and use it?	There will be pseudonymised data on criminal offences/convictions collected. The data processed will be the response to the data field: - 7.1 Adult (18+) involved in crime and/or ASB (at least one offence/arrest/named as a suspect/ASB incident) in the last 12 months. - 7.3 Young person (u18) involved in crime and/or ASB (at least one offence/arrest/named as a suspect/ASB We will only collect data on the presence/absence of evidence to support these statements. There will be no detail on the actual nature of offences collected.

Right to Restriction UK-GDPR Article.18	Restriction: • What processes will be in place to manage requests to restrict processing?	In the event a family wishes to restrict processing, the Family ID of the family in question would be shared by the LA to DLUHC and IFF Research. The restrictions on processing would then be put in place.
Automated Decision Making UK-GDPR Article.22	Automated Decision Making: • Will the processing involve automated decision making affecting a person? • If yes, please explain the circumstances. • What processes will be in place to manage objections to automated decision-making?	No
Joint Controllers & Processors UK- GDPR Articles.26 to 30	Data Sharing / Contracts: • Will the data be shared with other business units/teams/parts of the Department/ Organisation? • If yes how will the data be shared/disclosed? • Will the personal data be shared with an external organisation? - OGD? - Supplier? - Third party? • What kind of arrangement will be in place to covers this? - Contract? - Data Sharing Agreement? - Memorandum of Understanding? - Other?	The joint controller relationship between DfE and DLUHC will be covered by a data sharing Memorandum of Understanding (MOU) which outlines the roles and responsibilities of each of the departments. - This will be in place until the MOG move planned for May 2024. At that point, DfE will take on sole responsibility as Controller for the DSA with Local Authorities below. The data shared by Local Authorities to DLUHC will be covered by a Data Sharing Agreement. - These will be completed by LA data governance leads and signed where they are willing to share this data. The data will be shared with supplier IFF Research (data processor). - This is covered by the Early Help and Supporting Families National Insights data collection contract. The aggregated data and statistical outputs may be shared with OGDs, but this will not include any personal data.

	• How will the data be shared/disclosed with the other organisations?	
Security UK-GDPR Article.32	Security: • Will the data be encrypted? • Will the data be pseudonymised? If so, how? • How will the data be protected against risk of loss, confidentiality, availability, and integrity? • Will back-ups be taken? • Will the security of the system/premises be trailed regularly? • Will the security of the system be required to have any formal accreditation or independent certification (e.g. ISO27001)? • What processes will be in place to determine who will have access to the data/system? • What level of security clearance will be required to access the system/data? • What data protection/security training will users of the data/system be required to have? • How will access to the system be granted?	Cyber have assured IFF Research as a supplier and have provided separate assurance for the bespoke web portal which IFF will use to collect data from LAs. The assurance assessment can be found in Annex C. Egress, the file exchange software used as part of this project, is the DLUHC Cyber Security preferred software for secure file exchanging. Egress utilises identity-based AES 256-bit encryption using FIPS 140-2 approved cryptographic libraries. The bespoke Portal uses TLS1.3 to encrypt data in transit between the web application and end user device. Within IFF Research data transfers are via secure channel HTTPS and TLS over TCP to prevent man-in-the-middle attacks during communication with Azure services. Data is transmitted between Azure services and the on-premises web application through the utilisation of Power BI. PBI requires all incoming HTTP traffic to be encrypted using TLS 1.2 or above. Any requests attempting to use the service with TLS 1.1 or lower will be rejected. IFF are ISO27001 certified. Operational management of the service is in line with this standard. All IFF staff undergo a Right to Work check as well as a Criminal Record Declaration. For government officials in DLUHC and DfE, all those with access to this data will need to be at least CTC/Level 1B national security level vetted. The risk register used will be RADAR log for the Supporting Families programme.

	• What information asset register and/or risk register will the data be recorded on?	

Other privacy legislation and policies -		Comments
Privacy & Electronic Communications Regulations 2003	Technology Does the project/policy/initiative involve new or inherently privacy-invasive electronic communications technologies? For the avoidance of any doubt, 'communication' means any information exchanged or conveyed between finite parties by means of a public electronic communications service, but does not include information conveyed as part of a programme service, except to the extent that such information can be related to the identifiable subscriber or user receiving the information.	
	Communication providers Does the project/policy/initiative involve new or existing communication providers? For the avoidance of doubt, 'communication providers' means a person or organisation that provides an electronic communications network or an electronic communications service.[1]	
	Communication subscribers / users Does the project/policy/initiative involve new or existing communication subscribers / users? For the avoidance of doubt, 'communication subscriber' means a person who is a party to a contract with a provider of public electronic communication services for the supply of such services. 'User' means an individual using a public electronic communications service.	
Human Rights Act 1998	**Article 2: Right to Life** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to life, subject to any limitations as may be defined in Article 2(2)? For the avoidance of any doubt, the limited circumstances are that in peacetime, a public authority may not cause death unless the death results from force used as follows: • Self defence or defence of another person from unlawful violence; • Arresting of someone or the prevention of escape from lawful detention; and A lawful act to quell a riot or insurrection	

[1] Source – Communications Act 2003

	Article 3: Prohibition of Torture Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not subjected to torture or inhuman or degrading treatment? For the avoidance of doubt, this is an absolute right.	
	Article 4: Prohibition of Slavery or Forced Labour Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not held in servitude or forced to perform compulsory labour? For the avoidance of doubt, this is an absolute right; the following are excluded from being defined as forced or compulsory labour: • Work done in ordinary course of a prison or community sentence; • Military service; Community service in a public emergency; and normal civic obligations.	
	Article 5: Right to Liberty and Security Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not deprived of their liberty subject to certain limitations? For the avoidance of doubt, the following limitations apply when a person is: • Held in lawful detention after conviction by a competent court; • Lawfully arrested or detained for non-compliance with a lawful court order or the fulfilment of any lawful obligation; • Lawfully arrested or detained to effect the appearance of the person before a competent legal authority; • Lawfully detained to prevent the spreading of infectious diseases; • Lawfully detained for personal safety (applies to persons of unsound mind, drug addicts etc.); and Lawfully detained to prevent unlawful entry into the country or lawful deportation from the country.	
	Article 6: Right to a Fair Trial Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to have a public hearing within a reasonable time by an independent and impartial tribunal established by law? For the avoidance of doubt, the hearings included are both civil and criminal proceedings that are not specifically classified as hearings that must be heard 'in camera', i.e. closed to the public	

	Article 7: Right to no Punishment without Law Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to not be prosecuted for a crime that was not, at the alleged time of commission, constitute a criminal offence under national or international law? For the avoidance of doubt, this is an absolute right	
	Article 8: Right to Respect for Private and Family Life Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to respect for privacy in terms of their private and family life subject to certain qualifications? For the avoidance of doubt, the qualifications are: • Legal compliance; • National security; • Public safety; • National economy; • Prevention of crime and disorder; • Protection of public health and morals; Protection of rights and freedom of others.	
	Article 9: Right to Freedom of Thought, Conscience & Religion Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to freedom of thought, conscience and religion subject to certain qualifications? For the avoidance of doubt, the qualifications are: • Unless prescribed by law; • In interest of public safety; • Protection of public order, rights or morals; Protection of rights and freedoms of others.	
	Article 10: Right to Free Expression Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to hold opinions and express their views singly or in dialogue subject to certain qualifications? For the avoidance of doubt, the qualifications are as set out in Article 9 above.	

	Article 11: Right to Freedom of Assembly & Association Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to freedom of peaceful assembly and association with others subject to certain qualifications/ For the avoidance of doubt, the qualifications are as set out in Article 9 above.	
	Article 12: Right to Marry Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to marry and found a family subject to certain restrictions? For the avoidance of doubt, the restrictions are regulated by law so long as they do not effectively take away the right, e.g. age restrictions apply	
	Article 14: Right to Freedom from Discrimination Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be treated in a manner that does not discriminate the individual from others subject to certain restrictions? For the avoidance of doubt, this right is restricted to the conventions as set out in the European Convention of Human Rights 1950; the grounds for discrimination can be based on: • Sex • Race • Colour • Language • Religion • Political persuasion • Nationality or social origin • Birth • Other status.	
	Articles: 16 / 17 / 18 Not relevant for the purpose of this questionnaire	

Regulation of Investigatory Powers Act (RIPA) 2000	Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies to intercept communications? (For the avoidance of doubt, 'communications' is defined in RIPA Part V, section 81(1)). Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies pertaining to the acquisition and disclosure of data relating to communications? Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies pertaining to the carrying out of surveillance? Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies pertaining to the provision of the means by which electronic data protected by encryption or passwords may be decrypted or accessed? Does the project/policy/initiative undertake any of the functions of the Security Service, the Secret Intelligence Service or the Government Communications Headquarters?	

RISK ASSESSMENT

Risk Event, Cause & Impact	Risk Owner	Inherent Rating	Proximity	Mitigation	Target Rating	Risk has been recorded
(e.g. there is a risk that x, caused by y, will have the effect of z)	*(the individual accountable for the risk)*	*(assessment of risk with no mitigation or control in place. Use matrix in appendix 2)*	*(when do you expect the risk to occur?)*	*(actions to be taken to treat the risk)*	*(the rating to which the risk should be reduced if mitigations are actioned)*	*(Yes/No)*
Data breach where personal data is lost, leaked, or made public by mistake.	[redacted]	10	Any time until destruction date (March 2025)	Local authorities already working with vulnerable children and families within early help are experienced in protecting and handling sensitive data to a high standard and should have safeguards in place to prevent data breaches. The transfer of the data will be made using a secure platform so minimises a risk of data loss at the point of transfer from the local authority to the supplier. Once the data is with supplier and then with DfE and DLUHC, the data will be held securely and is not being passed onto another organisation so minimises the risk of the data being leaked.	5	

				The use of pseudonymised data prevents the dataset from being identifiable without access to LA systems. All DfE and DLUHC staff are trained on the use of data and Information Governance principles.		
Harm or distress occurs to data subjects due to some families becoming identifiable due to the specific details of their circumstances and small numbers on reports	K[redacted]	4	Every 6 months (once the collection reports have been produced/distributed)	A minimum number of families threshold will be placed on all reports so that if the number drops below a certain threshold (five cases), this will not be displayed. Mitigated through use of pseudonymised data and the collection of a breadth of data. Due to the breadth of the data collected and the pseudonymised nature of these data it is highly unlikely that data will be small enough or contain any information that would enable identification without concurrent access to LA systems. The smallest LA works with circa 50 families per year, which means the smallest submission from one LA we could expect to receive will be 100 families.	2	
Data subjects objecting to the use of data, and/or negative press reporting	[redacted]	4	Any time	Reporting will be at a high level. Only high-level national reports will be published as evaluation data only. Individual LA data will not be published. There is precedence for this level of data being published at a cohort level in Childrens Services (Children's Social Care data) and for evaluation of the Supporting Families programme (the National Impact Study).	2	
Data subjects' rights are not upheld.	Kirby Swales	3	Any time	In the event a family wishes to restrict processing, the Family ID of the family in question would be shared by the LA to DLUHC and IFF Research. The restrictions	1	

				on processing would then be put in place. These processes are in place to uphold the rights of the data subjects, in addition to the departmental and LA privacy notices to inform the data subjects on the planned use of their data.		
Data subjects being unaware of the purpose of data use.	[redacted]	3	Any time	We will ask LAs to update their privacy notices (held on websites and provided by workers to families on request) to explain that this will be shared with the national team on a pseudo-anonymised basis. We will also have a DLHUHC/DfE privacy notice on GOV.UK.	1	
Cyber assurance related risks: The Cyber assurance assessment of IFF research and the bespoke data collection platform they will be using to conduct the EH data collection identified three key risks. Firstly, there is a risk that due to the urgency of the work that the supplier will commence work before the DPIA is in place. Secondly, here is a further risk that the FileXchange software could be unacceptable to DLUHC for use. Finally, there is a low to medium risk that any attacks against the bespoke portal won't be picked up for nearly a month as the logs are only reviewed monthly.	[redacted]	4	Any time	We have delayed the initial collection to allow adequate time to consult the DP team to ensure the DPIA and DSA is sufficient for a collection of this size and sensitivity. Additionally, we have adopted the cyber recommended software Egress as opposed to FileXchange, which is DLUHC approved and involves no overseas third-party data transfer. Finally, we have increased the review frequency to once per week as recommended by the cyber assurance team.	2	

The dataset is accessed without a legitimate purpose and/or modified	[redacted]	4	Any time	Through Egress access to the data will be role based, and controlled by the Zone owner (DLUHC/Becky Leader). There will be two individuals in IFF appointed as Zone administrators, who will have the ability to download/edit/delete data. Zone administrators will only be able to download this data twice before it expires. Zone users will be able to create links for data upload but will not be able to download any of this data. On the SharePoint, access will be role based and password controlled.	2	
The quality of the data is poor/inaccurate	[redacted]	3	Any time	IFF will use their portal's bespoke data validation tool to correct data issues/inaccuracies. In the event there is an error in the Family ID/any other data field, this will be detected by the data validation reporting tool IFF Research have built into their online submission portal. After the initial collection window (approximately 3 weeks), there will be a 2-week data checking period. During this time, IFF will review the data validation reports for each LA submission and will raise any queries/errors identified in the data to rectify any errors. This process will occur on a rolling basis, following each collection.	1	
Inadequate contractual controls with Processor				We have weekly catch-up calls with our provider, and weekly progress updates during the collection periods (as per the contract). Additionally, within the contract, we have a process for contract termination in the event of poor performance/non-adherence to data protection arrangements (schedule 11 of contract).		

SIGN OFF AND RECORD OUTCOMES

ITEM	NAME/DATE	NOTES
Risks Approved by:		Integrate actions back into project plan, with date and responsibility for completion
Risks have been transferred to the project plan and appropriate risk register for continuous monitoring and review		
DPO advice provided:	**26/09/2023**	

Summary of DPO advice if applicable:

I have reviewed this version of the DPIA and left some comments, and amendments in track changes. This is clearly a data processing activity that, even with mitigations in place, will be "high risk" should any adverse incidents occur. The justification for processing, for obtaining a clear national picture on outcomes to inform decision-making, appears clearly justified.

Perhaps the biggest risk to this processing is outside of DLUHC/DfE control – this will be ensuring the LAs participating, agree on a consistent suitable vires for sharing their data extract at source, which is not easily covered for in legislation – however their broad "subsidiary powers" as the local level of government should cover this. I would advise against promoting the general power of competence (GPC) that LAs have as the vires, as this does not appear suitable for use in research work (in terms of reasonable expectations of data subjects involved) and some LAs have resisted its use in other data sharing proposals relating to Homelessness – this risk should be avoided here.

The security of data held apparently by IFF themselves i.e. outside of the Dept's Azure estate will require a rigorous Information Assurance assessment by Cyber Security, which appears to have been carried out. I am reassured by the statement in this DPIA that the mitigation of reviewing IFF's security and use arrangements of the data will be done every 3 months – it will be important to actually carry this out though. Strong contractual controls will also be important to put in place with the Processor alongside vendor due diligence.

I have suggested some additional risks for the risk register, most notably on data quality.

As this evaluation will include high risk processing, the security controls applied should be sufficiently robust for all parties including DLUHC and DfE. It is recommended that the department cyber security team must be content with the transfer and storage mechanisms proposed. I have already expressed that the use of CSV files, (for example, the possibility of the file being sent to the wrong person) is not recommended wherever disclosure of data may occur. I note the team have explored the possibility of using a departmentally approved transfer solution such as Egress rather than the supplier software, though my point here remains. Given the sensitivity of the information within the pseudonymised data set, I would suggest the project team explore any

further technical control measures possible to protect personal data in the event of a security breach. Further consideration will need to be given to ensure that 'copies' of the dataset are not kept, otherwise heightening the risk of a data breach. Access control provisions will also need to be strictly managed and controlled. Again, I advise as above that cyber security will need to be content with the controls.

Significant consideration has been given to the roles and responsibilities for this proposed processing, noting the anticipated Machinery of Government (MOG) changes which are planned for April (?) 2024. It is considered that both DLUHC and DfE have played a significant role in determining purpose and means of processing, and it is likely that both organisations are therefore joint controllers in respect of the processing to take place prior to MOG changes. It has been clarified that following this point, DLUHC will have no role to play and cease any involvement in the Early Help programme. In this case, DLUHC will cease to be a joint controller and DfE will become sole data controller immediately following MOG changes. DLUHC and DfE colleagues are in agreement that this is the correct designation of 'data controller' roles.

An MoU will need to be agreed by DLUHC and DfE setting out joint controllership arrangements. It is also advised that joint controller relationships do not always follow a uniform separation of responsibilities. That is, one controller may 'lead' on a certain area of compliance. In particular, I have already advised that DLUHC may wish to explore the identification of a single point of contact to handle subject rights requests pre-MOG changes, but note that a data subject will be able to exercise their rights against both controllers. I note the project team have actioned this.

IFF are acting as a data processor, and it is recommended that the contractual relationship with IFF reflects the now known joint-controller relationship between DLUCH and DfE. There had been some confusion over the role of IFF in subject rights requests, and I would recommend clarifying this process with IFF.

There has been some discussion as to whether and at what point data may be considered truly anonymised. The processing described in this DPIA is that of pseudonymised data, and should therefore be handled as personal data. I have provided a copy of the ICO guidance on anonymisation which should be considered further if there are to be any attempts to anonymise the dataset. For example, there is some mention of maintaining anonymised data beyond the 2025 retention date, but this will need to be considered further against a robust standard of anonymisation. In any case, this will not be a DLUHC obligation but that of DfE.

DPO advice accepted or overruled by:		If overruled, you must explain your reasons below

Comments:

DLUHC:

DPO advice has been provided over a period of engagement with the project team. This is potentially high risk processing, which will include very sensitive information about potentially up to 3 million individuals across a wide geographic area (up to 152 upper tier Local Authorities in England), likely to include some vulnerable individuals including children.

As already discussed, there will need to be a data sharing agreement in place with Local Authorities (LAs) who are independent data controllers here. It would be worth exploring whether this could include the planned data sharing with DLUHC and DfE as joint-controllers, and also covering the sharing

solely with DfE post-MOG changes. The DPIA identifies a vires that LAs *may* wish to rely on for the processing, though this will of course be the prerogative of each LA as an independent data controller. I have already advised on this and repeat my advice here that it would be useful to consider upfront whether there will be uniformity in LAs relying on this (or another) vires.

APPENDIX 1 – DETERMINING THE RISK LEVEL

Evaluation of likelihood of risk occurring:

Likelihood score	1	2	3	4	5
Description	Very Unlikely	Unlikely	Possible	Likely	Very Likely
Indicative Frequency	Will probably never happen	Not anticipated to happen, but possible	Might happen or recur occasionally	Will probably happen or recur, but not persistently	Almost certain to happen or recur, possibly frequently

Evaluation of impact should risk occur:

See the Risk Management Framework for further guidance on impact level descriptions by Risk Category.

Impact Score	1	2	3	4	5
Description	Very Low	Low	Medium	High	Very High
Indicative Impact	Unlikely to have any impact	May have an impact	Likely to have an impact	Highly probably it will have a significant impact	Will have a major impact

IMPACT LEVEL	PROBABILITY (that the risk will occur during the lifetime of the activity)				
	<10%	10-35%	35-65%	65-90%	90>%
	Very Unlikely 1	Unlikely 2	Possible 3	Likely 4	Very Likely 5
Very High 5	5	10	15	20	25
High 4	4	8	12	16	20
Medium 3	3	6	9	12	15
Low 2	2	4	6	8	10
Very Low 1	1	2	3	4	5

Appendix 4

RACI Matrix

Role and Responsibilities

Responsible **A**ccountable **C**onsulted **I**nformed

The responsibility assignment matrix below clarifies and defines the roles and responsibilities you need to allocate/consider when undertaking a DPIA

ROLES	Project Lead	Project Team	IAO	Data Protection Officer (DPO)	Security - IT	Procurement	Suppliers/ Processors	Risk Owner	External stakeholders (staff members/ members of public)	Data Protection Team	Legal Services
Completing the DPIA	A			I						I	
Input Required	C	C	C	C	C	C	C	C	C	C	C
Approving the DPIA			A					A (risks)			
Identifying Risks	C	C	C		C	C	C	C	C	C	C
Mitigating Risks	C	C	C		C	C	C	C	C	C	C

R Assigned to complete the DPIA

C An adviser, stakeholder, or subject matter expert who is consulted before a decision

A Has final decision-making authority and accountability for completion or action

I Must be informed after a decision or action

If you have carried out a DPIA that identifies a high risk and you cannot do anything to reduce it, prior consultation with the ICO is required under UK GDPR. You cannot go ahead with the processing until you have consulted with the ICO, consultation will be undertaken by the data protection team. The focus is on the 'residual risk' after you have taken any mitigating measures. If your DPIA identified a high risk but you have done things to reduce the risk so it is no longer high, you do not need to consult with the ICO.

Annex A Data fields – Case Level collection:

LA
LA family ID
Duplicate ID to be removed
Lead practitioner
Does a child in the family have an EHCP?
Date notification/referral received
Date assessment started
Date case closed
Reason for closure
Worked with family hub?
Case eligible for Supporting Families?
Case claimed for Supporting Families?
If claimed, which quarter was it submitted for claim?
1.1 Average of less than 90% attendance (inclusion of authorised absence is optional) for 2 consecutive terms
1.2 Average of less than 50% attendance unauthorised and authorised for 2 consecutive terms
1.3 Not able to participate and engage with education – motivation, emotional regulation and behaviour difficulties, risk of, or subject to, exclusions, concerns around suitability of Elective Home Education, child is off-roll and not receiving an education otherwise, risk of NEET
1.4 Child's special educational needs not being met
2.1 Expectant or new parent/carers who require additional or specialist support (e.g., young parents, parents who have been in care, parents with learning needs)
2.2 Child's (0-5 yrs) physical health needs not met (e.g., immunisations not up to date, concerning accidental injuries, dental hygiene)
2.3 Child's (0-5 yrs) developmental needs not being met (e.g., communication skills/speech and language, problem-solving, school readiness, personal, social and emotional development
3.1 Baby/child needs support with their mental health
3.2 Adult needs support with their mental health
3.3 Child and/or parent/carer require support with learning disabilities, neurodiverse conditions and/or physical health needs that affect the family (e.g., long-standing health conditions requiring management, physical disabilities requiring adaptations)
4.1 An adult has a drug and/or alcohol problem
4.2 A child or young person has a drug and/or alcohol problem

5.1 Parent / carers require parenting support
5.2 Harmful levels of parental conflict i.e., when it is frequent, intense or poorly resolved
5.3 Child / young person violent or abusive in the home (to parents/carers or siblings)
5.4 Unsupported young carer or caring circumstances changed requiring additional support
6.1 Emotional, physical, sexual abuse or neglect, historic or current, within the household
6.2 Child going missing from home
6.3 Child identified as at risk of, or experiencing, sexual exploitation
6.4 Child identified as at risk of, or experiencing, criminal, or pre-criminal, exploitation (e.g., county lines, radicalisation)
6.5 Child experiencing harm outside of the family (e.g., peer to peer abuse, bullying, online harassment, sexual harassment/offences)
6.6 Child identified as at risk of, or being affected by radicalisation
7.1 Adult (18+) involved in crime and/or ASB (at least one offence/arrest/named as a suspect/ASB incident) in the last 12 months
7.2 Young person (u18) at risk of crime – including gangs, serious violence and weapons carrying, or involved in harmful risk-taking behaviour
7.3 Young person (u18) involved in crime and/or ASB (at least one offence/arrest/named as a suspect/ASB
8.1 Family affected by domestic abuse or inter-personal violence and abuse - historic, recent, current or at risk (victim)
8.2 Adult in the family is a perpetrator of domestic abuse
8.3 Child currently or historically affected by domestic abuse
9.1 Families who are in local authority temporary accommodation and are at risk of losing this
9.2 Families not in suitable, sustainable housing and/or threatened with eviction /at risk of homelessness
9.3 Young people aged 16/17 at risk of, or who have been, excluded from the family home
10.1 Adult in the family is workless
10.2 Family require support with their finances and / or have unmanageable debt (e.g., rent arrears)
10.3 Young person is NEET
1.1 Sustained good attendance
1.2 Sustained improvement from very poor attendance
1.3 Improved engagement with education (e.g., pupils no longer on report, reduction/no detentions)
1.4 Family happy that special educational needs being met, and school / early years settings are providing adequate support.
2.1 Families are engaged with appropriate support that can be seen to be making a difference; capacity for positive, effective parenting increased and they are accessing and engaging with services
2.2 Child's physical health needs met, better awareness of home safety and accident prevention

2.3 Child's developmental needs are being met, allowing them to make progress at a pace that is suitable for them
2.3 Child has the right support in place to make progress.
2.3 Children and young people with probable/confirmed prenatal alcohol exposure and significant physical, developmental or behavioural difficulties are referred for FASD assessment
3.1 The baby/child's mental health and/or wellbeing has improved
3.1 Family/parents/carers feel better equipped to manage the child's mental health and well-being.
3.1 Early attachment relationships are improved/parents feel bonded to baby
3.2 The adult's mental health and/or wellbeing has improved
3.2 Family/parents/carers feel better equipped to manage the adult's mental health and well-being
3.3 Physical health needs are being well-managed and family have sufficient / the right support in place
4.1 Adult reducing / abstaining from substance use (as measured by rescreening)
4.1 Adult better equipped to manage the substance use. Adult understands the risk / impact of the substance use on the family and children and is able to promote safety and implement actions to reduce harm.
4.1 Assessment undertaken with child/family to determine impact of substance misuse upon child and child is benefitting from appropriate support (e.g., whole-family substance misuse work, affected-by service, young carers service, appropriate therapeutic support)
4.2 Child reducing / abstaining from substance use
4.2 Family / Child better equipped to manage the substance use and find alternative coping strategies, and understands risk / impact of substance use
5.1 Parent / carer demonstrates improved, positive parenting (e.g., improved parent / child interactions; positive attachment etc)
5.2 No harmful parental conflict and improved family relationship
5.2 Parents /carers understand the impact of the conflict on the children
5.3 No harmful child to adult or sibling abuse.
5.3 Child is better equipped to understand behaviours, develop coping mechanisms and self-manage.
5.3 Parent/carers better equipped to manage child's behaviour and relationship improved
5.4 Unsupported young carer now supported, including with change in caring circumstances
6.1 No longer abuse or neglect in the household
6.1 Child / family has been supported following abuse/neglect and has strategies to manage going forward
6.1 Children are in an emotionally and physically safe environment
6.2 Child no longer going missing
6.2 Child/family has been supported following missing episodes

6.3 Child not experiencing sexual exploitation
6.3 Child has been supported following sexual exploitation
6.3 Partners worked alongside child/family to manage risk of sexual exploitation
6.4 Child not experiencing criminal or pre-criminal exploitation (e.g., radicalisation)
6.4 Child has been supported following criminal exploitation
6.4 Partners worked alongside child/family to manage/reduce risk of criminal exploitation
6.5 Child no longer experiencing harm
6.5 Child confident in reporting and being taken seriously
6.5 Partners worked alongside child/family to develop strategies and support them to cope with, and respond to, abuse / harm outside of the home and to keep themselves safe.
6.6 Child not affected by radicalisation
6.6 Child has engaged with, and benefitted from, relevant support
6.6 Partners worked alongside child/family to manage or reduce risk
7.1 (7 or fewer incidents in 12 months) Adult no longer involved in crime
7.1 (8 or more incidents in 12 months) Adult demonstrates at least a 50% reduction in incidents of crime
7.2 Young person not involved in crime or anti-social behaviour.
7.2 Young person supported to better manage risks of becoming involved with crime, through accessing relevant services and fully engaging in this process.
7.3 (4 or fewer incidents in 12 months) Young person no longer involved in crime
7.3 (5 or more incidents in 12 months) Young person demonstrates at least a 50% reduction in incidents of crime, provided none of these are a severe offence as defined by the list of severe offences.
7.3 Young person supported to better manage risks of becoming further involved with crime, through accessing relevant services and fully engaging in this process.
8.1 Domestic abuse has stopped
8.1 Victim has a clear safety plan in place and knows how to seek help
8.1 Victim has received (or is receiving) appropriate support
8.2 Domestic abuse has stopped
8.2 Perpetrator understands crime, and impact on the victim(s) (including children), and is engaging with perpetrator support
8.3 Domestic abuse has stopped
8.3 Child feels safe at home

8.3 Child has received appropriate support
9.1 Family no longer at risk of losing temporary accommodation and have sustained temporary accommodation for 6 months or have moved into settled housing.
9.2 Family no longer at risk of eviction and/or in suitable and sustainable housing for 6 months
9.3 Young person no longer at risk of homelessness – remains with or is returned to family or wider family network with support available for 6 months
10.1 Adult is in work
10.1 Adult has made progress to work (e.g., gained a qualification, completed training, volunteering, is attending job interviews)
10.2 Family feels able to manage their finances
10.2 Debt is being managed or has been resolved
10.3 Young person is in education, employment or training

Annex B: Data fields - Demographic collection:

Local authority
Cohort type
Number of cases
Date cases from
Date cases to
Number of individuals in cohort
Number of adults
Number of children
Number of children age 0-4
Number of children age 5-6
Number of children age 7-10
Number of children age 11-13
Number of children age 14-15
Number of children age 16-17
Number of adults age 18 -24
Number of adults age 25-29

Number of adults age 30-39
Number of adults age 40-49
Number of adults age 50-59
Number of adults age 60+
Number of age unknown
Number of unborn children
Number of Male
Number of Female
Number of other gender categories
Number of "Gender data not collected"
Number of "Gender data refused"
Ethnicity group - Number of Asian or Asian British
Ethnicity - Number of Bangladeshi
Ethnicity - Number of Indian
Ethnicity - Number of Chinese
Ethnicity - Number of Pakistani
Ethnicity - Number of Any other Asian Background
Ethnicity group - Number of Black, Black British, Caribbean or African
Ethnicity - Number of African
Ethnicity - Number of Black Caribbean
Ethnicity - Number of Any other Black Background
Ethnicity group - Number of Mixed or multiple ethnic groups
Ethnicity - Number of Any other Mixed Background
Ethnicity - Number of Mixed White and Asian
Ethnicity - Number of Mixed White and Black African
Ethnicity - Number of Mixed White and Black Caribbean
Ethnicity group - Number of White
Ethnicity - Number of Traveller- Irish Heritage
Ethnicity - Number of White British
Ethnicity - Number of White Irish
Ethnicity - Number of Any other White Background
Ethnicity - Number of Roma/Roma Gipsy
Ethnicity group - Number of Other ethnic group

Ethnicity - Number of Arab
Ethnicity - Number of Any other Ethnic Group
Ethnicity - Number of Information not obtained
Number of "Ethnicity data refused"

Annex C: Cloud Security Assessment Matrix (Cyber Assurance)

(Notes: The 14-cloud security questionnaire must be presented to the cloud service provider to complete. Details of the completed questionnaire should be inserted in this section - To be completed by Information Assurance lead)

Principles	Question	Supplier's Response & Evidence	Compliance	Comments
1: Data in transit protection User data transiting networks should be adequately protected against tampering and eavesdropping	*1.1 How is data in transit protected between end user devices and the service?*	Egress [redacted]		
	1.2 How is data in transit protected internally within the service?	[redacted]		
	1.3 How is data in transit protected between the service and other services (e.g. where APIs are exposed)?	All data in transit is via TLS 1.2/3 between all services.		
2: Asset protection and resilience: User data, and the assets storing or processing it, should be protected against physical tampering,	2.1 Please list all countries where our data will be stored, processed and managed.	The data will be processed and stored in Microsoft Azure centres in the UK regions.		
	2.2 Please state the legal jurisdiction within which you, as a service provider, operate.	England and Wales		

loss, damage, or seizure.	2.3 Please outline the physical security measures you employ at the data centres hosting the service.	On-premise, the data centre is contained within locked, access and environmentally controlled server room located within our London Office domain. Only authorised staff are permitted the entry code. Azure Data Centre physical security - Physical security of Azure datacenters - Microsoft Azure | Microsoft Learn		
	2.4 Please describe how storage media containing our data will be protected from unauthorised access.	On-premise, virtual volumes are protected by access control mechanisms and are only accessible by authorised administrators. Physical access is restricted as above. Access to Azure services will be restricted to Azure AD authentication, which is further protected by MFA. Physical access is restricted as the link above.		
	2.5 Please describe how data will be erased when resources are moved or re-provisioned, when they leave the service or when we request it to be erased.	On-premise data is automatically deleted within a certain timeframe. This can be manually achieved on request. Azure based data retention can be customised according to the client preference. This data will be permanently removed once the services are shutdown.		
	2.6 How will storage media which has held customer data be sanitised or securely destroyed at the end of its life?	[redacted] Please see Physical security of Azure datacenters - Microsoft Azure | Microsoft Learn – Section: *Equipment disposal*, for EOL procedures on Azure equipment.		
	2.7 Please describe how you identify all equipment potentially containing our data, credentials or configuration information for the service at the end of its life (or prior to being recycled)?	Please see question 2.6		
	2.8 Please describe how you will ensure that any components	Please see question 2.6		

	containing sensitive data are sanitised, removed or destroyed as appropriate.			
	2.9 Do you ensure that accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker?	[redacted]		
	2.10 What is the service's level of availability? Please outline what measures you take to meet this, including your ability to recover from outages.	[redacted]		
3. Separation between users: A malicious or compromised user of the service should not be able to affect the service or data or another.	3.1 What other types of customer will we share the cloud platform with?	The service will be shared with no other customers.		
	3.2 Please describe how the service will provide separation of our data and service from other users of the service.	N/A		
4. Governance framework: The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.	4.1 Do you have a governance framework and processes for the service?	IFF are ISO27001 certified. Operational management of the service is in line with this standard.		
	4.2 Does this include a clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service? (This is typically someone with the title Chief Security Officer, Chief Information Officer or Chief Technical Officer).	[redacted]		
	4.3 Do you have a documented framework for security governance, with policies governing key aspects of information security relevant to the service?	IFF holds the ISO/IEC 27001:2013 certification. Our information security framework follows the controls as governed by this. Many of the documented controls within our ISMS are applicable to the bespoke IFF Reporting Portal		

	4.4 Are security and information part of your financial and operational risk management reporting mechanisms, ensuring that the board would be kept informed of security and information risk?	IFF operate and maintain a security and information risk register as part of our compliance with ISO27001. Updates on this risk register are fed back to the board at least annually or as required through necessity.		
	4.5 Do you have processes to identify and ensure compliance with applicable legal and regulatory requirements?	All relevant legislative statutory, regulatory, contractual requirements and the IFF's approach to meet these requirements is explicitly identified, documented and kept up to date.		
5. Operational security The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.	5.1 Please describe how you track the status, location and configuration of service components (hardware and software) throughout their lifetime.	On-premise, this server is an asset in our Asset Inventory register and is tracked with this. A data flow map is used to track the movement of the data and their service components within Azure and on-prem.		
	5.2 Please describe how changes to the service are assessed for potential security impact, then managed and tracked through to completion.	A change control procedure is in place to ensure security is considered before each significant change to systems and procedures. This involves an assessment against risks to confidentiality, availability and integrity due to the potential change. Please see section 3.2 Change Management in IFF's Secure operating procedures for IT A12 Secure Operating Procedur		
	5.3 How do you find out about new threats, vulnerabilities and exploitation techniques relevant to the service?	[redacted]		

	5.4 Do you prioritise the implementation of mitigations and track vulnerabilities until mitigations have been deployed?	High and Critical patches for vulnerabilities are applied within 14 days. Vulnerabilities are tracked in bi-weekly security meetings.		
	5.5 What are your timescales for implementing mitigations to vulnerabilities	14 days.		
	5.6 Please describe the level of protective monitoring included with the service.	[redacted]		
	5.7 Does the service generate audit events to support effective identification of suspicious activity?	Please see question 5.6		
	5.8 Does the service include the analysis of these events to identify potential compromises or inappropriate use of the service?	Please see question 5.6		
	5.9 Please describe the incident management processes you have in place for the service for responding to security incidents.	Information Security Incidents, including data breaches, must be reported immediately. Once reported all incidents are logged and classified by the Compliance Manager according to our ISO 27001 Security Incident Reporting Procedure. Incident reports are required to be completed including analysis of the root cause of the incident and an action plan to address the incident and prevent its recurrence.		
	5.10 Do you have pre-defined process in place for responding to common types of incident and attack?	IFF's security incident management plan outlines the steps to be undertaken in the event of a common incident or attack.  A16 Security Incident Manageme		
	5.11 Is there a defined process and contact route for reporting security incidents by consumers and external entities?	If there are any issues experienced by a client they would be invited to communicate via their IFF account manager.		
	5.12 Will you report relevant security incidents to customers?	In the event that a security incident results in compromised client data. The client in question		

	What are your timescales for doing this and in which formats?	would be contacted immediately. Remediation actions would be undertaken with the support of the client who's data may have been impacted in the incident.		
6. Personnel security Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.	6.1 Please describe what pre-employment screening you conduct on staff who will have access to our information, or who will be able to affect our service.	All staff undergo a Right to Work check as well as a Criminal Record Declaration.		
7. Secure development Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.	7.1 Do you conduct software development in line with industry good practice regarding secure design, coding, testing and deployment? Please provide an overview.	N/A - IFF outsource all software development.		
	7.2 Do you have configuration management processes in place to ensure the integrity of the solution through development, testing and deployment?	Yes, all configuration is carried out by the internal IT and security teams to ensure the most secure implementation.		
	7.3 Do you review new and evolving threats and improve the service in line with these?	New and emerging threats are flagged using our vulnerability scanning tool.		
8. Supply chain security The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the	8.1 Will customer information be shared with, or accessible to, any third-party suppliers?	No		
	8.2 Please describe how you manage security risks from third party suppliers?	All suppliers must sign a Data handling agreement (available on request) before information can be shared with them. This agreement sets out their security and privacy related responsibilities.		

service claims to implement		A15 Supplier Security Procedures.		
	8.3 Does your procurement process place security requirements on third party suppliers?	Yes		
	8.4 How do you ensure that third party suppliers conform with your security requirements?	Key suppliers (dependent on level of information access) may be assessed further as part of ongoing due diligence activities.		
9. Secure user management: Your provider should make tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.	9.1 Please list all the possible mechanisms by which you would accept management or support requests from customer (phone, web portal, email etc.)	If a client was having difficulty with the bespoke platform – we would invite them to make an initial support request through their IFF account manager.		
	9.2 Please describe how you ensure that only authorised individuals from customer organisation can use these mechanisms to affect customer use of the service.	IFF account managers would confirm with their client contact the legitimacy of any requests which might affect client use of the bespoke platform.		
	9.3 Please describe what functionality is exposed by the service's management interfaces and how you protect these.	[redacted]		
10. Identity and authentication: All access to service interfaces should be constrained to authenticated and authorised individuals. Authentication should take place over secure channels. Email, HTTP or telephone are vulnerable to interception and social engineering.	10.1 Please describe how users and administrators are authenticated to use the system/service.	[redacted]		
11. External interface protection: All external or less trusted interfaces of the service should be identified and appropriately defended.	11.1 Please list all the external interfaces (logical and physical) from which the backend and frontend of the system/application can be access or reached	[redacted].		

12. Secure service administration: Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data. The design, implementation and management of systems should follow enterprise good practice, whilst recognising their high value to attackers.	12.1 Please identify which service administration model you are using to manage the service out of: - Dedicated devices on a segregated network - Dedicated devices for community service administration - Dedicated devices for multiple community service administration - Service administration via bastion hosts - Direct service administration as defined here: https://www.ncsc.gov.uk/guidance/systems-administration-architectures	[redacted]		
13. Audit information for users: You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.	13.1 Please describe what audit information will be provided to, how and when it will be made available, the format of the data, and the retention period associated with it.	[redacted]		
14. Secure use of the service The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently you will have certain responsibilities when using the service in	14.1 Do you provide advice and guidance regarding any service configuration options available to customers and the security implications of customer choices?	[redacted]		

order for your data to be adequately protected.				

Cyber Assurance Assessment comments:

Cyber have completed the assurance of the Bespoke Portal used by IFF Research for your work. The outcome of the assessment is below; pay particular attention to the risk highlighted in yellow. If you have not done so already you will need to get the DPIA and Data Sharing agreement signed off by Data Protection. All the risks highlighted will be notified to the PMO for your business area.
We do need a copy of the updated Cyber Essentials certificate when they have completed their renewal; this is a condition of the assurance.

The assessment outcome is:

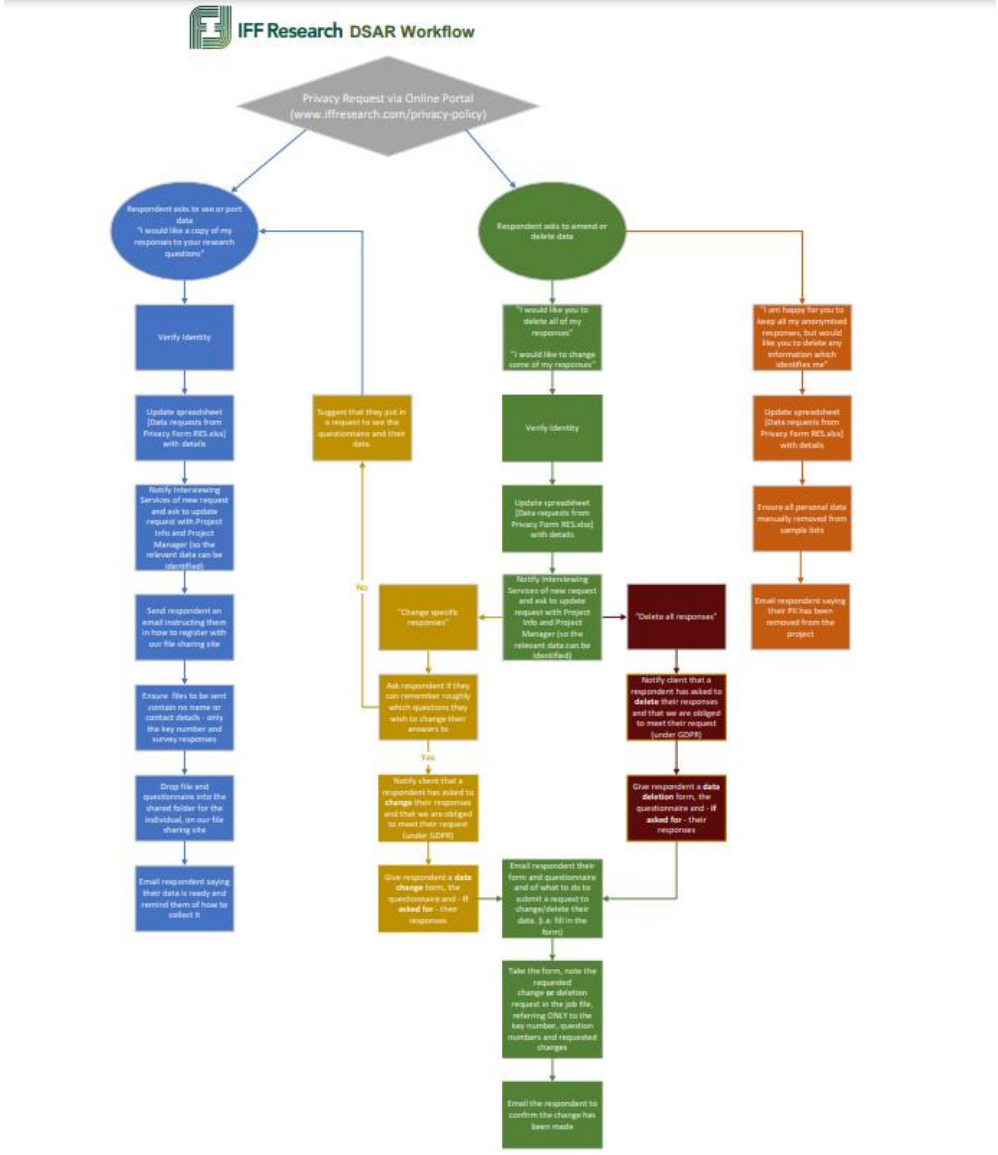
IFF Research along with the bespoke portal is assured to undertake engagements within DLUHC under the following conditions:

- *A DPIA is to be in place for this engagement given special category data will be collected. Data protection team is to be consulted around specific requirements.*
- *The supplier is to share a copy of their Cyber Essentials Plus certificate upon renewal in June as soon as possible after contract award.*
- [redacted]
- *No access to DLUHC systems. Any requirement to access DLUHC systems in future is to be under a separate approval.*

The risks identified are:

1. [redacted]

Annex D: IFF Subject Access Request procedure.


IFF Research DSAR Workflow
Privacy Request via Online Portal (www.iffresearch.com/privacy-policy)
Respondent asks to see or port data "I would like a copy of my responses to your research questions"
Respondent asks to amend or delete data
Verify Identity
Update spreadsheet [Data requests from Privacy Form RES.xlsx] with details
Notify Interviewing Services of new request and ask to update request with Project Info and Project Manager (so the relevant data can be identified)
Send respondent an email instructing them in how to register with our file sharing site
Ensure files to be sent contain no name or contact details - only the key number and survey responses
Drop file and questionnaire into the shared folder for the individual, on our file sharing site
Email respondent saying their data is ready and remind them of how to collect it
Suggest that they put in a request to see the questionnaire and their data.
No
"I would like you to delete all of my responses"
"I would like to change some of my responses"
Verify Identity
Update spreadsheet [Data requests from Privacy Form RES.xlsx] with details
Notify Interviewing Services of new request and ask to update request with Project Info and Project Manager (so the relevant data can be identified)
"Change specific responses"
Ask respondent if they can remember roughly which questions they wish to change their answers to
Yes
Notify client that a respondent has asked to change their responses and that we are obliged to meet their request (under GDPR)
Give respondent a data change form, the questionnaire and - if asked for - their responses
"Delete all responses"
Notify client that a respondent has asked to delete their responses and that we are obliged to meet their request (under GDPR)
Give respondent a data deletion form, the questionnaire and - if asked for - their responses
Email respondent their form and questionnaire and of what to do to submit a request to change/delete their data. (i.e. fill in the form)
Take the form, note the requested change or deletion request in the job file, referring ONLY to the key number, question numbers and requested changes
Email the respondent to confirm the change has been made
"I am happy for you to keep all my anonymised responses, but would like you to delete any information which identifies me"
Update spreadsheet [Data requests from Privacy Form RES.xlsx] with details
Ensure all personal data manually removed from sample lists
Email respondent saying their PII has been removed from the project

: