Department for Work & Pensions

DWP Privacy Impact Assessment (PIA)

Before completing this form, please read all the questions first. You must provide SRO and B-SIRO details otherwise the PIA will be returned to you for this information. You can find out more information about PIAs . DWP digital services must also complete [redacted]

Project details		
Project title	Living Together Data & Analytics	
PIA reference (allocated by DSDPP)		
Date PIA completed:	01/03/17	
PIA Version control: give the version of this PIA such as 1.0, 1.1, 2.0 etc.	1	**Project stage:** for example, Gate 0; ORR; Alpha; Beta Live
Contact name:	[redacted]	
Business Directorate:	Fraud, Error & Debt Programme	
Location:	[redacted]	
Email address:	[redacted]	
Telephone:	[redacted]	
Senior Responsible Officer (SRO): give name, email address and telephone number. **(This must be completed.)**	[redacted]	
Click here for: [redacted] give name, email address and telephone number. **(This must be completed.)**	[redacted]	
Tick which of the following applies:	This is: ☐ a new Project ☐ sharing personal information allowed by legislation ☐ sharing personal information with customer consent x☐ sharing personal information with a contracted provider ☐ sharing personal information in the public interest ☐ other. If other, describe briefly the circumstances that apply.	

Part 1 – this Part must be completed in all cases. DWP digital services must also complete [redacted]

Project details: Provide as much information as possible so that any privacy risks can be identified and measures taken to mitigate them
Project outline: Describe the project fully so that any reader (internal or external) can clearly understand the project purposes. You **must** include: • what the aims and objectives are • explain why the personal information needs to be used to achieve the objectives.
This measure has been scored by the Office For Budgetary Responsibility as part of the Budget 17 measures. Initially we are using 3rd Party Credit Reference Data to wash against our Income Support (IS) caseload as this has been identified as the area of highest fraud in the Living Together area. By using 3rd Party data we expect to be able to identify additional instances of this fraud that would previously have gone undetected. During the course of the contract we will test elements of other welfare benefits to identify potential future savings in this area as well as building on this initial work to identify lifestyle fraud and mortgage fraud. Not only will this help cleanse our IS caseload but it will reduce the amount of fraud entering the Universal Credit system as IS cases migrate over to UC. We need to send the information listed to ensure that we have identified the correct claimant and that we do not waste resource paying for information that we already held on our own systems. By sharing claimants details, other people we know to be in the household, and bank details we will receive a focused risk score from the supplier that will indicate high level risk cases that we were unaware of. Previous trials have shown that if we send minimal information we receive a high volume of false positive results and resource is wasted on investigating cases that are false or where the circumstances were already known to the Department
1. Stakeholders directly involved in the work: List the stakeholders including named DWP business areas; Local Authorities; contracted providers; other Government Departments; external non contracted organisations.
[redacted], DWP Legal, DWP Data Sourcing Team, DWP Fraud Error and Debt Analysts, DWP Fraud Error and Debt Finance Business Partner, DWP Customer Insight Team, DWP Housing Delivery Division
2. Has this, or similar, work been done before? Give details of any project, work or PIA of a similar nature which has been completed before and the PIA reference number(s), if known.
HMRC currently use the provider to risk score their cases. We have run a number of trials with Credit Reference Agencies over the last 2 years to support the evidence for this work During this time there have been no security incidents and adherence to exchange/retention of data procedures has been exemplary
3. What personal information is being used, collected, held or shared, and why? List the personal information, for example, name, address, National Insurance Number, Date of Birth etc. Give details of: • why it is necessary to use, collect, hold, share this personal information • how you will ensure that the personal information is only used for the purpose of this initiative.
The claimant file will contain the following information: • Claim NINO • Claim NINO Suffix • Claim Start Date • Forename 1 • Forename 2 • Surname • Sex Type • Date of Birth • Passported HB Flag • Sub Benefit Flag

- Bank or Building Society Code
- Bank or Building Society Account Number
- Address Lines 1 to 5
- Postcode
- Address Start Date
- Benefit Award Amount
- Benefit
- GB/NI
- Partner Status
- Claim Duration
- Mortgage/Loan Status
- Previous Risk Status
- Total Number on Claim
- CIS Household Count
- Local Authority District
- Date Last Scored
- No Times Scored
- No of Non-Dependants
- Children Flag

The household file will contain the following information:

- Claim NINO
- Household NINO
- Household NINO Suffix
- Household Forename 1
- Household Forename 2
- Household Surname
- Household Date of Birth
- Household Role
- Source
- Benefit

As detailed above. This information will allow GBG to ensure they have identified the correct claimant, that they do not return information on people living in the house that we already know about. We have Data sharing agreements in place and a contract will be signed by all parties to ensure adherence to agreed processes

4. What allows this personal information to be used or shared? Confirm the legal basis:

- the legislation that allows the sharing of personal information, or
- the customer's consent (include a copy of the consent form)or
- the public interest reasons overruling our duty of confidentiality to the individual.

Legislation- section 3(2) of the Social security Act 1998

5. Who are you sharing the personal information with and getting it from? Give details of the information flows to and from DWP at each stage. Give details such as:

- who will have access to the personal information, such as other government departments, third parties (organisations or individuals), contracted service providers, research organisations
- is this a bulk data share or a case by case data share?
- is there a Memorandum of Understanding or an Information Sharing Agreement for this data share? Include a copy of these
- the safeguards in place to ensure any third party will only use personal information for the purpose of this initiative
- the safeguards to limit inappropriate access and disclosure of the personal information.

The information will flow to [redacted] who manage the Governement DMI Framework. We will send a monthly file, potentially with 20,000 to 100,000 cases on it directly to [redacted] who without opening or storing the file will re-direct it to GBG who will undertake a number of Credit Reference checks. There will be a file for the benefit customers, and a Household file that will identify other

people we are aware of at the claimants address. This will avoid GBG sending back false positives on potential undeclared partners. GBG will only wash our data through their systems and will not undertake any other action, including intervention, on DWPs behalf. They will only use the data for the purpose of applying a risk score as laid out in the contract Once they have aggregated our risk scores, they will return a single file to DWP with a score against every record that we sent to them. They will not retain or store this file. We will have a signed contract. This is due by 12/5/17

6. How will the personal information be transferred securely? Include details of:

- transferring by electronic methods, including encryption arrangements, removable media, bulk data transfer arrangements, data linking arrangements, data matching arrangements, postal arrangements
- transferring personal information in hard copy format
- technical, physical and organisational security measures in place to protect the personal information against unlawful processing, loss, damage or destruction (please note these measures can also include staff vetting, third party contractual arrangements and staff training).

- Gateway Mandate G0143 has been approved.
- Access for the development of a SAS e-guide Project is covered by generic Business Case 1189 and testing and delivery to be covered by a separate Business Case to be raised once the build phase has commenced.
- A Data Transfer Request (DTR) will be submitted and approved for the issue of outbound data via the agreed secure method of delivery as detailed by the OCT documentation.
- A Data Transfer Request (DTR) will be submitted and approved for the receipt of the inbound response file from the supplier.
- When D&A have issued the outbound data results, the designated service provider will become the Data Controller and accept responsibility for continuing compliance with the Data Protection Act and ensure that all data supplied is kept securely.
- Data will be a .txt file pgp encrypted and transferred between DWP and service providers using SFTP.

7. How will this personal information be kept accurate and up to date? Explain the measures to ensure personal information obtained from individuals or other organisations is accurate and allows you to amend personal information, where necessary, to keep it up to date.

The first step will be to extract live data from DWP benefit systems, ensuring that it is accurate before being submitted to [redacted]. On return of the file, intelligence will be checked by Fraud and Error Services investigators as per the Business as Usual processes before starting any investigation

8. How long will the personal information be kept by DWP and all parties? Confirm:

- the retention period for this personal information
- compliance with the [redacted] or non-compliance with details of agreement with the Departmental Records Officer
- the retention period built into any IT system
- how DWP and the third party will review and securely destroy personal information when it is no longer required.

The designated service provider and DWP will ensure that the data is not kept for longer than is necessary to carry out the agreed functions and to delete/destroy upon completion of the exercise in accordance to Her Majesty's Government (HMG) Information Assurance (IA) Standard No 5. GBG will retain cases sent to them for 14 months then delete/destroy data in line with industry standards for data deletion

9. How will the personal information be stored securely by DWP and all parties?
Explain the secure storage arrangements for information held electronically and clerically. Include details of where the personal information will be stored and how will it be protected against:

- unauthorised or unlawful disclosure, access, use or modification
- loss, destruction or damage.

The cases selected for investigation will be automatically loaded onto FRAIMS. A copy of all risk scored records will be sent to the A&I Hub. A copy will also be retained in Centric to inform future selection of cases and a suitably anonymised file will be made available to analysts. Each copy will be retained in line with departmental data retention and destruction policies.

10. What arrangements are in place when a customer makes a written Subject Access Request for their personal information?

Please confirm that necessary steps have been taken to allow a Data Protection Officer to access the personal data held about an individual on this system, and to provide a copy (either a system generated print, or screen prints) of the information held, in an understandable format within the legal limit of 40 calendar days of receipt of the request.

All relevant information will be stored on FRAIMS as per normal business as Usual processes and be available on request

11. Does any new or additional IT, or digital service, have Departmental Security Accreditation?

☐ Yes

☐ In progress. If in progress, give the date that it is expected to be given

☒ No. If No, explain why it has not been provided or is not required.

There are no new services or systems required to undertake this end to end process

12. Is the personal information being transferred overseas outside of the UK or European Economic Area (EEA)? If personal information is being transferred outside of the UK or EEA, confirm to which countries. Explain the safeguards in place relating to the personal information at these locations.

No

Send your completed PIA by email to: [redacted]
Part 2 - to be completed by DWP digital services only.

1. Confirm the information security teams you are currently working with.

☐ Identity Management

☐ Technology Security Team

☐ Technology Security Build and Design Team

☐ None. If None, please confirm who is providing advice on security risks to personal information.

2. Are there security risks to personal information?

☐ Yes

☐ If Yes, provide a copy of your risk register and supporting information to explain the risk and any mitigation.

☐ No

3. Do you have a cookies policy?

☐ Yes. Provide a copy of your cookies policy. If Yes, is your cookies policy accessible via your site landing page? ☐ Yes. ☐ No.

☐ No. If No, see [redacted] for what must be included in a cookies policy.

4. Do you have a cookies banner?

☐ Yes. If Yes, provide a copy of the wording for your cookies banner.

☐ No. If No, explain why it has not been provided or is not required.

Are any cookies placed on a user's device before they see the cookies banner/cookies policy?

☐ Yes. If Yes, state what cookies are used and explain their purpose

☐ No.

Send your completed PIA by email to [redacted]