Home Office

Interim Data Sharing Protocol

Afghan Resettlement Policy (ARP)

April 2025

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at resettlementlapaymentsteam@homeoffice.gov.uk

Contents

Interim Data Sharing Protocol

This Interim Data Sharing Protocol (DSP) has been put in place to enable the sharing and the processing of personal data to support people arriving in the United Kingdom (UK) under the Afghan Resettlement Programme (ARP) and those eligible beneficiaries under the scheme already within the UK, which was launched on 1st March 2025. This protocol will run either until 1st May 2025 or until the ARP funding instructions are published on GOV.UK, whichever is later.

1. Aims and objectives of the DSP

1.1. The aim of this DSP is to provide a set of principles for information sharing including but not limited to the sharing on an interim basis of "personal data" as classified under the Data Protection Legislation. This DSP will provide cover prior to the publication of funding instructions as a result of no other DSP in place for this period.

1.2. For the purpose of this DSP, the Authority is the Home Office, and the Recipient is a participating local or regional authority supporting the delivery of the Afghan Resettlement Programme and to whom the Authority has agreed to provide Funding under this Instruction as a contribution towards eligible expenditure incurred supporting Beneficiaries.

1.3. This DSP sets out the rules that the Recipient must follow when handling information that includes personal data as defined in the UK Data Protection Legislation. The UK Data Protection Legislation stipulates specific obligations upon all individuals who process personal data which must be adhered to. The UK Data Protection Legislation requires that all sharing of personal data is carried out in accordance with the seven UK General Data Protection Regulation principles. The recipient, when processing personal data, in connection with supporting people under ARP in transitional accommodation and allocating settled accommodation to those on the ARP must comply with these principles of good practice.

2. Data protection legislation

2.1 The seven GDPR principles can be accessed via this link to the Information Commissioners Office Website: A guide to the data protection principles | ICO

2.2 Lawful Basis for Processing under GDPR:

The legal basis for the processing of the personal data covered in this DSP is Article 6(1)(e) of the (UK GDPR) – that is, that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

We also process special categories of personal data on the basis of Article 9(2)(g) of the UK GDPR where the processing is necessary for reasons of substantial public interest. This may include information about political beliefs, sexual orientation, religious beliefs and biometrics.

3. Security

3.1 The Recipient and its Staff shall exercise care in the use of information that they acquire during their official role, and to protect information which is held by them in accordance with the Data Protection Legislation. Such measures include:

- not discussing information about a Beneficiary in public; and
- not disclosing information to parties who are not authorised to have access to the shared information.

3.2 In addition to the above, the Recipient must ensure that:

- personal data received is processed solely for the purposes of discharging their obligations for supporting the Beneficiary under this protocol,
- all personal data received is stored securely,
- not disclosing information to third parties who are not authorised to have access to the shared information.
- only people who have a genuine need to see the data will have access to it,
- information is only retained while there is a need to keep it, and destroyed in line with government guidelines and Data Protection Legislation,
- all reasonable efforts have been taken to warrant that the Recipient does not commit a personal data breach of security,

- any information losses, wrongful disclosures or personal data breaches originating from the Authority are reported to the Authority's Security team at HOSecurity-DataIncidents@homeoffice.gov.uk

- they follow any information as provided by the Authority's Security Team and Data Protection Officer, who will provide direction on the appropriate steps to take e.g., notification of the Information Commissioner's Office (ICO) or dissemination of any information to the Beneficiary.

- The responsibility to notify the Authority is not withstanding the internal policies Strategic Migration Partners (SMPs), and local authorities will have regarding reporting data breaches to the ICO in their role as data controller.

3.3 Security breaches and incidents can result in government information being made available to those not authorised to have it or violate confidentiality. In the worst cases, a security incident or breach can jeopardise national security or endanger the safety of the public.

3.4 The Authority will make available further information as to what constitutes a personal data breach upon request. Both the Authority and the Recipient agree to advise and consult with each other on the appropriate steps to take, e.g., notification of the ICO or dissemination of any information to the data subjects.

3.5 As public sector bodies the Authority and the Recipient are required to process personal data in line with His Majesty's Government Security Policy Framework (Security policy framework: protecting government assets - GOV.UK (www.gov.uk)) guidance issued by the Cabinet Office when handling, transferring, storing, accessing, or destroying information assets.

4. Subject access requests

4.1 The Authority and the Recipient will answer any subject access or other requests made under the Data Protection Legislation that it receives for the data where it is the Controller for that data. In cases where such a request is received, both the Authority and the Recipient shall:

- consult the other before deciding whether or not to disclose the information;

- allow the other a period of at least five (5) working days to respond to that consultation;

- not disclose any personal data that would breach the principles of the Data Protection Legislation; and,

- give proper consideration to any arguments from the other as to why data should not be disclosed, and where possible reach agreement before any disclosure is made.

5. Data to be shared

5.1 The Authority will share a variety of documents with the Recipient providing information on the Beneficiary/s. The type of data will be dependent on how and under which route the Beneficiary arrived in the UK, and may include:

5.1.1 Family Questionnaire (where available)

5.2 The Authority will share with the Recipient the following documents:

5.2.1 UNHCR Resettlement Registration Form (RRF) (ACRS Pathway 2 only)

5.2.2 IOM Migration Health Assessment form (MHA) (all ARP Pathways)

5.2.3 UNHCR Best Interest Assessments and Determinations (ACRS Pathway 2 only)

5.2.4 IOM Pre departure Medical Screening Form (PDMS) and Pre-embarkation Certificate (PEC) (ARP – Afghan Resettlement Programme cohorts)

5.2.5 Home Office Matching Triage Questionnaire (ARP – Afghan Resettlement Programme cohorts)

5.2.6 IOM Direct Matching Questionnaire (ARP)

5.3 The above documents will contain the following personal information on a Refugee/Beneficiary:

UNHCR Resettlement Registration Form (RRF)

- Biographic data for each Refugee including marital status, religion, ethnic origin, and contact details in host country;
- Education, skills, and employment summary;
- Known relatives of the principal applicant and spouse not included in the referral submission;
- Summary of the Basis of the Principal Applicant's Refugee Recognition;
- Need for resettlement;
- Specific needs assessment;
- The number of people within a family due to be resettled, age and gender or family members;
- The language spoken;
- Ability to communicate in English; and

- Any known specific cultural or social issues.

MHA Form

- Consent from Refugee/Beneficiary to conduct a medical examination;
- Consent from the Refugee/Beneficiary to Medical Advisors to disclose any existing medical conditions to the Authority necessary for the resettlement process.

Best Interest Assessments and Determinations

- Information about any particular safeguarding circumstances and an assessment of the best interests of the individuals affected.

PDMS Form and PEC

- Biographic data for each refugee that requires this form;
- Medical information in relation to the Refugee/Beneficiary including medical history, updates on treatments and medication, on-going care requirements.

Home Office Matching Triage Questionnaire

- Biographic Data for Each Beneficiary including Name, Sex, Date of Birth, Primary Language.
- The number of people within a family due to be resettled, age and gender of family members.
- Ability to communicate in English.
- Education, Skills and Employment Summary.
- Mobility needs, impairments for each Beneficiary (includes dependants).

6. Storage, retention and destruction schedule

6.1 The Recipient will keep all personal information shared securely in accordance with the handling instructions associated with the information security classifications as well as its own data retention and destruction schedules.

6.2 Recipients will not retain the personal information for longer than is necessary for the purpose of resettlement activity.

6.3 A regular review shall be conducted by the Recipient to assess the necessity of retaining the Beneficiary's personal data. Once the data is no longer relevant for those purposes it will be destroyed securely.

7. Central points of contact for issues, disputes and resolution

7.1 The Recipient shall provide the Authority with reasonable co-operation and assistance in relation to any complaint or request made in respect of any data shared under this data sharing arrangement, including providing the Authority with any other relevant information reasonably requested by the Authority.

7.2 Any operational issues or disputes that arise as a result of this DSP must be directed in the first instance to the Local Authority Engagement Team Strategic Regional leads.

8. Staff responsibilities

8.1 Staff authorised to access a Beneficiary's personal data are personally responsible for the safekeeping of any information they obtain, handle, use and disclose.

8.2 Staff should know how to obtain, use and share information they legitimately need to do their job.

8.3 Staff should never access information shared under this DSP, unless it is part of their role, and they have a business need to do so.

8.4 Staff have an obligation to request proof of identity or takes steps to validate the authorisation of another before disclosing any information requested under this DSP.

8.5 Staff should uphold the general principles of confidentiality, follow the guidelines set out in this DSP and seek advice when necessary.

8.6 Staff must make sure they know what classification the information should have and stick to the rules for that level of protection.

8.7 Staff should not share any of the information shared or discuss individual details of cases outside of a business need and working environment.

8.8 Staff should never use removable media to store/move this information. Staff should keep work laptops and work phones secure at all times.

8.9 Staff should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal. Criminal proceedings might also be brought against that individual.

Sharing Data

8.10 Staff should never give out sensitive information over the phone or in any other way unless they are sure who they are giving it to, and they are entitled to that information.

8.11 Staff should not send any personal information, or information that could identify the case, by unsecure email.

8.12 Staff have an obligation to request proof of identity or takes steps to validate the authorisation of another before disclosing any information requested under this DSP.

8.13 Staff should uphold the general principles of confidentiality, follow the guidelines set out in this DSP and seek advice when necessary.

8.14 Staff should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal. Criminal proceedings may also be brought against that individual.

9. Freedom of information requests

9.1 Both the Authority and the Recipient will answer any requests made under the Freedom of Information Act 2000 that it receives for information that it holds solely as a result of, or about, this data sharing arrangement. In such cases where such a request is received, both the Authority and the Recipient shall:

- Consult the other before deciding whether or not to disclose the information.
- Allow the other a period of at least five (5) working days to respond to that consultation; and
- Not disclose any personal data that would breach the principles of the Data Protection legislation.

10. Method of transfer of a beneficiary's personal data

10.1 The Authority will use a secure process, known as MOVEit, to transfer the data which allows internal and external users to share files securely and shall provide the interaction between the parties.

10.2 The Recipient shall be given access to MOVEit over a web-based browser. Once this arrangement is operative, the Recipient shall, to the extent from time to time specified by the Authority, be required to use MOVEit for the purpose of its interface with the Authority under this DSP.

10.3 A list of authorised Staff should be available for inspection if requested by the Authority.

11. Restrictions on use of the shared information

11.1 All information on a Beneficiary that has been shared by the Authority must only be used for the purposes defined in Section 3 of this DSP, unless obliged under statute or regulation or under the instructions of a court. Therefore, any further uses made of the personal data will not be lawful or covered by this DSP.

11.2 Restrictions may also apply to any further use of personal information, such as commercial sensitivity or prejudice to others caused by the information's release, and this should be considered when considering secondary use of personal information. In the event of any doubt arising, the matter shall be referred to the Authority whose decision – in all instances – shall be final.

11.3 A full record of any secondary disclosure(s) must be made if required by law or a court order on the Beneficiary's case file and must include the following information as a minimum:

- Date of disclosure;
- Details of requesting organisation;
- Reason for request;
- What type(s) of data has been requested;
- Details of authorising person;
- Means of transfer (must be by secure); and
- Justification of disclosure.

11.4 The restrictions on secondary disclosures as set out in paragraph 11.1 and 11.2 of this DSP apply equally to third party recipients based in the UK and third-party recipients based outside the UK such as international enforcement agencies.

12. Audits

12.1 The Recipient agrees that it may be audited at the request of the Authority to ensure that the personal data has been stored and/or deleted appropriately, and that they have conformed to the security protocols set out in this DSP.

12.2 The Authority confirms that no other information would be reviewed or audited for this purpose.

Annex A – Record of changes to data sharing protocol (to previous published versions)

Clause, paragraph number	Details of change
Front cover	Interim Data Sharing Protocol for the Afghan Resettlement Policy (ARP)
Page 2	Explanation of the scope for the interim data sharing protocol until the 01 May 2025 or until the publication of the ARP Funding Instructions on GOV.UK, whichever is later.
Data Sharing Protocol	Expansion of the Aims and Objectives of the DSP from 1.1 to 1.4. Insertion of the seventh GDPR Principles in 2.1 Insertion of the lawful basis for processing data under the Legislation Framework in 2.2 Change of term in 3.2 from 'instruction' to 'protocol'. Expansion of Security in 3.2 and 3.4 Change of pathway within 5.2 to include ARP. Insertion of Home Office Matching Triage Questionnaire in 5.3 Expansion of Staff Responsibilities in 8. Insertion of 'Sharing Data' from 8.10 to 8.14.