Home Office

Department for Communities and Local Government

Department for International Development

SYRIAN VULNERABLE PERSONS RESETTLEMENT SCHEME

Data Sharing Protocol (DSP)

1. AIMS AND OBJECTIVES OF THE DSP

1.1 The aim of this DSP is to provide a set of principles for information sharing between the Authority and the Recipient.

1.2 This DSP sets out the rules that the Recipient must follow when handling information classified as "personal data" by the Data Protection Act (DPA) 1998.

Personal Data

1.3 The term "personal data" refers to any:

a. data, which relate to a living individual who can be identified from those data; or

b. from those data and other information which is in the possession of, or likely to come into the possession of, the data controller.

1.4 The DPA also defines certain classes of personal information as "'sensitive data" where additional conditions must be met for that information to be used and disclosed lawfully.

1.5 Under the DPA "sensitive personal data" is defined as information concerning:

- racial or ethnic origin,
- political opinions,
- religious or other similar beliefs,
- membership of trade unions,
- physical or mental health or condition,
- sexual life, and
- convictions, proceedings and criminal acts.

1.6 Sensitive personal data is subject to much stricter regulation than ordinary personal data and must only be processed when one of an additional number of conditions has been satisfied. The conditions relevant to the purposes of this DSP are:

- the data subject has given explicit consent, or
- it is necessary in order to protect the vital interests of the individual, or
- the processing is carried out in the course of its legitimate activities by a non-for-profit organisation and exists for political, philosophical, religious, or trade-union purposes, with appropriate safeguards, in relation to people who are members or have regular contact with the organisation in connection with its purposes, and there is no disclosure to third parties without consent, or
- the information has been made public as a result of steps deliberately taken by the data subject, or

- The processing is necessary for or in connection with legal proceedings, or for establishing, exercising or defending legal rights

2. DATA PROTECTION ACT 1998 (DPA)

2.1 The DPA stipulates specific obligations upon all individuals who process personal data which must be adhered to. The DPA requires that all transfers of information fall within its eight data protection principles and requirements. The Recipient, when processing personal data in connection with the Instruction, **must** comply with these principles of good practice.

2.2 Personal data must be processed in accordance with the eight data protection principles in Schedule 1 of the DPA.

3. PURPOSE OF DATA SHARING

3 1 The Authority will share personal data described at Section 7 of this Annex B to inform the Recipient of the specific needs of the Beneficiaries, and aid the ongoing resettlement planning.

4. SECURITY

4.1 The Recipient and its Staff shall exercise care in the use of information that they acquire in the course of their official role, and to protect information which is held by them in accordance with the DPA. 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.

4.2 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 Beneficiaries under this Instruction,
- all personal data received is stored securely,
- 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,
- all reasonable efforts have been taken to warrant that the Sponsor does not commit a breach of security.
- any information losses, wrongful disclosures or breaches of security relating to information originating from the Authority are reported to the Authority immediately (i.e. within 24 hours of becoming aware), in first

instance through Strategic Regional Leads and notifying the Authority's Corporate Security Unit at: HOSecurityenquiries@homeoffice.gsi.gov.uk

- The Authority 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 Beneficiaries.
- Security breaches and incidents can result in government information being made available to those not authorised to have it or violate confidentiality, and can also cause embarrassment to ministers and damage the reputation of the department. In the worst cases, a security incident or breach can jeopardise national security or endanger the safety of the public.

4.3 The Authority will make available further information as to what constitutes a security breach upon request.

4.4 As public sector bodies the Authority and the Recipient are required to process personal data in compliance with both the mandatory requirements set out in CESG Information Assurance Top Tips for Handling Personal Data[1] and the Her Majesty's Government Security Policy Framework (HMG SPF) guidance[2] issued by the Cabinet Office when handling, transferring, storing, accessing or destroying information assets.

5 LEGAL CONSIDERATIONS AND BASIS FOR THE SHARING OF INFORMATION

5.1 The Authority and the Recipient are legally obliged to handle personal information according to the requirements of the Data Protection Act 1998 and the Human Rights Act 1998 (HRA).

Legal powers to share data: Authority to Recipient

5.2 As a Crown Government Department, the Authority has Common Law ('Ram') powers to do whatever a natural person may do (subject to overarching legal constraints), and can share and process data so long as it complies with the principles of the DPA,

5.3 In accordance with the first principle of the DPA the Authority will ensure the data is processed fairly and lawfully by ensuring that:

- The processing is necessary for the exercise of any functions of the Crown, a Minister of the Crown or a government department in accordance with Schedule 2 paragraph 5(c) of the DPA.
- The processing is necessary for the exercise of any other functions of a public nature exercised in the public interest by any person – in accordance with Schedule 2 paragraph 5(d) of the DPA.

---

[1] Replacement for the Information Assurance Standard 6 guidance

[2] https://www.gov.uk/government/publications/security-policy-framework

- Where the personal data to be processed is sensitive personal data, the processing is necessary for the exercise of the functions of the Crown, a Minister of the Crown or a government department – in accordance with Schedule 3 paragraph 7(1)(c) of the DPA.

5.4 Section 59(1)(e) of the Nationality, Immigration and Asylum Act 2002 allows the Authority to participate in a project designed to arrange or assist the settlement of migrants (whether in the UK or elsewhere).

Legal powers to share data: Recipient to Authority

5.5 Section 1 of the Localism Act 2011 provides the Recipient with a general power to do anything an individual can do to the extent that sharing information is compatible with other legal obligations (e.g. the DPA and the terms of the Funding Instruction).

6 FREEDOM OF INFORMATION AND SUBJECT ACCESS REQUESTS

Freedom of Information Requests

6.1 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 DPA.

Subject Access Requests

6.2 The Authority and the Recipient will answer any subject access or other requests made under Part II of the DPA that it receives for the data where it is the Data 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 DPA; 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.

DATA TO BE SHARED

6.3 The Authority will share with the Recipient the following documentation on a Beneficiary.

- UNHCR Resettlement Referral Form (RRF)
- Migration Health Assessment form (MHA)
- Best Interest Assessments and Determinations

6.4 The above documents will contain the following personal information on a Beneficiary:

UNHCR RRF

- biographic data for each Beneficiary including contact details in host country,
- known relatives of the principal applicant and spouse not included in referrals submission,
- summary of the Basis of the Principal Applicant's Refugee Recognition[3],
- Need for resettlement[4],
- specific needs assessment[5],
- 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[6].

MHA Form

- consent from Beneficiary to conduct a medical examination,
- consent from the Beneficiary to Medical Advisors to disclose any existing medical conditions to the Authority necessary for the resettlement process[7].

Best Interest Assessments and Determinations

- information about any particular safeguarding circumstances and an assessment of the best interests of the individuals affected[8].

[3] classed as sensitive personal information under the DPA
[4] classed as sensitive personal information under the DPA
[5] depending on the content, this could be classed as potentially sensitive personal information under the DPA
[6] depending on the content, this could be classed as potentially sensitive personal information under the DPA
[7] classed as sensitive personal information under the DPA

6.5 The RRF is provided to the Authority by e-mail from the UNHCR. Once received, the MOVEit portal will be used to share secure documents with the Recipient.

6.6 The above documentation when shared with the Recipient will be classified as "**OFFICIAL-SENSITIVE**" by the Authority in accordance with the Government Security Classification Scheme (GSCS)[9].

7 METHOD OF TRANSFER OF A BENEFICIARY'S PERSONAL DATA

7.1 The Authority will use a secure web-based tool, known as MOVEit, which allows internal and external users to share files securely and shall provide the interaction between the parties.

7.2 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 Instruction.

8 LEVEL OF ACCESS TO THE MOVE IT PORTAL

8.1 The Recipient will appoint a Local Administrator who will be responsible on behalf of the Recipient for authorising access requests to the Recipient's designated File Share Area within MOVEit.

8.2 The Recipient will make requests for additional access to MOVEIt to the Authority. All requests for additional access to the Recipient's organisation's designated File Share Area received by Authority will be dealt with on a case-by-case basis and only granted if necessary for the purpose of the Recipient discharging their obligations for supporting Beneficiaries in accordance with the contract.

8.3 .

8.4 Access shall only be permitted to a Recipient who, for the purposes of supporting the Beneficiaries:

- commits to treating the personal data in accordance with its obligations, in particular Clause 3 (Confidentiality and Data Sharing), unless the Recipient has received prior written consent from the Authority;

8.5 Access shall only be permitted to Staff who, for the purposes of supporting the Beneficiaries:

---

[8] depending on the content, this could be classed as potentially sensitive personal information under the DPA

[9] Further information regarding the GSCS can be found on-line at - https://www.gov.uk/government/publications/government-security-classifications

- have a genuine “need to know”;
- are permitted to view the data as part of their official duties;
- have signed a confidentiality agreement[10].

8.6 The Local Administrator must remove access immediately from a member of Staff who no longer requires access to MOVEit and the FSA.

8.7 An up-to-date list of Staff who have been granted permission to access the FSA and the reason for granting access shall be kept by the Local Administrator.

8.8 The list of authorised Staff should be available for inspection if requested by the Authority

9 RESTRICTIONS ON USE OF THE SHARED INFORMATION

9.1 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.

9.2 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.

9.3 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.

9.4 The restrictions on secondary disclosures as set out in Paragraph 10.1and 10.2 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.

[10] The Recipient will be responsible for setting up, managing, recording and storing a procedure.

10 PROTOCOLS FOR RECIPIENT'S PROCESSING SENSITIVE PERSONAL INFORMATION[11]

10.1 The Recipient shall only access sensitive personal data pertaining to a Beneficiary's experience in their country of origin and medical health history in exceptional circumstances and if deemed as absolute necessary for the permitted purpose i.e. to fully assess the specific physical and/or psychological needs of a Beneficiary and not without prior consent from the Authority/Beneficiary

10.2 The Recipient must document how any sensitive personal data pertaining to a Beneficiary's experience in their country of origin and medical records was used by the Sponsor for the purposes of discharging their obligations in accordance with the Instruction.

10.3 In circumstances where it is deemed necessary to share the sensitive personal data with third parties for the permitted purpose the Recipient must administer additional handling instructions for handling the data which must be determined by the Authority.

10.4 The Authority shall make available its own Handling Instructions as a guide upon request.

11 STAFF RESPONSIBILITIES

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

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

11.3 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.

11.4 Staff should uphold the general principles of confidentiality, follow the guide-lines set out in this DSP and seek advice when necessary.

11.5 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.

12 STORAGE, RETENTION AND DESTRUCTION SCHEDULE

12.1 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.

[11] As described at Clause 7.2 of this Annex B

12.2 Recipients will not retain the personal information for longer than is necessary for the purpose set out in this DSP. A regular review shall be conducted by the Recipient to assess the necessity of retaining the Beneficiary's personal information. Once the information is no longer relevant for those purposes it will be destroyed securely.

Destruction Procedures

12.3 It is the Recipient's responsibility to ensure that any information provided by the Authority for the purposes of supporting a Beneficiary are destroyed securely once all resettlement needs are complete.

12.4 If storing any paper files, the paper file should be destroyed using a confidential paper shredder and disposed of securely.

12.5 When destroying personal records, the Recipient will arrange the secure destruction or deletion of the data, in accordance with the seventh principle of the DPA, HMG Security Policy Framework and in accordance with the security classification marking for the data.

13 AUDITS

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

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

14 CENTRAL POINTS OF CONTACT FOR ISSUES, DISPUTES AND RESOLUTION

14.1 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.

14.2 Any operational issues or disputes that arise as a result of this DSP must be directed to the relevant contact points noted at Clause 4.2 of this Annex B.