Home Office

Department for Work & Pensions

PROCESS LEVEL MEMORANDUM OF UNDERSTANDING (PMoU)

BETWEEN

THE HOME OFFICE

AND

DEPARTMENT FOR WORK AND PENSIONS

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

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

Contents

Introduction and Participants to the Memorandum of Understanding (MoU)

The Participants to this MoU are

1. THE HOME OFFICE[1] of 2 Marsham Street, London, SW1P 4DF, specifically UK Visas and Immigration Strategy, Transformation and Performance Team, hereafter referred to as "Home Office."

And

2. DEPARTMENT FOR WORK AND PENSIONS of Caxton House, Tothill Street, London, SW1H 9NA, specifically Digital Cross Boundary Team, hereafter referred to as "DWP."

Collectively Home Office and DWP are referred to as "Participants", and individually are referred to as a "Participant."

This MoU sets out the information sharing arrangement between the aforementioned Participants. For the context of this MoU, 'information' is defined as a collective set of Data[2] and/or facts that, when shared between the Participants through this MoU, will support the Participants in delivering the Purpose of the data sharing activity described in the section on purpose and benefits of the data sharing.

This MoU is not intended to be legally binding. It documents the respective roles, processes, procedures and agreements reached between Home Office and DWP. This MoU should not be interpreted as removing, or reducing, existing legal obligations or responsibilities of each Participant, for example as Controllers under the Data Protection Legislation Act 2018.

---

1 Home Office – for the purposes of this MoU means the functions of Border, Immigration and Passport functions only and not the whole of the Home Office and its Executive Agencies

2 All references to "Data" include Personal data, Special Category data, Non Personal Information, and de-personalised Information.

Personal data as meaning "any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifiers"

Formalities

Date of review

This MoU will be reviewed annually.

Administration

The Home Office and DWP will each instruct a MoU Manager to deal with the administration of this data sharing arrangement.

Either Participant may inform the other of a change to the MoU Manager in writing.

Legal bases to share data

Participants are legally obliged to handle personal information according to the requirements of the Data Protection Legislation (EU General Data Protection Regulation (GDPR), the Data Protection Act 2018) and the Human Rights Act (HRA) 1998, along with any other relevant legislation.

As well as meeting the requirements of the Data Protection Legislation 2018, and the HRA, the Participants are bound by the Common Law Duty of Confidentiality.

No information will be exchanged in breach of any prohibitions on onward disclosure and information will be exchanged in a way which is compliant with the overarching principles of the Data Protection Legislation, any statutory data sharing powers, the Common Law Duty of confidentiality and the HRA.

Home Office to DWP

As a Crown Department, the Home Office will rely on Common Law powers to share the personal information as set out in this MoU with DWP to exercise its immigration functions.

DWP to Home Office

Section 20 of the Immigration and Asylum Act 1999 as amended by Section 55 of the Immigration Act 2016 allows DWP to supply information to the Home Office for processing EEA applications under Section 55 (a) or (dd) as set out below:

(a) the administration of immigration control under the Immigration Acts or

(dd) anything else that is done in connection with the exercise of a function under any of the Immigration Acts

The EU Exit Settlement Scheme (the scheme) will be governed by new Immigration Rules, which come under the 1971 Immigration Act.

Statutory Data Processing Conditions

From 25 May 2018 the relevant statutory conditions for processing personal data for both Participants are set out below:

Home Office

Article 6(1)(e) ”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.”

DWP

Article 6(1)(e) “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.”

Data Protection Impact Assessment (DPIA)

The completion of a DPIA has been carried out by both Participants including an Equality Impact Assessment conducted by the Home Office.

HRA 1998 the right to respect for private and family life

There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or orals or for the protections of the rights and freedoms of others.

The sharing under this data sharing arrangement will satisfy Article 8 as it is:

- In pursuit of a legitimate aim: The aim of this data sharing arrangement is to support the Home Office in the delivery of its statutory functions
- Proportionate: The information transferred is proportionate for the needs of this data sharing arrangement. The minimum information necessary for the purpose is transferred and no more. A pseudo (Correlation) ID will be used when the data is returned, rather than the NINO, Date of Birth and Name
- Appropriate and necessary to a democratic society: Preventing and detecting unlawful activities and maintaining public safety of all kinds is an activity necessary to a democratic society

Common Law Duty of Confidentiality

Individuals applying under the EU Settlement Scheme will be aware of the potential for data sharing via the privacy notices (see paragraphs 3.14 and 3.15) provided by each Participant. As such there can be no expectation or circumstance that would create an expectation of confidentiality on the part of individuals whose data is shared between the Participants for the agreed purpose set out in the section on purpose and benefits of the data sharing.

Privacy Notices

Home Office

The Home Office on-line application form for the EU Settlement Scheme for Indefinite Leave to Remain (ILR) or Leave to Remain (LTR) in the United Kingdom will require applicants to sign a declaration. The declaration will include an understanding that their personal data /information may be shared with other government departments and make reference to DWP specifically, for decision making and immigration purposes and will ensure that the declaration complies with the principles of the Data Protection Legislation.

DWP

DWP have no direct Agent or customer interaction. This is a system to system data transfer only.

Role of Controller in respect of the data sharing arrangement

A Controller means “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.”

Home Office and DWP will be Controllers “‘in common” during the physical transfer process and as such are required to satisfy their Data Protection obligations as Controllers.

DWP will become sole Controller for the personal data received – for the purposes for which it was shared and as such are required to satisfy their Data Protection obligations as Controller.

Home Office will become sole Controller for the personal data received - for the purpose for which it was shared and as and as such are required to satisfy their Data Protection obligations as Controller

Purpose and benefits of the data sharing

To support the EU Settlement Scheme and manage the influx of applications as the UK leaves the EU, the Home Office has developed an Application Programming Interface (API). This will enable the online Home Office Access UK web-based portal (using the gov.uk platform) to check an applicant's activity in the UK using DWP and HMRC data to support a residency assessment (final decision to be undertaken by a Home Office caseworker). This will be achieved by directly accessing DWP and/or HMRC records in real-time during the online application. The residency assessment will determine whether or not an applicant is eligible for ILR or LTR.

The API will run on the current Access UK web-based portal, giving the applicant a point of access anywhere in the UK and by digital means.

The implementation of the API to allow DWP and HMRC's data to be accessed in real-time will:

- Reduce the Home Office reliance on paper documentation with a potential of 3.6m eligible applicants
- Reduce caseworker processing time
- Reduce fraud and error
- Improve customer journey

Data to be shared and the systems the data will be derived from

EU Settlement Scheme applicants

To meet the criteria for ILR, EEA nationals must generally provide evidence that they have been continuously resident in the UK for five years. If an applicant does not meet the criteria for ILR, their application will be considered for LTR whereby the applicant will need to demonstrate residence in the UK within six months of their application date. Non-EU nationals may qualify for ILR or LTR under this scheme if they have a relationship with an EEA national and that EEA national ('the sponsor') meets the above residency criteria.

Data to be supplied to DWP via the API

The individual will enter their details into the online application system on Access UK and will include the following personal data:

- Forename
- Surname
- NINo (optional, but required to generate the API check with DWP)
- Date of Birth
- Any previously held or other names

The data will be transferred by the API using a software to software interface to match the individual against DWP records.

Data to be supplied by DWP via the API

If a matching record is found on DWP systems within either the current tax year or six preceding years, DWP will return the following information relating to each benefit type:

- Correlation ID
- Start date
- End date
- Benefit type
- Date of death

- Gone abroad flag

The following DWP benefit types are within the scope of this data sharing arrangement:

- State Pension and New State Pension
- Housing Benefit
- Jobseekers
- Employment Support Allowance
- Carers Allowance
- Universal Credit
- Personal Independent Payment
- Disability Living Allowance
- Income Support
- Maternity Allowance
- Incapacity Benefit
- Attendance Allowance
- Severe Disablement Allowance

Type of data share

This will be a regular data share for the purpose as set out in the section on purpose and benefits of the data sharing of this MoU.

Description of how the data sharing will occur

The data will be provided by the applicant as part of their online application. During this online application, the API will allow this detail to be checked against DWP systems to identify whether any relevant benefit records exist. The output from DWP will be returned in real time and aggregated with information obtained from HMRC. A Caseworker will then use this data to inform a calculation to determine whether an applicant's UK residence indicates whether they are eligible for consideration for ILR or LTR under the scheme. If the API check is unsuccessful or the person cannot be found during the initial check made during the online application, a Home Office Caseworker may instigate the check again following the submission of the application if there is reason to believe a successful match is possible and it will benefit the applicant. If the application concerns a non-EEA national, the API check may be conducted on the EEA national sponsor by the Caseworker, but only when satisfactory documentary evidence is not available.

Retention and destruction schedule

Raw data accessed from DWP systems will only be available for the duration of the calculation and will not be retained by the Home Office. Instead, the Home Office will apply the relevant business rules for the EU Settlement Scheme to produce a summary of qualifying months DWP holds records for pertaining to the applicant. This summary will contain either a positive or a negative output for each month in the period assessed. No further details will be retained. This summary will be stored on Home Office systems in line with existing data protection protocols and held for 10 years before secure destruction.

Permitted uses of the data in respect of this MoU

Access will only be permitted to authorised personnel from DWP and the Home Office who have:

- the appropriate security clearance determined by their own department to handle the data
- a genuine business need to access the data

Onward disclosure to third parties

No onward disclosure to third parties is required under this data sharing arrangement.

Roles of each Participant to the MoU

Role of Home Office

- Data will be provided to DWP via the API, the agreed secure transfer method agreed by both Participants and within Home Office data security instructions
- Only allow access to the data by the caseworker(s) working on the application
- Ensure that staff handle this data in line via API and in accordance with the Government Security Classification marking of “Official Sensitive” where applicable
- Only store the data for as long as it there is a business need to do so;
- Provide applicants with clear guidance regarding how they complete their application to facilitate these checks and what actions they need to take following the results to complete their application with the Home Office
- The Home Office MoU Manager will ensure that a review of the MoU is carried out

Role of DWP

- Identify the appropriate data required to make the search from DWP records
- Only allow access to that data by the team carrying out the matching
- Ensure that staff handle this data in line via API, the approved secure method agreed by both Participants and within DWP data security instructions
- Enable access to the relevant data via the API, a secure method agreed by both departments under the Government Security Classification Marking of “Official-Sensitive” where applicable
- Only store the data for as long as it there is a business need to do so
- Provide designated points of contact for the Home Office to utilise, should the technical process underpinning this data sharing arrangement not function
- The DWP MoU Manager will ensure that a review of the MoU is carried out

Accuracy of the shared data

The applicant who will enter their details on the online application system; this data will be provided to DWP via the API. DWP must take all reasonable steps to ensure that the data being returned to the Home Office as a result of matching the applicant’s details against DWP held data is both accurate and up-to-date in accordance with the requirements of the Data Protection Legislation.

Arrangements for notifying the other Participant of inaccuracies during the data sharing process

Data shared between Participants should be subject to procedures and validations intended to ensure data quality.

The data DWP hold is a snapshot of data taken from legacy systems and as such DWP are reliant on the benefit processor having input the information correctly. To the best of DWP's knowledge the data is accurate at point of extract.

When data matching is undertaken full testing will take place to ensure that the solution is working as documented in the requirement.

Should DWP identify any error within the processing, that could affect the eligibility of the applicant; DWP will notify Home Office within 24 hours and endeavour to fix the error within 5 working days of problem identification.

Subject Access Requests (SAR) for information held by receiving Participant

Home Office and DWP shall respond to requests from data subjects exercising their right of subject access and/or their right to request the cessation of processing, in accordance with the requirements of Data Protection Legislation.

In the event that a subject access request (SAR) is received and only relates to personal information held by the receiving Participant; the receiving Participant will issue a formal response following their internal process and procedures for responding to the SAR within the statutory timescales.

SAR for information held partially by receiving Participant

Where it is identified that the receiving Participant does not hold all the information requested, they are only expected to disclose the information they have available, in accordance with their obligations under the Data Protection Legislation. There is no statutory requirement to re-direct SARs or provide details of OGDs/Participants in the response.

Freedom of Information Act (FoIA) Requests and Transparency

Home Office and DWP are both public authorities for the purposes of the FOIA. This means that any information held by Home Office and DWP is accessible by the public on written request, subject to certain limited exemptions.

Home Office and DWP shall demonstrate a commitment to openness and transparency regarding information sharing arrangements under this MoU, subject to any limitations posed by security or confidentiality requirements.

In the event that an information access request relating to Information Sharing activities under this MoU is received, both Participants agree to consult with the other in line with the Code of Practice as implemented by section 45 of FOIA.

Handling of personal data and data security

Where Participants are deemed to bear the responsibility of a Controller, they must ensure that any personal data received pursuant to this MoU are processed in accordance with their obligations under the Data Protection Legislation.

Additionally, as part of the Government, both Participants must process personal data in compliance with the mandatory requirements Her Majesty's Government Security Policy Framework (HMG SPF) guidance issued by the Cabinet Office when handling, transferring, storing, accessing or destroying Information assets. HMG SPF guidance document can be accessed via the following link: www.gov.uk/government/publications/security-policy-framework

Participants must ensure effective measures are in place to protect personal data in their care and manage potential or actual incidents of loss of the personal data. Such measures will include, but are not limited to:

- Personal data should not be transferred or stored on any type of portable device unless absolutely necessary, and if so, it must be encrypted and password protected to an agreed standard
- Participants will take steps to ensure that all staff are adequately trained and are aware of their responsibilities under the GDPR and Data Protection Act 2018and this MoU
- Access to personal data received by Participants pursuant to this MoU must be restricted to personnel on a legitimate need-to-know basis, and with security clearance at the appropriate level
- Participants will comply with the Government Security Classifications Policy (GSCP) where applicable

Where the recipient of personal data disclosed under this MoU, experiences a security incident or data breach, the Participant experiencing the breach must report any data losses, wrongful disclosures or breaches of security relating to personal data originating to the Participant that provided the data within 24 hours of becoming aware of the breach. They should also consult with and advise the other Participant on the appropriate steps to take (e.g. informing the Information Commissioner's Office (ICO) or notifying the data subjects). Please see the section on security breaches, security incidents or loss or unauthorised disclosures of data.

Monitoring and reviewing arrangements

This MoU relates to a regular exchange and will run until April 2026 but must be reviewed at least biennially to assess whether the MoU is still accurate and fit for purpose.

Reviews outside of the proposed annual review can be called by representatives of either Participant. Any changes needed as a result of that review may be agreed in writing and appended to this document for inclusion at the formal annual review.

A record of all reviews will be created and retained by each Participant.

Issues, disputes and resolution

Any issues or disputes that arise as a result of exchange covered by this MoU must be directed to the relevant contact points. Each Participant will be responsible for escalating the issue as necessary within their given commands.

Where a problem arises it should be reported as soon as possible. Should the problem be of an urgent nature, it must be reported by phone immediately to the designated business as usual contact and followed up in writing the same day. If the problem is not of an urgent nature it can be reported in writing within 24 hours of the problem occurring.

Termination

This MoU may be terminated by giving three months' notice by either Participant.

Both Participants to this MoU reserve the right to terminate this MoU with three months' notice in the following circumstances:

- by reason of cost, resources or other factors beyond the control of the Home Office or DWP
- any material change occurs which, in the opinion of the Home Office and DWP following negotiation significantly impairs the value of the data sharing arrangement in meeting their respective objectives

In the event of a significant security breach or other serious breach of the terms of this MoU by either Participant the MoU will be terminated or suspended immediately without notice.

Security breaches, security incidents or loss or unauthorised disclosures of data

A security breach is a situation where the rules on handling and protecting information or equipment have been broken.

A security incident is a situation which results in the loss or theft of, or unauthorised access to the Home Office/DWP information or equipment.

Examples of serious security breaches, incidents, loss or unauthorised disclosure may include:

- accidental loss or damage to information
- damage or loss of information by means of malicious software/hacking
- deliberate or knowingly disclosure of information to a person not entitled to receive the information; emailing classified/sensitive information to personal email accounts
- leaving classified/sensitive papers in an unsecure or publicly accessible area
- using social networking sites to publish information which may bring either Participant's organisations into disrepute

The designated points of contact are responsible for notifying the other Participant in writing in the event of loss or unauthorised disclosures of information within 24 hours of the event.

The designated points of contact will discuss and agree the next steps relating to the incident, taking specialist advice where appropriate. Such arrangements will include (but will not be limited to) containment of the incident and mitigation of any ongoing risk, recovery of the information, and assessing whether the Information Commissioner and/or the data subjects will be notified. The arrangements may vary in each case, depending on the sensitivity of the information and the nature of the loss or unauthorised disclosure.

Where appropriate and if relevant to the incident, disciplinary misconduct action and/or criminal proceedings will be considered.

Signatories

Signed on behalf of the Home Office.

Signed on behalf of DWP.