Home Office

HM Revenue & Customs

PROCESS LEVEL MEMORANDUM OF UNDERSTANDING (PMoU)

BETWEEN

HER MAJESTY'S REVENUE AND CUSTOMS

AND

THE HOME OFFICE

In Respect of the Exchange of Information for the EU Settlement Scheme

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 PMoU

This is a Process Memorandum of Understanding (PMoU) made under the terms of the overarching Umbrella Memorandum of Understanding (UMoU) between Her Majesty's Revenue and Customs (HMRC) and the Home Office. Any information shared pursuant to this PMoU is subject to the provisions set out in the UMoU between Home Office and HMRC including any conditions set out therein and this PMoU should therefore be read in conjunction with the UMoU

This PMoU will be entered into by UK Visas and Immigration Strategy, Transformation and Performance Team on behalf of the Home Office and CDO, CDIO on behalf of HMRC, who are responsible for the purpose-specific information sharing activity to which this PMoU relates.

Collectively the Home Office and HMRC are referred to as 'Participants', and individually are referred to as a "Participant."

Formalities

Date of review

This MoU will be reviewed annually.

Powers to share personal data between the Participants

The relevant legal bases to share information involving personal data between the Participants are set out below.

Home Office

Section 21 Immigration and Asylum Act 1999;

Section 36 Immigration, Asylum and Nationality Act 2006;

Common Law Power of the Secretary of State (where the above does not apply).

HMRC

Section 18 Commissioners of Revenue and Customs Act 2005 (CRCA) (to be read in conjunction with sections 17 and 20 of that Act and section 19 Anti-Terrorism, Crime & Security Act 2001);

Section 36 Immigration, Asylum & Nationality Act 2006;

Section 40 UK Borders Act 2007.

Lawful bases for processing personal data in accordance with Article 6 of the GDPR

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.”

HMRC

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.”

Privacy Information Notices

Home Office

The Home Office on-line application form for the EU Settlement Scheme will require applicants to agree to a declaration. The declaration will include an understanding that their personal data/information may be shared with other government departments for decision making and immigration purposes and will ensure that the declaration complies with the principles of the GDPR and the Data Protection Act 2018.

HMRC

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

Third Party Processing

No third-party processing will take place.

Data Protection Impact Assessment (DPIA)

The completion of a DPIA for the EU Settlement Scheme has been undertaken by the Home Office.

Controller status of the receiving participant

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

HMRC 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.

The 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 information 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 Home Office to check an applicant's activity in the UK using HMRC and DWP data to support a residency assessment (final decision to be undertaken by a Home Office caseworker). This will be achieved by directly accessing HMRC and/or DWP records in real-time during the online application. The residency assessment will identify, based on the information available, whether or not an applicant is eligible for settled status (ILR) or pre-settled status (LTR).

The online application will be accessible from www.gov.uk giving the applicant a point of access anywhere in the UK and by digital means.

The implementation of the API allowing HMRC and DWP'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

Information to be shared and the systems the information will be derived from

EU Settlement Scheme applicants

To meet the criteria for ILR, EEA nationals must generally provide evidence that they have been continually resident in the UK for five years and that residency has not lapsed. If an applicant does not meet the criteria for settled status, 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 EU national and that EU national ("the sponsor") meets the above residency criteria.

Data to be supplied to HMRC via the API

The individual will enter their details into the Home Office's online application system and will input the following personal data:

- Forename
- Surname
- NINo (optional, but required to generate the API check with HMRC)
- 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 HMRC records.

Data to be supplied by HMRC via the API

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

- Employment start date
- Employment end date
- Date of PAYE payments
- Date Self-Assessment record set up

- Self-Assessment Tax return dates of receipt
- Self-Assessment Tax years
- Self-Assessment total income in each tax year
- Self-employment income in each tax year

The Home Office API will extract relevant information from these records to create a residency footprint based on all PAYE income and the tax years of self-assessment returns that contain income from self-employment.

Type of information sharing activity

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

Method of information sharing

The data will be provided by the applicant as part of their online application. During this online application the API will allow the details to be checked against HMRC systems to identify whether any relevant income records exist. The output from HMRC will be returned in real time and aggregated with information obtained from DWP. This will inform a calculation to determine whether an applicant's UK residence indicates they are eligible for consideration for settled status or pre-settled status under the scheme. Once the application has been submitted, a Home Office caseworker will view the outcome of this calculation to help them make a decision on the application.

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-EU national, the API check may be conducted on the EU national sponsor by the caseworker, but only when satisfactory documentary evidence is available.

Freedom of Information Act (FoIA) Requests

The Participants will demonstrate a commitment to openness and transparency regarding information sharing activities under this PMoU.

In the event that an FoI request relating to information sharing activities under this PMoU is received the Participants accept to consult with the other in line with the Code of Practice made under section 45 of FoIA.

Subject Access Requests (SARs)

Individuals can request a copy of all the information that either Participant holds on them by making a SAR. This may include information that was disclosed to that Participant under this PMoU. Where this is the case, as a matter of good practice, the Participants will liaise with each other to endeavour that the release of the information to the individual will not prejudice any ongoing investigation/proceedings.

Handling of personal data and personal data security

Participants will be deemed to be Controllers (as defined in the Data Protection Act 2018) and as such must ensure that information shared that involves the sharing of personal data is handled and processed in accordance with the Data Protection Act 2018. Additionally, the Participants must process the information being shared in compliance with the mandatory requirements set by 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 Security Policy Framework.

The Participants will ensure effective measures are in place to protect information in their care and manage potential or actual incidents of loss of information. By way of example without limitation, such measures may include:

- information not being transferred or stored on any type of portable device unless absolutely necessary, and if so, it must be encrypted and password protected to an approved standard
- taking steps to ensure that all relevant staff are adequately trained and are aware of their responsibilities under the Data Protection Act 2018 and this PMoU
- access to information received by the Participants pursuant to this PMoU must be restricted to employees on a legitimate need-to-know basis, and with security clearance at the appropriate level
- the Participants will comply with the Government Security Classifications Policy (GSCP) where applicable: Government Security Classification Policy

Accuracy of the shared data

The applicant will enter their details on the online application system; this data will be provided to HMRC via the API. HMRC will 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 HMRC held data is both accurate and up-to-date in accordance with the requirements of the Data Protection Act 2018.

In circumstances where the recipient of the information is intending to use the information to make a decision that will impact directly on the data subject, the receiving Participant must be satisfied that there is sufficient and accurate information available to them before making a final decision and should always seek to clarify, or make further enquiries with the data subject, or with the disclosing Participant in the event that decision is subsequently disputed/appealed by the data subject.

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

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

The data HMRC hold is a snapshot of data taken from legacy systems and as such HMRC are reliant on the benefit processor having input the information correctly. To the best of HMRC'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 HMRC identify any error within the processing, that could affect the eligibility of the applicant, HMRC will adhere to the agreed support model in place.

Data subject’s rights

The Participants have the technical capability and procedures in place to sufficiently comply with all the data subject’s rights under the Data Protection Act 2018 including the technical capability to identify, provide and erase personal data should either Participant be legally required to do so.

Retention and destruction schedule

Raw data accessed from HMRC 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 HMRC 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 information in respect of this PMoU

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

- the appropriate security clearance determined by their own department to handle the data (state level of security level clearance)
- a genuine business need to access the information

Onward disclosure to third parties

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

Roles of each Participant to the PMoU

Role of Home Office

- Data will be provided to HMRC via the API which is the agreed secure transfer method approved by both Participants and within Home Office data security instructions
- Only allow access to the data by those on the whitelist. Neither the applicant nor the caseworker will be able to view HMRC raw data – only the result of the calculation after the EU Settlement Scheme rules have been applied
- Ensure that staff handle this data in line with the 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
- Allow HMRC Internal Audit to carry out an audit in deciding whether HMRC should continue to provide the data, upon request
- Provide written, signed assurance that they have complied with these undertakings regularly upon request
- Provide regular evaluation of the efficacy and value of the information exchange to HMRC to HMRC’s CDO Live Service Team

HMRC

- Identify the appropriate data required to make the search from HMRC 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 HMRC 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 via The Support Model for the Home Office to utilise should the technical process underpinning this data sharing arrangement not function

Monitoring and reviewing arrangements

Regular Exchanges

This PMoU relates to a regular information exchange and will run until April 2026 but must be reviewed at least annually to assess whether the PMoU 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 approved 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.

Complaints handling/ Issues, disputes and resolution

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.

Costs

There are no charges associated with this PMoU.

Termination

This PMoU may be terminated by giving a minimum of three months' notice by either Participant.

The Participants to this PMoU reserve the right to terminate this PMoU in the following circumstances:

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

Where the information sharing relates to a one- off information sharing activity, the PMoU will terminate upon completion of the exercise.

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

Personal Data Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to personal data transmitted stored or otherwise processed.

Examples of serious personal data breaches may include

- accidental loss or damage to the personal data
- damage or loss of personal data by means of malicious software/hacking
- deliberate or knowingly disclosure of personal data to a person not entitled to receive the data
- emailing classified/sensitive information containing personal data to personal email accounts
- leaving classified/sensitive papers containing personal data in an unsecure or publicly accessible area
- using social networking sites to publish information containing personal data which may bring either Participant's organisations into disrepute
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

The designated points of contact are responsible for notifying the other Participant in writing in the event of personal data breach within 24 hours of the event.

The designated points of contact will discuss and jointly decide 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 personal data, 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 personal data and the nature of the loss or unauthorised disclosure.

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

Signatories

Signed on behalf of the Home Office.

Signed on behalf of HMRC.