Home Office

Data Protection Impact Assessment (DPIA)

EU Settlement Scheme

Proposal/ Project/Activity title	**EU Settlement Scheme**
Information Asset Owner(s)	**Gabrielle Monk**

Final Version 1.0

Home Office

Contents

Data Protection Impact Assessment

Document Control 2

DPIA Stage 1 3

DPIA Stage 2 7

Section 1: Background and contacts 7

Section 2: Personal Data 8

Section 3: Purpose of the Processing 19

Section 4: Processing Activity 21

Section 5: Risks of the Processing 26

Section 6: Data Sharing/Third party processing 27

Section 7: International transfers 31

Section 8: Referal to ODPO 32

Section 9: Referal to Data Board 32

Home Office

DPIA Stage 1

Summary of the processing

1. Does the proposal/project/activity involve the processing[1] of personal data, or is new legislation which relates to the processing of personal data being considered?[2]

☒ Yes ☐ No

If the answer to this question is 'No', then the rest of the form does not need to be completed. If the answer is 'Yes', please continue.

2. Does the proposal/project/activity involve any of the following?

- a new way of processing personal data
- the use of a new form of technology for a new or existing process
- new legislation which relates to the processing of personal data being considered
- substantial changes to an existing project/programme/processes involving personal data, which would include a significant increase in the volume or type (category) of data being processed

☒ Yes ☐ No

If the answer to this question is 'No', then the rest of the form does not need to be completed. If the answer is 'Yes', please continue.

3. What is the purpose of the processing?

The EU Settlement Scheme will enable EEA and Swiss citizens resident in the UK by the end of the transition period (31 December 2020), and their family members, to obtain the UK immigration status which they will require in order to remain here

[1] In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).
[2] Data protection legislation applies to 'personal data' which is defined as any information which relates to a living identifiable person who can be directly or indirectly identified by reference to an identifier. The definition is broad and includes a range of items, such as name, identification number, location data, or on-line identifier etc.

after 30 June 2021. It will also enable family members of people of Northern Ireland to obtain a UK immigration status on broadly the same terms as family members of Irish citizens

Screening questions

4. **Does the processing activity include the evaluation or scoring of any of the following?**
    - profiling and predicting (especially from “aspects concerning the data subject's performance at work”)
    - economic situation
    - health
    - personal preferences or interests
    - reliability or behaviour
    - location or movements.

    ☐ Yes ☒ No

5. **Does the processing activity include automated decision-making with legal or similar significant effect?** i.e. processing that is intended to take decisions about data subjects which will produce “legal effects concerning the natural person” or which could “significantly affect the natural person”.

    ☐ Yes ☒ No

    Although automated processes are involved, an actual caseworker takes the decision whether to grant status under the Immigration Rules.

6. **Does the processing activity involve systematic monitoring?** i.e. processing used to observe, monitor or control data subjects, including data collected through networks or “a systematic monitoring of a publicly accessible area” e.g. CCTV.

    ☐ Yes ☒ No

7. **Does the processing activity involve mostly sensitive personal data?** This includes special categories of personal data, data about criminal convictions or offences, or personal data with the security marking of Secret or Top Secret.

    ☒ Yes ☐ No

The EU Settlement Scheme will collect data regarding criminal convictions and offences, which applicants are asked to declare.

The photographs uploaded during the application may indicate racial/ethnic origin and identity documents will confirm nationality.

Marriage certificates may indicate religious belief, but this has no bearing on any decision. Civil partnership certificates or evidence of a durable same-sex partnership may indicate sexual orientation, but this has no bearing on any decision.

Where family members are applying, any required evidence of dependency may include details of a physical or mental health condition or other data of a highly personal nature.

Where applicants are unable to provide the required identity document due to compelling practical or compassionate reasons, the evidence they present in relation to those reasons may include details of physical or mental health conditions or other data of a highly personal nature.

Data received from the Department for Work and Pensions (DWP) or HM Revenue & Customs (HMRC) may disclose personal data such as disability, maternity, etc, but this has no bearing on any decision.

Biometric data will be collected (photographs for all applicants, fingerprints for non-EEA citizens without a biometric residence card issued under the EEA Regulations).

Information may be supplied that confirms a person's gender or change in gender, but this has no bearing on any decision

8. **Does the processing activity involve data processed on a large scale?** If sharing with a third party external to the Home Office large scale is defined as 1,000 plus pieces of personal data in a single transaction or in multiple transactions over a cumulative 12 month period.

   ☒ Yes ☐ No

9. **Does the processing activity involve matching or combining datasets that are being processed for different purposes?** e.g. data originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject. *NB:* This does not include matching or combining datasets from different IT systems that are processed for the same purpose and legal basis e.g. CID and CRS.

☒ Yes ☐ No

10. **Does the processing activity involve mostly data concerning vulnerable data subjects or children?**

☐ Yes ☒ No

A significant number of applicants will be children or vulnerable adults.

11. **Does the processing activity involve the innovative use or application of new technological or organisational solutions?** e.g. combining use of fingerprints and facial recognition for improved physical access control, etc.

☒ Yes ☐ No

12. **Will the processing activity in itself prevent data subjects from exercising a right (under Data Protection Legislation and the UK GDPR) or using a service (provided by) or a contract (with) the Department?**

☐ Yes ☒ No

13. **Is the introduction of new legislation or a legal regulatory measure which relates to the processing of personal data being considered?**

NB: If yes, this may require consultation with the Information Commissioner.

☐ Yes ☒ No

If you have answered 'yes' to more than one of the above screening questions (Q 3 to 12), a DPIA must be completed. If you have answered 'no' to each of the screening questions but feel the planned policy/process/activity is significant, or carries reputational or political risk, you should complete the full DPIA. If you are not sure whether a DPIA should be completed, please consult the Office of the Data Protection Officer (ODPO).

If you have completed Stage 1 and do not need to complete Stage 2, send your Stage 1 assessment to the ODPO.

Home Office

DPIA Stage 2

Section 1: Background and contacts

1.1 Proposal/Project/Activity title:
EU Settlement Scheme

1.2 Information Asset title(s) (if applicable):

EU Settlement Scheme Data

1.3 Information Asset Owner(s) (IAO):

Email:	<Redacted>
Name:	Gabrielle Monk
Telephone Number:	<Redacted>
Information Asset title:	EU Settlement Scheme

1.4 Person completing DPIA on behalf of the IAO named at 1.3 above):

Email:	<Redacted>
Name:	<Redacted>
Telephone Number:	<Redacted>
Business Unit/Team:	<Redacted>

1.5 Date DPIA commenced:
30/03/2019

1.6 Date processing activity to commence (if known):
30/03/2019

NB: if the processing activity is already ongoing, please explain why the DPIA is being completed retrospectively.

The DPIA is not retrospective it is a living document, it existed in an earlier iteration for earlier processing.

1.7 Information Asset Register reference (if applicable):
EU Settlement Scheme

1.8 DPIA version:
1.0 Final 1.0

1.9 Linked DPIAs *NB*: attach word versions, do not provide links.

View and prove online status service

Update My Details (UMD) Service (EUSS)

1.10 DPIA proposed publication date (where applicable, and if known):

The date of publishing is to be confirmed.

The DPIA will be published on an ad hoc basis to fulfil previous commitments made to Parliament and to citizens in responses to Parliamentary Questions and FOI requests.

Section 2: Personal Data

2.1 What personal data is being processed?

An application to the EU Settlement Scheme requires the collection and processing of personal data as follows: Evidence of Identity: Names Nationality, including dual or previous nationality Date of Birth Sex Passport or national identity card or Home Office issued biometric residence card issued under the EEA Regulations or biometric residence permit – meta data (number, date of issue, expiry date, issuing authority, certificate information), including an image of the document. Alternative evidence of identity and nationality where the Secretary of State agrees to accept alternative evidence where the applicant is unable to obtain or

produce the required document due to circumstances beyond their control or to compelling practical or compassionate reasons.

Biometric Data:

Photographic images of applicant

Fingerprints of non-EEA citizen applicant without a biometric residence card issued under the EEA Regulations.

Evidence of Residence:

National Insurance number, if provided (it is made clear on the online and paper application forms that providing a National Insurance number is optional).
Applicants also have an option to provide documentary evidence of residency.

Data from HMRC & DWP:

As outlined in the respective Processing Memorandum of Understanding agreed between Home Office, DWP and HMRC, raw data accessed from their systems will only be available for the duration of the period of calculation and will not be retained by the Home Office.

A summary will be produced relating to qualifying months HMRC and DWP holds records for pertaining to the applicant.

Further guidance can be found at https://www.gov.uk/guidance/eu-settlement-scheme-uk-tax-and-benefits-records-automated-check

Immigration History:

Permanent Residence document issued under the EEA Regulations.

Indefinite Leave to Enter or Remain granted under UK law.

Any other previous immigration history.

Evidence of Suitability

Declaration of criminality in the UK and overseas.

Declaration of security, terrorism, and war crimes.

Home Office checks of Police National Computer and Warnings Index.

Evidence of Relationship

Documentary evidence supplied to prove a family relationship, e.g. birth certificate; marriage certificate; civil partnership certificate; Home Office issued residence card; non-prescriptive evidence demonstrating a durable relationship; non-prescriptive evidence demonstrating that an applicant is dependent on their sponsor, or a member of their household or in strict need of their personal care on serious health grounds.

Contact information

Email address and telephone numbers for the applicant and any person who assisted them in completing the application.

Memorable answers for the purposes of authentication of the person if they contact the Home Office to discuss the application.

Note:

The EU Settlement Scheme also includes applications based on EU law derivative rights, e.g. Surinder Singh, Zambrano carers. These basically reflect existing requirements under the EEA Regulations and the data required is much the same as for a residence document in those categories under the EEA Regulations. For example, where the applicant is applying as a family member of a qualifying British citizen (Surinder Singh), the applicant will be required to provide evidence that they resided together in the host member state and that genuine family life was created or strengthened during that residence. Those elements are not included in detail in this DPIA; the personal data processed for the applicant is otherwise equivalent to that for an EEA citizen applying under the EU Settlement Scheme as outlined in this section.

The EU Settlement Scheme also includes applications based on retained rights under the Free Movement Directive, e.g. following the termination of the applicant's marriage or civil partnership to an EEA citizen and whether other criteria are met, such as their continued residence being warranted by "particularly difficult circumstances", such as being the victim of domestic abuse, with the evidence they present including data of a highly personal nature.

The EU Settlement Scheme has also been available to the family members of the people of Northern Ireland since 24 August 2020. An application requires the collection and processing of personal data as for any EUSS applicant but in

addition the provision of evidence that the person of Northern Ireland is British, Irish or both; was born in Northern Ireland; and at the time of their birth at least one of their parents was British, Irish, both or otherwise entitled to reside in Northern Ireland without any restriction on their period of residence.

2.2 Which processing regime(s) applies: general processing regime (UK GDPR/Part 2 DPA), and/or law enforcement processing regime Part 3 DPA?

General processing (UK GDPR/Part 2 DPA) ☒

Law enforcement (Part 3 DPA) ☐

The primary purpose for processing is administrative (UK GDPR Part 2). However, we may on a case by case basis also process personal data under Part 3 (law enforcement processing) of the Data Protection Act where this is appropriate. Part 3 processing is outside of the remit of this DPIA and core application processing.

2.3 Does the processing include any of the following special category, or criminal conviction data?

Criminal conviction data	☒	Yes	☐ No
Race or ethnic origin (including nationality)	☒	Yes	☐ No
Political opinions	☐	Yes	☒ No
Religious or philosophical beliefs	☐	Yes	☒ No
Trade union membership	☐	Yes	☒ No
Genetic data or biometric data for the purpose of uniquely identifying individuals	☒	Yes	☐ No
Health	☒	Yes	☐ No
Sexual orientation or details of the sex life of an individual	☒	Yes	☐ No

Race or ethnic origin (including nationality)

Yes, the applicant must state what nationality (or nationalities) they hold or have held. The photographs uploaded during the application process may indicate racial/ethnic origin.

Political opinions

No.

Religious or philosophical beliefs

It is not a requirement to declare or assess religious or political beliefs, but documents provided to support an application may identify a religious belief. This information will be retained in the form of document scans but not specifically recorded as an item of data on the case working systems.

Trade Union membership

It is not a requirement to declare or assess any membership of Trade Unions, but documents provided to support an application, e.g. payslips, may identify membership of a Trade Union. This information will be retained in the form of document scans but not specifically recorded as an item of data on the case working systems.

Genetic data or biometric data for uniquely identifying individuals

Yes. Biometric data will be collected during the application process – photographic images for all applicants, and fingerprints for non-EEA citizens without a biometric residence card issued under the EEA Regulations – for the purposes of identity verification.

Health

Yes, where relevant to the applicant's eligibility under the scheme. For example, evidence demonstrating that an applicant is dependent on their sponsor, or a member of their household or in strict need of their personal care on serious health grounds, may include details of a physical or mental health condition.

Data received from DWP regarding benefits entitlement may disclose data such as disability or maternity.

Health information may also be provided to the Home Office in a request for Assisted Digital support, to apply without the required identity document or for an exemption to providing fingerprint biometrics.

Sexual orientation or details of the sex life of an individual

Yes, evidence of a civil partnership or of a durable same-sex partnership may indicate sexual orientation, but sexual orientation or that a relationship relied upon is same-sex has no bearing on any decision. This information will be retained in the form of document scans but not specifically recorded as an item of data on the case working systems.

2.4 Does it include the processing of data relating to an individual aged 13 years or younger?

☒ Yes ☐ No

Yes. The personal data required to be processed is the same for children as for adults, except that we do not enrol the fingerprint biometrics of non-EEA children aged under 5 years or require persons under the age of 18 to declare criminal convictions.

2.5 (If 'yes') What additional safeguards are necessary for this processing activity? If none, explain why.

The duty in section 55 of the Borders, Citizenship and Immigration Act 2009 to have regard to the need to safeguard and promote the welfare of a child under the age of 18 in the UK, together with Article 3 of the UN Convention on the Rights of the Child, means that consideration of the child's best interests must be a primary consideration in immigration decisions affecting them. A child applicant's personal data will be processed in the same way, and subject to the same safeguards, as others, and subject also to any additional measures required to safeguard and promote the child's best interests, such as referral to the relevant local authority where there are safeguarding concerns.

We have a duty to safeguard and ensure the security of individuals personal information. We do that by having systems and policies in place to limit access to their information and prevent unauthorised disclosure. Staff who access personal information must have appropriate security clearance and a business need for accessing the information, and their activity is subject to audit and review.

2.6 Will data subjects be informed of the processing?

☒ Yes ☒ No

Yes, in the processing of an application,

No, where it is a safeguarding referral and informing the data subject of the referral may place them at risk.

2.7 (If 'yes') How will they be informed/ notified?

Yes, in the processing of an application.

Individuals applying under the scheme will be aware of how their data may be used via the Borders, Immigration and Citizenship: Privacy Information Notice and

a “how we use your personal information” guidance page for the scheme – a link to this is provided to each applicant during the online application process and those who request a paper form receive this in hard copy. The application forms for the scheme require the applicant to sign/agree to a declaration. This includes confirmation that they understand that their personal data /information may be shared with other government departments (DWP/HMRC) for decision-making and immigration purposes. This declaration ensures that the application process complies with the GDPR and data protection legislation transparency, disclosing who with and how we share their personal data.

No, where it is a safeguarding referral and informing the data subject of the referral may place them at risk In some cases, a referral to local authority/police where the application reveals that there are safeguarding concerns for a child may be required and the Home Office will act in the child’s best interests.

2.8. Which HO staff and/or external persons will have access to the data?

Data may be accessed by the Home Office staff responsible for the processing of and decision-making on applications under the scheme, and for related purposes, such as providing guidance to applicants who contact the Settlement Resolution Centre.

Data may be accessed by officials from the Home Office who are assigned to assess the application or the results of criminality and security checks.

Home Office staff who have both a duty and legal powers to view a person’s status in a specific context, e.g. Border Force when a person enters or leaves the UK and Immigration Enforcement to confirm a person’s status and take action as appropriate where a person has no legal basis for remaining in the UK.

Home Office staff who are required to provided statistical analysis and the publication of reports.

Home Office staff who are required to maintain the live service of the system, resolving technical, policy or legal issues on a case by case basis.

2.8a. How will access be controlled?

Access to the data is governed by role-based access control. Staff must first be nominated by a manager prior to being added to an access group. The dataset available to staff is limited to only the information required to perform their duties.

IT administrators also have access to this data which is also managed by role-based access control. Access to the data is granted on a need to know basis and

only given to those IT administrators who have the appropriate clearance and who have a valid requirement to access live data. Access to live datasets is audited on an ongoing basis.

2.9 Where will the data be stored?

The data is stored by the Home Office in its immigration databases.

2.10 If the data is being stored electronically, does the storage system have the capacity to meet data subject rights (e.g. erasure, portability, suspension, rectification etc)?

☒ Yes ☐ No

2.11 If 'Yes' explain how these requirements will be met.

The system meets the Home Office guidelines on the storage and care of data as set out in the official Home Office guidance.

Applicants can exercise all their right to request personal information that is held in the Home Office's immigration records including any standalone systems. This includes making a Subject Access Request. There are three types of request an applicant can make, all of which are free of charge. The three types of requests are Basic, Specific and Detailed. Requests can be made in writing or by completing an online application form which can be accessed via this link:

https://visas-immigration.service.gov.uk/product/saru

2.12 For law enforcement processing only: If the data is being stored electronically, does the system have logging capability (as per s.62 DPA)?

☒ Yes ☐ No

If 'no', what action is being taken to ensure compliance with the logging requirement?]

N/A

[2.13 For law enforcement processing only: Will it be possible to easily distinguish between different categories of individuals (e.g. persons suspected of having committed an offence, victims, witnesses etc.) as well as between factual and non-factual information (as per s.38 DPA)?

☒ Yes ☐ No

If 'no', what action is being taken to ensure compliance with s.38 DPA?]

The scheme's primary purpose for processing is administrative (UK GDPR Part 2) and on a case by case basis will also process data under Part 3 (law enforcement processing) of the Data Protection Act 2018 where this is appropriate and in strict accordance with Data Protection legislation.

Whilst applicants to the EU Settlement Scheme are case worked on a specific database, information on individuals suspected of committing a crime or have been convicted of a criminal offence will be recorded on other Home Office Immigration systems and as such can be accessed. Part 3 processing is outside of the remit of this DPIA and core application processing.

2.14 What is the retention period for the data?

The Borders, Immigration and Citizenship privacy information notice provides information on how personal information is used within the borders, immigration, and citizenship system and how long information will be held for. https://www.gov.uk/government/publications/personal-information-use-in-borders-immigration-and-citizenship

The EUSS is however a new scheme which is distinctly different from other routes and requires a different set of considerations to determine a proportionate retention period.

The rights granted by the EU Withdrawal Agreement (and by the EEA EFTA Separation Agreement and the Swiss Citizens' Rights Agreement) are more far reaching than those which can be granted to any other foreign nationals applying for immigration to the Home Office. The Citizens' Rights Agreements protect the rights of EEA and Swiss citizens who were residing in the UK, and UK nationals who were residing in the EEA or Switzerland, at the end of the transition period on 31 December 2020 and of their family members. The Agreements protect their right to be joined by their existing close family members at any point in the future, where the family relationship was formed by the end of the transition period (or a child is born or adopted after the transition period) and continues to exist when the family member seeks to join them.

The longevity of rights under the Citizens' Rights Agreements means those granted EUSS status will be relying on their digital status to evidence those rights for decades to come and, where they are granted settled status (indefinite leave to enter or remain in the UK) under the EUSS, this may be relevant to the status

(British citizenship) of a child born to them.

As well as retaining the immigration status outcome, data from the relevant application made will need to be retained. For example, to demonstrate an accurate record of the products that a person applied for and when, and their circumstances at the time.

This is so that when future applications are made by that individual, or by their family members eligible to join them under the Citizens' Rights Agreements, records held by the Home Office can be used to help evidence the basis for the application.

To allow for this information to be available to support relevant applications made by or in respect of EEA or Swiss citizens born in the UK just before the end of the transition period, and by or for children, grandchildren and great-grandchildren of primary rights holders under the Agreements, the EUSS retention period will be 100 years from the last application outcome.

2.15 How will data be deleted in line with the retention period and how will the deletion be monitored?

Data will be deleted in line with the data retention period via the monitoring of data retention and deletion policy and processes so that operating processes adhere to the required legislation, including Data Protection legislation, Freedom of Information Act 2000, Sec. 46 and the organisational guidelines relating to the disposal of information.

However, it should be noted that as a result of the Independent Inquiry into Child Sexual Abuse, which commenced in February 2015, the Permanent Secretary placed a moratorium on the disposal of all information throughout the Home Office, including all operational records and case files. This is currently in force and will remain so until further notice.

2.16 If physically moving/sharing/transferring data outside the Home Office, how will it be moved/shared?

Please see the information provided at paragraph 2.17 below

2.17 What security measures will be put in place to ensure the transfer is secure?

All Home Office staff who handle personal data are required to do so lawfully and correctly, adhering to the Data Protection Principles. This includes requiring all Home Office staff and any suppliers directly involved in the processing of personal data to complete appropriate training on a regular basis, and for Information Asset Owners to be responsible for ensuring adequate safeguards and control measures are in place within their assigned area of control.

We make the most of the available technology and processes to mitigate the risk of information disclosure when moving data. In summary, they are:

- Protection of information in transit by default with the use of virtual private networks (VPN) as well as end to end application level encryption.
- Enforcing need to know using logical access controls.

Understanding security reviews and penetration testing to validate the effectiveness of risk mitigation.

Information is transmitted via VPN and end to end app level encryption when sent across public network infrastructure.

Encryption of data at rest.

Seeking formal approval from the Information Assets Owner prior to any data transfer.

Utilising a commercial data sharing platform, specifically procured by the Home Office for the purpose of sharing data securely.

2.18 Is there any new/additional personal data being processed? This includes data obtained directly from the data subject or via a third party.

☒ Yes ☐ No

If 'yes', provide details below:

Applications to the scheme largely require the provision by the applicant of generic personal data required by other immigration applications or in applications for the issuing of documentation under the EEA Regulations. The online application also includes provision for real-time automated checks of some HMRC and DWP data to use this as evidence of UK residence and thereby remove or minimise the need for the applicant to provide documentary evidence of that residence, and includes the scope for the applicant to self-verify their identity through a smartphone app. The personal data collected and processed is set out in section 2.1.

2.19 What is the Government Security Classification marking for the data?

OFFICIAL/OFFICIAL-SENSITIVE	☒
SECRET	☐
TOP SECRET	☐

2.20 Will your processing include the use of Cookies?

☒ Yes ☐ No

If 'no' go to section 3.

If 'yes', what sort of Cookies will be used? Tick the correct categories:

1) Essential (no consent required)	☒	Yes	☐	No
2) Analytical (consent required)	☒	Yes	☐	No
3) Third party (consent required)	☐	Yes	☒	No

2.20.a. If cookies fall into categories 2) & 3) **how will you ensure data subjects are aware and can give active consent to the use of cookies?**

Essential cookies are used to store the session ID. They are required as some of the services are session based and if not used the applicant will not be able to use the application process.

Analytical cookies are saved to the user's device information, but no personal information is stored and would for example include which pages they have visited.

The applicant will see a banner which outlines that gov.uk uses cookies to make the site simpler and seeks the applicant's consent. Once accepted the applicant will be informed that cookies have been accepted and a link is provided advising them that the cookie settings can be changed by them at any time.

Section 3: Purpose of the Processing

3.1 What is the purpose of the processing?

The EU Settlement Scheme will enable EEA and Swiss citizens resident in the UK by the end of the transition period (31 December 2020), and their family members, to obtain the UK immigration status which they will require in order to remain here after 30 June 2021. It will also enable family members of people of Northern

Ireland to obtain a UK immigration status on broadly the same terms as family members of Irish citizens.

3.1.a Which processing regime(s) applies: general processing regime (UK GDPR/Part 2 DPA), and/or law enforcement processing regime Part 3 DPA?

General processing (UK GDPR/Part 2 DPA) ☒

Law enforcement (Part 3 DPA) ☐

The primary purpose for processing is administrative (UK GDPR Part 2). However, we may on a case by case basis also process personal data under Part 3 (law enforcement processing) of the Data Protection Act 2018 where this is appropriate. Part 3 processing is outside of the remit of this DPIA and core application processing.

3.2. <u>General processing only</u>: What is the (UK GDPR Article 6) lawful basis for the processing?

Consent	☐
Contract	☐
Legal obligation [see 3.3(a)]	☐
Vital Interest	☐
Performance of a public task [see 3.3(a)]	☒
Legitimate Interest	☐

3.2.a. <u>General processing only</u>: If processing special category data or criminal convictions data
What is the (UK GDPR Article 9) condition for processing the special category data?

N/A	☐
Consent	
Employment/Social Security	☐
Vital Interests	☐
In the public domain	☐
(Exercising/defending) legal rights	☐
Substantial Public Interest	☒
Public healthcare	☐
Archiving or Research	☐

Appropriate Policy Document: Special Category Data UKGDPR Part 2 DPA

3.3. Is the purpose for processing the information described at 3.1 above the same as the original purpose for which it was obtained by the Department?

☒ Yes ☐ No

The information was originally collected for the purpose as set out in 3.1. The Home Office may, in very limited circumstance, process the data for other purposes, but only to carry out its statutory duties (e.g. for safeguarding or law enforcement). This is set out in the scheme-specific privacy information notice on gov.uk. "how we use your personal information" guidance page

Individuals applying under the scheme will be aware of how their data may be used via the Borders, Immigration and Citizenship: Privacy Information Notice and a "how we use your personal information" guidance page for the scheme – a link to this is provided to each applicant during the online application process and those who request a paper form receive this in hard copy. The application forms for the scheme require the applicant to sign/agree to a declaration. This includes confirmation that they understand that their personal data /information may be shared with other government departments (DWP/HMRC) for decision-making and immigration purposes. This declaration ensures that the application process complies with the GDPR and data protection legislation transparency, disclosing who with and how we share their personal data.

Section 4: Processing activity

4.1 Is the processing replacing or enhancing an existing activity or system?

If so, please provide details of what that activity or system is and why the changes are required.

☐ Yes ☒ No

This is a new scheme designed to enable EEA and Swiss citizens resident in the UK by the end of the transition period (31 December 2020), and their family members, to obtain the UK immigration status which they will require in order to remain here after 30 June 2021. It will also enable family members of people of Northern Ireland to obtain a UK immigration status on broadly the same terms as family members of Irish citizens.

4.2 Is the processing a new activity?

☒ Yes ☐ No

Yes, but in line with the primary purpose of the Home Office in the provision of immigration status and operation of immigration controls.

4.3 How many individual records or transactions will be processed (annually) as a result of this activity?

Based on Office for National Statistics Annual Population Survey data, Home Office internal analysis estimates that the total number of EEA citizens and their family members eligible to apply for the EU Settlement Scheme by the end of the transition period on 31 December 2020 is likely to be between 3.5 million and 4.1 million.

We are unable to predict annual application numbers however, to continue to meet user needs and to better understand the number of applicants to the scheme, the Home Office has been exploring ways to identify repeat applications by individuals.

The latest quarterly statistics (up to 30 September 2021), show that 9% of applications were from repeat applicants (530,290). This indicates that an estimated 5.66 million people had applied to the scheme by the end of September 2021. Further information and detailed breakdowns of EUSS applications can be found in the latest quarterly EUSS statistical release at https://www.gov.uk/government/collections/eu-settlement-scheme-statistics

These estimates cannot be directly compared with estimates of the resident population of EU/EEA nationals in the UK, as figures include non-EEA national family members and eligible EEA nationals not resident in the UK. None of these are usually included in estimates of the resident EU/EEA population. Further information on this can be found in the Home Office EU Settlement Scheme statistics User Guide at Home Office EU Settlement Scheme statistics: user guide - GOV.UK (www.gov.uk)

4.4 Is this a one-off activity, or will it be frequent and/or regular?

This is a bespoke scheme designed to enable EEA and Swiss citizens resident in the UK by the end of the transition period, and their family members, to obtain the UK immigration status which they will require in order

to remain here after 30 June 2021. The deadline for applying, for those resident here by 31 December 2020, will be 30 June 2021, with scope for a late application to be made by those with reasonable grounds for missing the deadline. It will also enable family members of people of Northern Ireland to obtain a UK immigration status on broadly the same terms as family members of Irish citizens. Those EEA and Swiss citizens resident in the UK by the end of the transition period and granted status under the scheme, and relevant people of Northern Ireland, will have a lifetime right to be joined by their existing close family members and future children, who will also be able to apply for status under it and in those circumstances the scheme will continue to operate indefinitely.

4.5 Does the processing directly relate to the processing of personal data that includes new legislative measures, or of a regulatory measure based on such legislative measures? If 'no', move onto 4.6.

☒ Yes ☐ No

4.6 If the answer is yes, please explain what that processing activity is, including whether or not the HO will be accountable for the processing of personal data?

The EU Settlement Scheme will enable EEA and Swiss citizens resident in the UK by the end of the transition period (31 December 2020), and their family members, to obtain the UK immigration status which they will require in order to remain here after 30 June 2021. It will also enable family members of people of Northern Ireland to obtain a UK immigration status on broadly the same terms as family members of Irish citizens.

4.7 Does the processing activity involve another party? (This includes other internal HO Directorates, external HO parties, other controllers or processors).

☒ Yes ☐ No

4.8. In what capacity is the other party acting?

- Part of the HO ☒
- Controller in their own right (i.e. non HO) ☐
- Joint Controller with the HO ☐
- Processor (public body) on behalf of the HO ☒
- Processor (non-public body) on behalf of the HO ☒

Data is available to Borders, Immigration and Citizenship directorates within the Home Office and a subset of data to two other Government Departments (DWP and HMRC) involved in the processing of information from applicants who choose to provide their National Insurance number to help assess UK residence.

Some applicants to the EUSS will be non-EEA citizens. In these circumstances, as well as providing biometrics and supporting evidence in their EUSS application, they will also need (if they do not have a biometric residence card issued under the EEA Regulations) to enrol their biometrics in person with a Home Office commercial partner.

In such cases, at the end of their EUSS application form, the customer will be signposted to the commercial partner's website. The customer will need to click a button on the application form that will hand them, along with a subset of their own data provided within their EUSS online journey, to the commercial partner's website.

This is to improve their customer journey by integrating their application with the commercial partner's booking process rather than the customer having to create a separate account before they attend their appointment.

Information regarding organisations having access to personal information can be found in the privacy notices for the HO Borders, immigration and citizenship: privacy information notice - GOV.UK (www.gov.uk) and the UK Visa and Citizenship Application Services (ukvcas.co.uk) including UK Visa and Citizenship Application Services EUSS FAQs

We use private sector companies within the UK or EEA as part of this work. Each is contracted to the Home Office to act on behalf of the Home Office where the Home Office remains the data controller and full details are included in section 6.

4.9 Will any personal data be transferred outside the UK?

☐ Yes ☒ No

No. We will not generally be transferring data outside the EEA. There may, however, on a case by case basis be a need for information supplied in an application as documentary evidence to be verified with the organisation that generated the original document. It is possible that these organisations may be outside the EEA, e.g. a University at which the applicant is studying

(which, for a period of up to 12 months, will not break the continuity of their UK residence for the purposes of an application for status under the scheme).

When we do this, we seek to take appropriate steps to safeguard information, for example by agreeing a memorandum of understanding. We may rely on the "public interest "derogation in Article 49(1)(d) of the UK GDPR where necessary.

4.10 Does the proposal involve profiling that could result in an outcome that produces legal effects or similarly significant effects on the individual?

☐ Yes ☒ No

4.11 Does the proposal involve automated decision-making?

☐ Yes ☒ No

No, decision making resides with a caseworker for each application.

4.12 Does the processing involve the use of new technology?

☒ Yes ☐ No

If 'yes': Describe the new technology, including details of the supplier and technical support.

The EU Exit: ID Document Check app, which the applicant can use to self-verify their identity, represents new technology for the Home Office, although the core checks performed by the app are fundamentally based around mature processes which have been successfully utilised by the Home Office in the immigration system for many years.

In summary, the app process is very similar to the e-gates deployed at the UK border. The app performs digital security checks on an applicant's biometric passport, national identity card or biometric residence card to verify that the document is genuine, and the data has not been tampered with. The app then uses facial matching technology to verify that the applicant is the rightful holder of that genuine document. The app also includes a "liveness check" to verify genuine presence and confirm a real person is using the app.

The app was developed by a commercial partner working closely with Home Office teams. The live service is also supported by the same commercial

partner. Further details can be found here relating to personal information and checks identity checks https://www.gov.uk/guidance/eu-settlement-scheme-how-we-use-your-personal-information

4.13 Are the views of impacted data subjects and/or their representatives being sought directly in relation to this processing activity?

☒ Yes ☐ No

Yes, via the user groups representing EU citizens and others, including vulnerable groups, advising the Home Office on the development and operation of the scheme and through the testing phases which preceded the opening of the scheme on 30 March 2019.

Section 5: Risks of the Processing

5.1 Are there any other known, or anticipated risks associated with the processing of personal data that have been identified by the project/ programme/initiative owner, which have not been captured in this document?

☒ Yes ☐ No

Applications to the scheme largely require the provision by the applicant of generic personal data required by other immigration applications or in applications for the issuing of documentation under the EEA Regulations. The risks associated with the processing of personal data in this scheme, e.g. persons attempting to access data that is not their own and loss of data in electronic or physical form, are the same as in other operations, but the scheme has implemented changes to mitigate these similar risks further.

5.2 What steps have been taken to mitigate these risks?

The ability for the persons to self-verify their identity via the EU Exit: ID Document Check app.

The immediate return of identity documents submitted by post and before the decision on the application.

Two factor authentications for persons saving and returning to their application online.

Verification of email and phone in the application process to confirm the applicant has access to these.

Verification of memorable answers if a person contacts the Settlement Resolution Centre for guidance, to ensure the person asking about the application is the person who made the application or their representative.

The use of Application Programming Interfaces with HMRC and DWP, minimising the volume and type of documentary evidence an applicant may have to submit.

Processes that require the consent of the applicant before allowing any third party claiming to represent them from accessing information.

Two factor authentications for accessing status information online once status under the scheme has been granted.

5.3 Can you demonstrate that the risks to the individuals are sufficiently balanced by the perceived public protection benefits?

☒ Yes ☐ No

If 'yes' provide details and go to question 5.4.

The risks of the data processing are not considered to outweigh the public interest benefits of granting status in the UK promptly and efficiently to those eligible for the scheme. Further information on this is outlined in answer 5.2 above and relevant risk registers.

5.4 Are these risks included within a risk register?

☒ Yes ☐ No

Section 6: Data Sharing/Third party processing

Complete this section if you have answered 'yes' to question Q.4.7.

6.1 External contact details for data exchange/ processing

For the EU Exit: ID Document Check app:

World Reach Software
<Redacted>

For HMRC data:
Redacted>

<Redacted>
<Redacted>

<Redacted>

For DWP data:
<Redacted>
<Redacted>
<Redacted>
<Redacted>

For commercial partners and enrolment of biometrics.
<Redacted>

6.2 How long will the data be retained by the receiving organisation or processor for the purpose for which it is received?

***See 2.14**

(See 2.8 ,2.9 and 2.10) Data accessed from HMRC and DWP systems will only be available to the system for the duration of the calculation (in real time) of the UK residence indicated by that data and will not be retained by the Home Office.

For the EU Exit: ID Document Check app, no personal information is retained on either the applicant's device, or the systems of the relevant commercial partner, which transfer data instantaneously to the Home Office which is then deleted upon confirmation of receipt in real time. The only exception are the images used for the liveness check, which are retained on commercial partner systems for 2 days where the check was passed or 60 days where it was failed – this is a core part of the liveness check service allowing our commercial partner to detect patterns of fraudulent use. The Home Office continues to review the time period for which these images are held by the commercial partner. The relevant commercial partner retains a range of non-identifiable, non-attributable telemetry data to monitor performance of the app and inform service improvements.

For commercial partners and enrolment of biometrics mentioned in paragraph 4.6 information on how long that data will be retained for can be found in the privacy notice UK Visa and Citizenship Application Services (ukvcas.co.uk)

6.3 How will it be destroyed by the receiving/ processing organisation once it is no longer required for the purpose for which it has been received?

***See 2.15**

(See 2.8 ,2.9 and 2.10)

Data accessed from HMRC and DWP systems will only be available to the system for the duration of the calculation (in real time) of the UK residence indicated by that data and will not be retained by the Home Office. The Home Office will apply the continuous qualifying period rules for the scheme reflected in Appendix EU to the Immigration Rules to produce a summary of qualifying months of UK residence indicated by this calculation. No further details will be retained. This summary will be stored on Home Office systems. Further guidance can be found at https://www.gov.uk/guidance/eu-settlement-scheme-uk-tax-and-benefits-records-automated-check

For the EU Exit: ID Document Check app, the commercial partners have clearly documented processes for the deletion of data and compliance is actively monitored by the Home Office Data and Security teams, including through internal audits and site visits.
(See 2.8 ,2.9 and 2.10) Data accessed from HMRC and DWP systems will only be available to the system for the duration of the calculation (in real time) of the UK residence indicated by that data and will not be retained by the Home Office.

For the EU Exit: ID Document Check app, no personal information is retained on either the applicant's device, or the systems of the relevant commercial partner, which transfer data instantaneously to the Home Office which is then deleted upon confirmation of receipt in real time. The only exception are the images used for the liveness check, which are retained on commercial partner systems for 2 days where the check was passed or 60 days where it was failed – this is a core part of the liveness check service allowing our commercial partner to detect patterns of fraudulent use. The Home Office continues to review the time period for which these images are held by the commercial partner. The relevant commercial partner retains a range of non-identifiable, non-attributable telemetry data in order to monitor performance of the app and inform service improvements.

For commercial partners and enrolment of biometrics mentioned in paragraph 4.6 information on when data will be destroyed can be found in the privacy notice UK Visa and Citizenship Application Services (ukvcas.co.uk)

6.4 Is the data sharing process underpinned by a non-binding arrangement (Memorandum of Understanding (MoU) or equivalent) or binding agreement (Treaty or contract)?

☒ Yes ☐ No

A memorandum of understanding with both HMRC and DWP has been published. The Home Office has contractual arrangements in place with the relevant commercial partner covering data handling for the EU Exit: ID Document Check app.

6.5 Provide details of the proposed HO MoU/Contract signatory and confirm they have agreed to be responsible for the data sharing/processing arrangement detailed in this document.

Name: Gabrielle Monk
Grade: SCS PB1
Head of EUSS and SRC, Settlement, Hong Kong (BNO) and Windrush Compensation Scheme
Contact email: <Redacted>
Contact telephone: <Redacted>

6.7 Will the other party share any HO data with a third party including any 'processors' they may use?

☐ Yes ☒ No

If yes, please provide the identity of the processor and confirm details of that arrangement will be included in the formal written arrangement between the HO and the receiving/processing organisation.

Technical impact and viability

6.8 Which of the following reflects the data processing? The process may meet several of these descriptions.

Data extract: *Are you working through and assessing data to secure relevant information?*

☒ Yes ☐ No

Data matching: *Are you comparing several sets of data?*

☒ Yes ☐ No

Data reporting: *Are you processing data to produce accurate analysis?*

☐ Yes ☒ No

Data exchange/feed: *Are you sharing the data between programmes?*
☒ Yes ☐ No

Direct access: *Are you obtaining data by going directly to where it is physically located?*
☐ Yes ☒ No

Other
☐ Yes ☒ No

6.9 Has any analysis or feasibility testing been carried out? For example, through a proof of concept or pilot exercise?

☒ Yes ☐ No

If yes, provide details. If no, explain why it is not required.
HO Digital Data and Technology conduct full tests and integration of new products for the EU Settlement Scheme.

6.10 Confirm if: development work is required to ensure systems are DP compliant?

☐ Yes ☒ No

Security Checklist

6.11 Given the security classification of the data, are you satisfied with the proposed security of the data processing/transfer arrangements detailed at 2.16 and 2.17 above?

☒ Yes ☐ No

Further consultations and engagement with HO security are being planned for the lifetime of the scheme.

Section 7: International transfers

7.1 Does the activity involve transferring data to a country outside of the UK (including Crown Dependencies, Overseas Territories and Sovereign Base Areas)?

☐ Yes ☒

We will not generally be transferring data outside the EEA. There may, however, on a case by case basis be a need for information supplied in an application as documentary evidence to be verified with the organisation that generated the original document. It is possible that these organisations may be outside the EEA, e.g. a University at which the applicant is studying (which, for a period of up to 12 months, will not break the continuity of their UK residence for the purposes of an application for status under the scheme).

When we do this, we seek to take appropriate steps to safeguard information, for example by agreeing memoranda of understanding. We may rely on the derogation in Article 49(1)(d) of the GDPR where necessary.

7.2 Does the country have a positive adequacy decision?

N//A

7.3 Does the HO already have a binding or non-binding data sharing arrangement with this country?

N/A

Section 8: Referral to ODPO

8.1 Referral to the ODPO

<Redacted>

8.2 ODPO Review complete

< Redacted>

8.3 IAO sign-off

<Redacted>

Section 9: Referral to Data Board

<Redacted>

9.2 Referred to the HO Data Board Secretariat

< Redacted>

9.3 Action taken by the respective IAO(s)

< Redacted>