Data Protection Impact Assessment (DPIA)

Proposal/ Project/Activity title	**Digital Status - View and Prove**
Information Asset Owner(s)	**<REDACTED>**

Version 3

Document Control

	Name	Job Title	Date
DPIA Drafted by	REDACTED	**Status Product Manager**	11/09/2024
Reviewed by	REDACTED		
Lead DPP for business area	REDACTED		
Lead business owner /project manager/policy owner	REDACTED	**Status Capability Lead**	TBC

Version/Change history

Version	Date	Comments
Draft 2.1	04/06/2021	Transferred to new template
Final 2.1	10/06/2021	REDACTED
Draft 2.2	2024-09-11	REDACTED
Draft 2.3	2024-10-29	REDACTED
Final 2.2	2024-10-30	REDACTED

Approved by (Information Asset Owner (IAO) or person acting on behalf of the IAO):

IAO approval is only required if Stage 2 of this template is completed. Project manager sign off is sufficient if the questions outlined in Stage 1 are answered in negative.

Name	Title	Date
REDACTED	REDACTED	30/10/2024

Contents

REDACTED

Guidance on when and how to complete this template is provided in the Data Protection Impact Assessment (DPIA) Guidance on Horizon – **this guidance should be read before completing the DPIA.**

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?** *Provide a brief (up to 100 words) description of the processing activity e.g. sharing with a third party; storing data in a new way; automating a data processing activity; developing a new policy that requires new legislation or amendments to existing legislation etc.)*

[NB: this question is repeated at 3.1 at which point you can add more detail/ background.]

[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.

People with a UK immigration status must prove their immigration status to third parties in a variety of circumstances, including access to employment, housing, public healthcare, benefits, education and banking. As part of the transformation of the UK immigration system to "digital by default" individuals issued visa and other immigration status will be provided with digital proof of their status via online services, rather than the issue of a physical document.

The majority of migrants in the UK are now issued a digital immigration status or "eVisa" which they can access and share using online services, one of which is *View and Prove.*

This DPIA seeks to assess the *View and Prove* functionality.

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

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

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

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.

DPIA Stage 2

Section 1: Background and contacts

1.1 Proposal/Project/Activity title:

View and Prove online service expansion

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

Immigration status information is derived from a number of data sets relating to the casework of immigration cases within UKVI, Border Force and Immigration Enforcement which result in the creation of an immigration status. This data is held in the Person Centric Data Platform, which aggregates information held in the following caseworking and supporting systems:

Case Information Database (CID)
Central Reference System (CRS)
Atlas Caseworking System (Atlas)
Immigration & Asylum Biometric System (IABS)
Asylum Seekers Support System (ASYS)
Irish Visa Application Centre System (IVACS)
Pega

1.3 Information Asset Owner(s) (IAO):

Email:	REDACTED
Name:	REDACTED
Telephone Number:	REDACTED
Information Asset title:	Digital Status

Email:	Click or tap here to enter text.
Name:	Click or tap here to enter text.
Telephone Number:	Click or tap here to enter text.
Information Asset title:	Click or tap here to enter text.

Email:	Click or tap here to enter text.
Name:	Click or tap here to enter text.
Telephone Number:	Click or tap here to enter text.
Information Asset title:	Click or tap here to enter text.

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: DDAT

1.5 Date DPIA commenced:
27/11/2020

1.6 Date processing activity to commence (if known):

Ongoing – updates to status profiles from 31/10/2024

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

The DPIA is being updated to include changes to the scope of data processing which has increased as part of the Home Office rollout of digital immigration status or "eVisas"

1.7 Information Asset Register reference (if applicable):
Digital Status

1.8 DPIA version:
2.2

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

View and Prove is one of three online services which enable people with an immigration status to check and share their status online. The same digital immigration status or eVisa can also be shared with other Government departments and Agencies via three Application Programming Interfaces (APIs).

Right to Work	URN 329.21
Right to Rent	URN 239.20
Immigration Status API (DVLA)	URN 341.21

Immigration Status API (SLC)	URN 63.24
RtHC (NHS)	URN 82.19
RtPF (DWP)	URN 82.20
RtPF (HMRC)	URN 81.20
RtPF (Islington Council - Connect)	URN 228.22
RtPF (Social Security Scotland)	URN 49.22

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

NB: Provide below information about whether the DPIA will be published in part or in full, and the reason why it will be published.

The Home Office does not routinely publish DPIAs, as there is no legislative requirement to do so. This does not mean we would not make it available to the regulatory authority should the need arise – that being the Information Commissioners Office. We will also consider any request for publication received under FOI or on advice received by the Home Office Data Protection Officer or the ICO

Section 2: Personal Data

NB: These questions relate to the personal data being processed in the processing activity described within this DPIA only. It is acknowledged that in many instances the personal data being processed will originate from other HO sources and therefore be subject to their own set of rules governing access, retention and disposal.

2.1 What personal data is being processed?

The *View and Prove* service processes identity and immigration status data of people who have been granted a visa or other form of leave to remain in the UK.

This data is retrieved by *View and Prove* from the Home Office Person Centric Data Platform (PCDP) and the Immigration and Asylum Biometric Store (IABS).

Retrieval of the data occurs every time a *View and Prove* user signs into the online service on gov.uk through two step authentication (*View and Prove* itself does not retain or persist personal data).

The data that *View and Prove* can retrieve includes the data of applicants to the EU Settlement Scheme (EUSS) and the data of an increasing range of migrants granted leave to remain (LTR) indefinite leave to remain (ILR), leave to enter (LTE) or indefinite leave to enter (LTE) the UK. It also includes the data of people who have been granted humanitarian, asylum or other protected status.

The specific data the *View and Prove* service retrieves and presents to status holders when they sign into the service is:

- A face image of the status holder, retrieved from IABS
- The full name of the status holder
- *The date of birth of the status holder (October 2024)*
- *The nationality of the status holder (October 2024)*
- A national insurance number (NINo) for the status holder, if held by the Home Office
- The type of leave held by the status holder (ILR, LTR, LTE, ILE, or an EUSS status, which could be a Certificate of Application, Pre-Settled Status, or Settled Status) retrieved from the PCDP
- A Status title which describes the type of visa or status they hold, e.g. Skilled Worker, retrieved from the PCDP
- The start date of the leave held and the end date of leave held (for most status holders)
- If the status holder has lost their immigration status, some information may be provided on the reason for loss of status, e.g. “Cancelled"
- Codes from the PCDP which *View and Prove* translates into plain English descriptions of the conditions of the status holder’s leave in the UK, e.g. “You can work” or “You can access public funds”

To sign into *View and Prove*, the service processes additional data which must be entered online by the Status holder to access the service:

- Identity Document Number (e.g. passport number)
- Date of birth

This data is used for authenticating the status holder and does not appear on a status holder’s eVisa.

The sign in process uses “two factor authentication” whereby after a status holder enters their ID document number and date of birth as part of the sign-in process, they are sent a security code which they must enter online as the last step in the sign-in process. *View and Prove* two-factor authentication processes the following data:

- Mobile telephone number, and / or
- Email address

This data is only used for two-factor authentication and does not appear on the status holder’s eVisa

People who wish to share their digital immigration status or eVisa with a third party can use *View and Prove* to generate a "Share Code". Share Codes are nine-character alphanumeric codes which can be copied and passed on to any third party with whom the status holder wishes to share their eVisa.

These codes can be entered into the online *Check someone's Immigration Status* service (itself a part of *View and Prove*) along with the status holder's date of birth. This service will then present the third party with a view of the status holder's eVisa.

Check someone's immigration Status retrieves and presents the following data:

- A face image of the status holder, retrieved from IABS
- The full name of the status holder
- The type of leave held by the status holder (ILR, LTR, LTE, ILE, or an EUSS status, which could be a Certificate of Application, Pre-Settled Status, or Settled Status) retrieved from the PCDP
- A Status title which describes the type of visa or status they hold, e.g. Skilled Worker, retrieved from the PCDP
- The start date of the leave held and the end date of leave held (for most status holders)
- Codes from the PCDP which View and Prove translates into plain English descriptions of the conditions of the status holder's leave in the UK, e.g. "You can work" or "You can access public funds"

Check Someone's Immigration Status service asks third parties checking a status holder's eVisa to enter some details about themselves. The service also processes the following data:

- Free text entry for "Reason for Check"
- Free text entry for "Organisation doing the check"
- Free text entry for "Job Title"

2.2 Which processing regime(s) applies: general processing regime (UK GDPR/Part 2 DPA), and/or law enforcement processing regime Part 3 DPA?
NB: this question is repeated at Q.3.1.a.

General processing (UK GDPR/Part 2 DPA) ☒

Law enforcement (Part 3 DPA) ☐

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

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

☒ Yes ☐ No

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

Existing measures afforded to all applicants through this system are deemed sufficient to also protect implicated child data. Children's status is generally accrued to them via the parent's UANs. They are not the focus cohort of this process.

2.6 Will data subjects be informed of the processing?

☒ Yes ☐ No

If 'yes' go to Q2.7 *If no, explain why.*

Click or tap here to enter text.

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

The service relies on data that has previously been submitted by the individual, or a responsible adult acting on their behalf, as part of an application to the EU Settlement Scheme or for another eVisa or digitised immigration route. The data is collected in line with the Borders Immigration and Citizenship System Privacy Information Notice, and is retained within the Person Centric Data Platform (PCDP). Both the individual and checker sides of the service also have their own privacy policy notice, accessible from the service (https://view-immigration-status.service.gov.uk/privacy for individuals and https://view-immigration-status.service.gov.uk/view/privacy for checkers).

To use this particular service, the individual can access their own information, and then choose to share it with a third party.

Third parties using the service will be asked to provide information such as the name of their organisation, their job title and the purpose of the check. The service indicates that this is collected so that the Home Office can make improvements to the service and that we will retain the data in line with data retention policy to ensure a record of the check is retained. This information will ultimately be available to HO staff for audit purposes.

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

The functionality facilitates trusted third parties to access View and Prove for specific individuals.

The information underlying the individuals' profile is drawn from existing HO caseworking systems, so is already accessible by HO caseworkers.

REDACTED

2.8a. How will access be controlled?

REDACTED

2.9 Where will the data be stored?

Biographic and immigration status data is stored within the Person Centric Data Platform (PCDP) database, hosted on Amazon Web Services (AWS). The face images retrieved and displayed on *View and Prove* is stored on IABS, a proprietary Home Office system.

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

If 'No' explain why not below and go to Q2.12

Click or tap here to enter text.

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

Subject rights are managed by a specific team within the Home Office who interact with the data via a case management system, ATLAS. Requests can be actioned through information published in privacy information notices. As the service provide a snapshot of information for wider consumption, any rights requests will be actioned first on core systems and then reflected on *View and*

Prove when the status is requested. All requests will be assessed on a case by case basis.

[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?]

Click or tap here to enter text.

[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)? *e.g. criminal record (fact); allegation (non-factual)*

☐ *Yes* ☐ *No*

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

Click or tap here to enter text.

2.14 What is the retention period for the data?

Underlying data inclusive of audit insight, is retained only as long as it is required for operational purposes and in line with policy. Personal data will be typically retained for 25 years after a decision to grant settlement or naturalisation and for 15 years after the last action in other cases.

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

Deletion of underpinning data will be in line with wider management of Home office data i.e. data will be retained in line with the retention timeframe or for as long as needed for the purpose it was collected for.

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

No data is physically moved outside the Home Office. The data is presented online but is not retained by the *View and Prove* service, and persists only as long as the user is accessing the online service. After signing out, the only trace of the data will be anything retained in the user's web browser. There is no functionality to prevent copying of the data from the read only service, however accessing third parties are beholden to confidrntiality rules under data law for lawful and proportionate onward use as provided by the data subject.

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

REDACTED

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:

REDACTED

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?**

A banner is displayed on the site when they access the service giving them the option of accepting all cookies, customising or rejecting.

Section 3: Purpose of the Processing

3.1 What is the purpose of the processing? Provide a detailed description of the purpose for the processing activity. This section needs to provide an overview (in plain English) that can be read in isolation to understand the purpose and reasons for the processing activity.

Individuals with a UK immigration status are required to prove their status is a variety of circumstances to access employment, housing or public services. *View and Prove* provides a method for status holders to check and prove their immigration status online, without recourse to physical documentation.

Employers, landlords and other public and private sector organisations in the UK have a statutory duty to carry out checks of people's immigration status. These include checks for right to work, right to rent, open a bank account, or access local authority services. These checks must include some verification of the status holder's identity, hence the inclusion of a face image on the service.

View and Prove processes the data of immigration status holders to enable these checks to take place.

The purpose of collecting data on users of the *Check someone's immigration status* service (itself part of *View and Prove*) is to provide an audit trail for third parties to demonstrate compliance with their statutory responsibilities, e.g. should there be dispute about whether an organisation carried out the immigration status check they were meant to, the data collected as part of their use of the *Check someone's Immigration Status* service provides evidence they fulfilled their duty.

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) ☒ - **go to question 3.2.a**.

Law enforcement (Part 3 DPA) ☐ - **go to question 3.2.b.**

3.2.a. <u>General processing only</u>: What is the (UK GDPR Article 6) lawful basis for the processing? Choose an option from the list:

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

NB: Legitimate Interest cannot be relied upon by the Home Office for processing carried out in order to fulfil or support a public task.

[3.2.b. <u>Law enforcement processing only</u>: What is the (Part 3 DPA) lawful basis for the processing? Choose an option from the list:

Consent	☐
Necessary for a law enforcement purpose	☐]

3.3. If you have selected 'legal obligation' or 'performance of a public task' for general processing (for Q3.2.a), OR if the processing is for a law enforcement purpose

Indicate below the legal basis and relevant legislation authorising the processing of the data:

Common law (list HO function/objective below) ☐

Click or tap here to enter text.

Royal Prerogative (HMPO only) ☐

Explicit statute/power (list statute below) ☒

IANA 2006 and Immigration Act 2014, and secondary legislation made under these Acts, which legislate for an online checking service (SI 2007/3290 and 2014/2874).

Implied Statute power (list statute below) ☐

Click or tap here to enter text.

3.4.a. General processing only: If processing special category data or criminal convictions data (see Q2.2 above)

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	☐

[3.4.b. Law enforcement processing only: If processing sensitive data for a law enforcement purpose: What is the (DPA Schedule 8) condition for the processing?

Consent	☐
Substantial public interest (for a statutory purpose)	☐
Administration of justice	☐
Vital Interests (of the subject or another)	☐
Safeguarding children and individuals at risk	☐
Data already in the public domain	☐
Legal claims (seeking advice, legal proceedings, defending rights)	☐
Judicial acts	☐

Preventing fraud (working with anti-fraud organisations) ☐
Archiving ☐]

3.5 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

If 'no', what was the original purpose and lawful basis?

Original purpose: Click or tap here to enter text.

Original Lawful basis:

Consent	☐
Contract	☐
Legal obligation	☐
Vital Interest	☐
Performance of public task	☐
Legitimate Interest	☐

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

The View & Prove service will replace the use of Biometric Residence Permits which are being decommissioned at the end of 2024.

If the answer is 'yes' go to 4.3

4.2 Is the processing a new activity? This description should include details (if appropriate) of what resources are needed to build the model? (e.g. FTEs, skills, software, external resource)

☐ Yes ☐ No

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

As of the drafting date of this document, the *View and Prove* service is accessed online by status holders about 800,000 times a month and by third parties using the *Check someone's Immigration Status* service about 100,000 times a month. These figures are indicative rather than exact as they rely on the use of web analytics.

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

REDACTED

4.4 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

4.5 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?

Click or tap here to enter text.

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

☒ Yes ☐ No

If the answer is "No" go to 4.7.

If the yes answer is 'yes' and where the other party is external to the HO, please ensure section 6 is completed.

4.6.a 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 ☐

Provide details here:

Third parties accessing the data through the controlled process.

4.7 Will any personal data be transferred outside the UK?

☐ Yes ☒ No*

If 'no' go to 4.8. If 'yes', provide brief details of the countries and complete Section 7.

*Any organisations globally provided with the link can view and action data accordingly, however this occurs through gov.uk services within the UK.

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

☐ Yes ☒ No

If yes, provide details

Click or tap here to enter text.

4.9 Does the proposal involve automated decision-making?

☐ Yes ☒ No

If yes, provide details

Click or tap here to enter text.

4.10 Does the processing involve the use of new technology?

☐ Yes ☒ No

If 'no', go to question 5.1.

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

Click or tap here to enter text.

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

☒ Yes ☐ No

a) If 'yes', explain how this is being achieved

The Home Office has been issuing digital immigration status since 2018 (EU Settlement Scheme) and consultation with user groups (employers, banking etc) has taken place regularly since inception. In addition to user group consultation, user research with customers (holders of digital status who use *View and Prove*) has been conducted at regular intervals to obtain feedback on the customer experience, to guide improvement of the services. Feedback is also collected directly on the *View and Prove* service itself which includes links to feedback forms by which users can share their experience of the service, again, this feedback is used to drive continuous improvement of the services.

b) **If 'no', what is the justification for not seeking their views?**

Click or tap here to enter text.

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

If 'yes' provide details and go to question 5.2.

- Inadvertent sharing of identity details, immigration status details or face image
- Unlawful disclosure of personal information, after the individual has withdrawn consent to share their data.
- Presenting inaccurate identity details, immigration status details or face images to status holders and third parties

REDACTED

5.2 What steps have been taken to mitigate these risks?

- Protection of information in transit by default,
- Enforcing need to know using logical access controls,
- Enforcing extra privacy protection to the most sensitive information and maintaining information retention processes, (see 2.14)
- Encryption of data at rest
- Two-factor authentication to prevent unauthorized access to individuals' profiles
- Provision of Resolution Centre (support helpline) to resolve identity and immigration status inaccuracies
- Customers can also self-report status inaccuracies using the Status Error Corrections form on GOV.UK. Reports are handled by BIDMU.

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.

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

The risk to the individual of being presented with inaccurate information, and of inaccurate information being shared with a third party, on *View and Prove* is minimised by:

- The availability of online self-service to report and correct inaccurate details held by the Home Office, e.g. a misspelled name
- The availability of the Resolution Centre (support helpline) to report and resolve inaccuracies
- A feature for status holders to preview their eVisa before creating a Share Code so they can check their details are correct before passing the Share Code to a third party

The risk of unauthorised access and inadvertent sharing is minimised by:

- The use of secure two factor authentication to sign into View and Prove
- The use of time limited share codes for third parties to access Check someone's Immigration Status
- The availability of the Resolution Centre (support helpline) to "lock" access to *View and Prove* on request from verified status holders

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.4.6.

6.1 External contact details for data exchange/ processing

View and Prove enables migrants to look at their own immigration status online. If the migrant wishes to share their immigration status, they generate a share code and pass it onto a third party. The third party can then use the Share Code to access a limited view of the migrant's immigration status online. The third party could be any individual or organisation in the UK (or any other country). **There is no single third party or group of third parties who process the data shared in this way.**

6.2 What is the legal basis/power/statutory gateway for the processing activity?

Common law (list HO function/objective below) ☐

Click or tap here to enter text.

Royal Prerogative (HMPO only) ☐

Explicit Statute/power (list statute below) ☒

IANA 2006 and Immigration Act 2014, and secondary legislation made under these Acts, which legislate for an online checking service (SI 2007/3290 and 2014/2874).

Implied Statute/power (list statute below)

IANA 2006 and Immigration Act 2014, and secondary legislation made under these Acts, which legislate for an online checking service (SI 2007/3290 and 2014/2874).

☐

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

***See 2.14**

6.4 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**

6.5 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

If no, provide details why a formal written arrangement is not required and move to 6.7

Data sharing via *View and Prove* is only done by status holders themselves via the choice to generate a Share Code.

6.6 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: Click or tap here to enter text.
Grade: Click or tap here to enter text.
Business Unit/Area: Click or tap here to enter text.
Contact email: Click or tap here to enter text.
Contact telephone: Click or tap here to enter text.

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.
Click or tap here to enter text.

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

a) If 'Other, please provide details
Click or tap here to enter text.

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.
A private beta phase was conducted.

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

☐ Yes ☒ No

If yes, provide details including time frame

Click or tap here to enter text.

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

6.12 Confirm you have read the associated guidance and, if necessary, consulted with HO Security and the relevant DDaT teams, including Home Office Cyber Security (HOCS):

NB: If your processing activity involves any use of IT systems or physical documentation being sent outside of the Home Office to a non-governmental organisation, you must consult with HOCS, prior to your DPIA being submitted.

Yes, I have read the guidance and/or consulted with HO Security

6.13 If the answer is 'no': What needs to happen to ensure that adequate security arrangements are achieved?

Click or tap here to enter text.

6.14 Will the data be stored and be accessible off-site?

☒ Yes ☐ No

6.15 If 'yes', have you considered the security arrangements that need to be in place to prevent the data from being accidentally or deliberately compromised? Please provide details.

☒ Yes ☐ No

For the status holder's security, two factor authentication is used to sign into *View and Prove.* Anyone wishing to access the service must have the status holder's identity document number, date of birth, and their mobile telephone or email account. The Share Codes used to provide third parties with a view of the status holder's eVisa have a limited shelf life and after 90 days become invalid, preventing the holder of a Share Code from possessing unlimited access to the status holder's eVisa.

Section 7: International transfers

Only complete this section if you have answered yes to question 4.7.

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 ☐ No

If 'yes', specify the country. If 'no', go to Section 8.

Click or tap here to enter text.

7.2 Does the country have a positive adequacy decision?

☐ Yes ☐ No

a) If 'no', **under what legal basis do you propose to transfer the data?**

i) General processing only:

- Pursuant to a legally binding Treaty which contains appropriate safeguards for the rights of data subjects and includes effective legal remedies for those rights ☐
- Pursuant to an administrative (non-binding) arrangement approved by the UK Information Commissioner which recognises the rights of data subjects and includes binding rules providing effective legal remedies for those rights ☐
- On the basis that the transfer is necessary for 'important reasons of public interest' which are recognised in statute or common law (and set out in a non-binding MoU) ☐

ii) Law enforcement processing only:

- Pursuant to a legally binding Treaty which contains appropriate safeguards for the rights of data subjects and effective legal remedies for those rights ☐
- On the basis that the transfer is necessary for 'in individual cases for any of the law enforcement purposes' which are recognised in statute ☐

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

☐ Yes ☐ No

If no, skip 7.4 a)

a) If 'yes', does the arrangement cover the purpose(s) for which you need to share data?

☐ Yes ☐ No

If you have selected no for 7.3, you will need to consider reviewing the existing agreement to include the new processing activity

I. If 'yes', **does the arrangement recognise the rights of data subjects?** Does it include effective legal remedies for data subjects' rights; or set out important reasons of public interest and how those reasons are legally founded; or set out why the transfer is necessary in individual cases for a law enforcement purpose?

☐ Yes ☐ No

If yes go to Section 8

II. **If 'no', how do you propose to document the terms of the understanding with the other country?**

Click or tap here to enter text.

Note: You should consult guidance on Overseas Security and Justice Assistance (OSJA) to determine whether an assessment of human rights, International Humanitarian Law, political and reputational risks is required.

Section 8: Referral to ODPO

8.1 Referral to the ODPO

8.1) Date referred to the DPO

05/07/2019

8.2) Comments/recommendations:

Please address comments and resubmit

8.3) Date returned to the author:

11/07/2019

8.4) Date referred to the ODPO:

30/11/2020

8.5) Comments/recommendations:

Review complete, no further comments

8.6) Date returned to the author:

01/12/2020

8.7) Date referred to the ODPO:

28/10/2024

8.8) Comments/ recommendations:

ODPO review process complete. Recommendation that the guidance for senders and recievers is robust, covering when and how it is appropriate to use this data and data protection standards.

8.9) Date returned to author:

28/10/2024

8.2 ODPO Review complete

8.10) Date sent to IAO for sign off:

30/10/2024

8.11) Name of IAO or person signing on behalf of:

REDACTED

8.12) Date returned to the author:

30/10/2024

8.13) Comments (including approved to proceed Y/N):

Yes

.