Data Protection Impact Assessment (DPIA)

Proposal/ Project/Activity title	**Digital Status - Right to Work**
Information Asset Owner(s)	**REDACTED**

Version 9.3

Document Control

	Name	Job Title	Date
DPIA Drafted by	**REDACTED**	**Head of SVEC**	**21/03/2022**
Reviewed by	**REDACTED**		**29/04/2025**
Lead DPP for business area	**REDACTED**		
Lead business owner /project manager/policy owner	**REDACTED**	**Status Capability Lead**	**02.03.22**

Version/Change history

Version	Date	Comments
Draft 9.1	03/06/2021	Existing DPIA transferred to new templated
FINAL 9.1	10/06/2021	Approved by IAO
9.2	03/03/2022	Draft to reflect removal of BRP/BRCs from the approved document list.
Draft 9.3	29/04/2025	Reviewed and updated IAO

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**	29/04/2025

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.]

All employers have a responsibility to carry out right to work checks. This is done by employers conducting simple checks before they employ someone, to make sure the individual is entitled to take the work in question. The Home Office has developed

[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.

the online right to work checking service to support employers in conducting secure right to work checks and make it easier for individuals to demonstrate their right to work. The service allows employers to check that current/prospective employees have the right to work in the UK, and any associated restrictions/conditions in respect of that right to work.

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

    The service allows employers to check that current/prospective employees have the right to work in the UK, and any associated restrictions/conditions in respect of that right to work.

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:
Online Right to Work service

1.2 Information Asset title(s) (if applicable):
Right to work 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:	Immigration status information
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:	Status Verification, Enquiries and Checking

1.5 Date DPIA commenced:
21/03/2022

1.6 Date processing activity to commence (if known):
28/01/2019
A change in policy has resulted in the need for a DPIA review due to Biometric Residence Permits and Biometric Residence Cards no longer allowing an employer to generate a statutory excuse. From 6th April 2022 employers and employees will need to use the online right to work service.

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

1.8 DPIA version:
V9.2

1.9 Linked DPIAs *NB*: attach word versions, do not provide links.
DPIAs relating to other services developed as part of the Status Checking project. Currently includes
- Online Right to Rent Service
- View and Prove Online Status Service
- Digital Status Checker - right to free healthcare
- Digital Status Checker – DWP right to public funds
- Digital Status Checker – HMRC right to public funds
- Digital Status Checker – Right to enter API

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

There is an intention to publish this DPIA proactively as we believe there is a public interest in doing so. However, a decision has not been made on what we will publish, in what format or when. Therefore, there is no set publication date and we reserve the right to just publish a summary of the key parts of this DPIA to aid transparency. It is envisage the DPIA will be published in the second half of 2022.

Section 2: Personal Data

2.1 What personal data is being processed?

Forename

Surname

Middle name(s) (if known)

Aliases (if known)

Last known address (including postcode)

Photograph

Right to work entitlement

Start and end date of entitlement

Document number (BRC/BRP/C/Nationality ID card/Passport)

The scope of the service currently extends to those who have been granted immigration status and given a Biometric Residence Permit or Card, those granted status under the EU Settlement Scheme, those granted status under the UK's points-based immigration system whose evidence of status is provided digitally and those holding a British National Overseas (BNO) visa or Frontier workers permit whose evidence of status is provided digitally.

The service will also increasingly support those with a pending application/appeal who have continuing rights in the UK. Employers will no longer be able to rely on a Biometric Residence Permit and Biometric Residence Card to generate a statutory excuse against payment of a civil penalty. Prospective employees will need to share their right to work digitally to prove their right to work in the UK. Biometric Residence Cards and Biometric Residence Permits are still being issued to customers and must be used to access and share their right to work digitally, however the physical document cannot be used by an employer in the UK to generate a statutory excuse.

Such an individual's immigration case history is interrogated to establish their current immigration status and right to work entitlement, along with any conditions or restrictions attached to this. This data is used to provide a headline right to work status that is shown on the individual's profile.

The immigration case history is used to determine the individuals current immigration status and right to work entitlement, along with any conditions or restrictions

attached to this. This data is used to provide a headline ‘right to work status’ that is shown on the individual’s profile.

There are two ways to access the online service, dependent on your circumstances.

UKVI Account Holders:

For people who applied for EUSS or on the Points Based System, they will have created a UKVI account which they will use to the access Right To Work service.

They will enter their ID documentation no and their date of birth. They will then enter their email or phone number to receive the two factor authentication code.

BRP/C Holders:

For individuals who hold either a BRC or BRP, they will log in using their BRP/C number and their date of birth. BRC/P holders will not be asked for authentication details via SMS or email and will go directly to their profile. In the case of a BRP/C holder, if the card has been cancelled as reported as lost or stolen, it cannot be used to access the service.

This authentication is used to determine the identity of the individual, establishing their case history and entitlements.

The name and a facial image of the person is displayed following successful authentication, along with their confirmation that they have a right to work. They can choose to share this with a landlord or letting agent by generating a ‘share code’.

Employers:

When the employer accesses the service, they are required to input information for the purposes of audit records. For employers this will be their name and the company name. The employer can then see the same information as was presented to the individual.

Home Office staff:

Where individuals require help to use online services, due to digital exclusion, the HO Resolution Centre (RC) will be able to assist them with sharing their status. This includes RC agents being able to access the service at the individual’s request, using their log in details and generate a share code on their behalf, to be provided to the employer. To be able to do this, the RC agent will input their details into the agent view of the service to support customers. The RC agent would input their username and their POISE user ID, name and surname for audit purposes.

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.

Click or tap here to enter text.

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 as part of an application for immigration leave. The data is collected in line with the standard Border Immigration and Citizenship System Privacy Information Notice

and is retained within the Person Centric Data Platform (PCDP). Both the applicant and employer 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 employers).
To use this particular service, the individual can access their own information, and then choose to share it with a third party (employer).
Employers using the service will be asked to provide information such as the name of their organisation, which may be their own name if this is their company name.
The service privacy policy sets out that this information is collected so that the Home Office has a record that the employer has made the check, along with other information on how this data will be used and stored. This information will then be available to HO staff for audit purposes.
Individuals may also refer at anytime to the range of Privacy Information pertaining to Home Office immigration practices on the gov.uk website, including the Borders, Immigration and Citizenship Notice and Personal Information Charter.

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

The information underlying the individuals' right to work status 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?

The data from which the right to work status is derived, and the audit record of checks conducted by employers using the service is stored within the Person Centric Data Platform (PCDP) database, which is hosted on Amazon Web Services.

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. Individuals know how to act on their rights via public facing privacy information, rights 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 is retained only as long as it is required, in line with wider HO published data retention policy. Audit information will similarly be retained in line with requirements.

Employers are required to retain evidence that they have conducted appropriate checks for the duration of the individual's employment, plus two years after and therefore retention of this data is to support Home Office compliance requirements.

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 HO data. This will be performed following review of data relevance in light of moratoria.

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

To enable the employer to access this information, the individual can choose to generate a unique share code. The employer then needs to enter the share code and the individual's date of birth.

The service temporarily stores data to support the sharing activity between the individual and the employer. This is contained within a secure service to support the

journey whereby an employer accesses an individual's information. This process creates a temporary account that is valid for 90 days, after which time it is deleted.

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 or rejecting (non-essential) cookies. The preference is retained for one month when given, in addition, there is a dedicated page that individuals can access to view which cookies might be used, what they are for and how long they will be valid for before expiring

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.

All employers in the UK have a responsibility to prevent illegal working, in supporting the aim of effective immigration control. This is done by employers conducting simple right to work checks before they employ someone, to make sure the individual is not disqualified from carrying out the work in question by reason of their immigration status.

The law on preventing illegal working is set out in sections 15 to 25 of the Immigration, Asylum and Nationality Act 2006 (the 2006 Act), section 24B of the Immigration Act 1971, and Schedule 6 of the Immigration Act 2016.

Under section 15 of the 2006 Act, an employer may be liable for a civil penalty if they employ someone who does not have the right to undertake the work in question if that person commenced employment on or after 29 February 2008.

The Home Office has developed the online right to work checking service to support employers in conducting right to work checks and to make it easier for individuals to demonstrate their right to work.

The service allows employers to check that current or prospective employees have the right to work in the UK, and any associated restrictions or conditions in respect of that right to work. The service design puts the individual job applicant in control of their data, choosing who and when they allow access. The service is part of the broader Status Checking project, which is delivering common components to calculate status values (such as right to work) and developing mechanisms through which this information can be queried and presented – such as publicly available user interfaces or system to system APIs.
This service is both automating the calculation of the right to work status information and enabling this to be shared with a 3rd party (through the choice of the individual to whom the data relates).

REDACTED

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. General processing only: 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. Law enforcement processing only: 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, 2021/689 and2022/242).

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	☐

Appropriate Policy Document: Special Category Data Part 2

[3.4.b. <u>Law enforcement processing only</u>: 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 online service also enables individuals to share only the required personal data to fulfil this check thereby improving security of their personal data and promoting the principle of data minimisation. The online service has replaced a pre-existing HO 'check a BRP' service, although this continues to provide an exception route for eligible individuals' who are unable to use the online service for technical reasons. The online service represents a significant reduction in response time compared to the manual service.

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?

REDACTED

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

Frequent

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 4.7.

☐ 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?

Click or tap here to enter text.

4.7 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.

4.8 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.

Click or tap here to enter text.

4.9 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.

4.10 Does the proposal involve automated decision-making?

☐ Yes ☒ No

If yes, provide details

Click or tap here to enter text.

4.11 Does the processing involve the use of new technology?

☐ Yes ☒ No

If 'no', go to question 5.1.

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

Click or tap here to enter text.

4.13 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

Click or tap here to enter text.

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 individual's details.
- Unlawful disclosure of personal information, after the individual has withdrawn consent to share their data.
- Producing inaccurate results for employers

REDACTED

5.2 What steps have been taken to mitigate these risks?

REDACTED

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.

Steps have been taken to minimise these risks, which we believe are outweighed by the benefit of delivering the right to work policy and enabling individuals to exercise their rights digitally and employers to check right to work more easily, securely and safely, particularly during the COVID-19 pandemic .

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

The service is accessed by a range of user controlled and auditable persons to facilitate the right to rent verification process.

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 2014/2874, 2021/689 and 2022/242).

Implied Statute power (list statute below) ☐

Click or tap here to enter text.

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

System is accessed as part of digital status verification by a range of relevant persons, use terms are controlled by security measures and user accounts.

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.

N/A

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.

The data can be used to facilitate the right to work which may involve onward sharing by those accessing the system to facilitate this.

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.
Internal testing, followed by private beta trial phase were carried out in advance of launching the service

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

☒ Yes ☐ No

If yes, provide details including time frame

Development work to deliver the online service has been carried out in advance of the testing phases.

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

See details at 2.17 above

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

NB: Any subsequent changes made to the DPIA by the business must be done clearly and transparently and in accordance with accepted version control convention. In the event of changes being made, earlier versions of this DPIA must be retained for auditing purposes and in-line with your agreed retention period.

If substantive changes are made to this DPIA, you must re-refer to the ODPO for a new review.

Date referred to the ODPO	Reviewed by	Date returned to the Author	Comments/recommendations
11/03/2022	REDACTED	18/03/2022	REDACTED
30/04/2025	REDACTED	30/04/2025	REDACTED
22/05/2025	REDACTED	23/05/2025	REDACTED

8.3 IAO sign-off

Date referred to IAO	Name of IAO or person signing on behalf of	Date returned to the Author	Comment (including approved to proceed Y/N)

Section 9: Referral to Data Board

This section is only required if one or more of the criteria for referral to the HO Data Board is met (see DPIA guidance). Referral to the HO Data Board will be completed by the ODPO after consultation with the business owner(s) listed in part 1 of this DPIA. **Guidance** is available on Horizon.

9.1 Criteria for referral to the HO Data Board:

Criteria	Met
REDACTED	
REDACTED	
REDACTED	
REDACTED	
REDACTED	
REDACTED	

REDACTED	
REDACTED	
REDACTED	
REDACTED	
Specific referral circumstances:	
REDACTED	
REDACTED	
REDACTED	
REDACTED	
Other: [add detail]	

9.2 REDACTED

REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED			

9.3 REDACTED

Effective Date	REDACTED
Last Review Date	REDACTED
Next Review Date	
Owner	REDACTED
Approved by	REDACTED
Audience	REDACTED