Data Protection Impact Assessment (DPIA) Template

Proposal/ Project/Activity title	**Facial Recognition**
Information Asset Owner(s)	**Gordon Summers**

URN:105.25

Document Control

	Name	Job Title	Date
DPIA Drafted by	Richard Granger	**Project manager**	**26/06/2025**
Reviewed by	Phillip Warham	**Programme Manager**	**26/06/2025**
Lead DPP for business area	Jackie Rowson	**IE Data Protection Lead**	**1 & 19 May 2025**
Lead business owner /project manager/policy owner	Andy Clark	**IE Business Rules Programme Manager**	

Version/Change history

Version	Date	Comments
Draft 0.1	01/05/2025	First draft
Draft 0.2	19/05/2025	Changes after review by DPO contacts
Draft 0.3	10/06/2025	Changes after review by HOLA
Draft 0.4	26/06/2025	ODPO Review
Final 1.0	01/09/2025	Sign off by SRO
Final 1.1	09/09/2025	Minor changes
Final 1.2	15/09/2025	Minor Changes
Final 2.0	24/09/2025	Sign off by SRO
Final 3.1	21/11/2025	Minor Changes

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
Gordon Summers	Deputy Director of ICE North & IAO	01 September 2025

Contents

Guidance on when and how to complete this template is provided in the Data Protection Impact Assessment (DPIA) Guidance on SharePoint – **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. **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.]

   Immigration Enforcement (IE) intend to pilot the use of live facial recognition (LFR) as a precision tactic to locate people who are sought by IE for law enforcement purposes. An initial pilot is being planned in Holyhead for November 2025, focussing on individuals who have previously been deported from the UK. The pilot will look to match facial images from the deportation list with those entering through Holyhead using LFR. The processing should allow the identification of people who are returning in breach of a Deportation Order

3. **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

[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.

- 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. If you have answered 'No' to this question but you are proceeding with completion of the DPIA please provide a brief reason below.

Click or tap here to enter text.

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?** NB: Consult link for profiling and automaton definition in law and scope.

   ☐ 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. ATLAS.

☐ 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 one or more 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).

Have you considered an Equality Impact Assessment (EIA)? There is a current template and guidance document available to support the composition of EIAs. The public sector equality duty (PSED) requires public bodies to have 'due regard' to the need to eliminate discrimination, advance equality of opportunity, and foster good relations when developing policies and delivering services. The Home Office requires that an EIA is completed for all policies, guidance and operational activity, apart from that covering internal restructuring. Once complete an EIA must be signed off by an appropriate Senior Civil Servant, the assessment stored locally and a copy sent to the Public Sector Equality Duty Team .
The PSED Team can also provide advice when considering the duty.

☒ Yes ☐ No

If you have completed Stage 1 and do not need to complete Stage 2, send a SharePoint link of your Stage 1 assessment to the ODPO and the Data Catalogue

Appropriate links are required to be created for '*people in home office with link*'. Please see How to share DPIA links for guidance on how to do this.

DPIA Stage 2

Section 1: Background and contacts

1.1 Proposal/Project/Activity title:

Immigration Enforcement – Live Facial Recognition

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

Immigration and Asylum Biometric System (IABS) - Image data for persons subject to a Deportation Order

1.3 Information Asset Owner(s) (IAO):

Email:	Click or tap here to enter text.
Name:	Gordon Summers
Telephone Number:	Click or tap here to enter text.
Information Asset title:	ICE North
Email:	Click or tap here to enter text.
Name:	Frances Buzzeo
Telephone Number:	Click or tap here to enter text.
Information Asset title:	IABS

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

Email:	Click or tap here to enter text.
Name:	Richard Granger
Telephone Number:	Click or tap here to enter text.
Business Unit/Team:	Emerging Technology, Data and Innnovation
Directorate:	Immigration Enforcement

1.5 Date DPIA commenced:

15/04/2025

1.6 Date processing activity to commence (if known):

Click or tap to enter a date.

NB: If the processing activity is already ongoing, please explain why the DPIA is being completed retrospectively. A failure to produce an assessment for high risk processing before processing commences is a breach of Article 35 of the UKGDPR and will require an incident report.

Click or tap here to enter text.

1.7 Information Asset Register reference (if applicable):

Click or tap here to enter text.

1.8 DPIA version:

Version 3.1

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

1. ATLAS
2. Data Services and Analytics (DSA)
3. Border Force
4. Immigration and Asylum Biometric System (IABS)

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

01/11/2025

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 intention is to proactively publish this DPIA as the processing of data is controversial and it is anticipated there will be public interest in its publication.

IE will publish a redacted copy of the Facial Recognition DPIA to aid transparency. IE will also consider any request for the DPIA under a Freedom of Information Act (FoIA) request, if it is deemed appropriate to do so, or on advice received by the Office of the Data Protection Officer (ODPO) and/ or the ICO.

IE have also completed further documentation in support of the Facial Recognition Proof of Concept; this includes the Surveillance Camera Commissioner Risk Assessment. Redacted versions of all documents will be published on a dedicated webpage for LFR deployments.

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 LFR will capture video footage of a public space within the port; and scan such footage for facial images. Those facial images will then be run against a watchlist of persons subject to a Deportation Order. If a match is found, it will be alerted to a human decision maker who will then decide as to whether the match is well-founded.

When reviewing alerts the LFR operator will have access to the following information for individuals on the watchlist. The operator will use this information to make an informed decision to refer the match to IE Officers to intercept the individual.

- Full Name
- Date of Birth
- Nationality
- Immigration references
- Personal Identity reference (UID2)
- Immigration Fingerprint Bureau (IFB) reference
- Deportation Order Issue Date
- Image

When encountering an individual who is subject to a match from the LFR system, IE officers will have access to all HO platforms to view further information for individuals on the watchlist. All information on this list below is held within secured Home Office Databases that are subject to their own DPIAs and is available to IE officers only under existing operational procedure.

- Name
- Date of Birth
- Gender
- Nationality
- Travel Document
- Immigration references – Home Office (HO) Reference, Personal Identity reference
- Contact Details – Phone Number, Email Address, Addresses
- Travel Details
- Immigration Case types and outcomes
- Detention details
- Return details
- ATLAS Special Conditions – including markers of potential vulnerability or health markers
- Reporting Details
- Barriers to removal
- Criminality including offences and Multi-Agency Public Protection Arrangements (MAPPA)Associations
- Electronic Monitoring Data

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.

Whilst the LFR system will process facial images for those under the age of 13 who enter the Zone of Recognition. Individuals under the age of 18 will not be included in the watchlist and therefore they should not lead to a match.

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?

Processing of data will be conducted in line with the existing Borders, Immigration and Citizenship: privacy information notice.

In addition, further notification will be given to passengers that is specific to LFR deployments, IE will ensure that: -

a) LFR Deployments are, where possible without undermining the objectives for the Deployment, prior notified to the public using the IE website – such notifications will give a purpose for the Deployment (for example, to primarily Identify those returning to the United Kingdom in breach of Deportation Orders); and
b) LFR awareness raising measures will; include:
    a. Signage within the port to the use of LFR in the area, signage will be placed ahead of entrance to the Zone of Recognition and will be an appropriate size and clarity.
    b. Deployment notifications will be published on the Gov.uk website in line with IE's LFR policy document, where this will not have a detrimental effect on the deployment objectives.
    c. The LFR vehicle will have Police branding and remain visible and open to passengers to allow for engagement with individuals.
    d. Leaflets and supporting literature will be provided to further transparency with passengers
c) literature is prepared for persons who may be Engaged (to include information outlined within the privacy notice).

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

Access to watchlist data will be shared via an encrypted USB device. This will be uploaded to the LFR system managed by a SPOC at South Wales Police (SWP) and Greater Manchester Police (GMP).

Operational IE, SWP, GMP and Border Force Officers will have access to the data via the pre-defined Watchlist generated prior to the deployment.

The LFR system will be managed by Police Officers during deployment, IE will provide Authorising Officers (AO) to ensure correct deployment and usage of the system. AOs will be correctly trained to support operators and IE personnel to respond to alerts.

Please note – All HO staff, contractors, Border Force and SWP personnel will be security cleared to the appropriate level, typically SC.

2.8a. How will access be controlled?

To share the required data. IE personnel will integrate multiple platforms to identify individuals for the purpose of composing the watchlist.

The LFR watchlist is generated from Home Office systems it will be curated into a csv file which will be held on Home Office systems. The watchlist will be moved from a HO laptop in a secure building to an approved storage device to enable transfer of the watchlist to the LFR system laptop. If an alert is generated the image will be held within the LFR laptop LFR system for up to 24 hours. The system and storage device will be wiped after 24 hours and all data deleted.

For this deployment Police CCTV cameras will be used to operate the LFR system. The CCTV cameras are only for the operation of LFR technology and not for CCTV capturing purposes. If any footage is generated during the deployment in error, this will be deleted by GMP as soon as is practicable and in any case within 24 hours.

For the purpose of this deployment no CCTV footage will be retained following the deployment by Immigration Enforcement.

For IABS – Image data will be downloaded into secure folders with restricted access via SharePoint. Access will be limited to named users with varying, controlled access levels depending on business need. Image data will be collated from IABS according to existing guidance and will be subject to any security constraints as stated within said documentation.

Once shared with police colleagues the data will be stored in line with their data protection policies. Existing MoUs between IE and NPCC will be used to facilitate the transfer of data between both bodies.

Platforms containing business data are strictly controlled as set out below:

1. SC Clearance is required
2. Regular audit of access and privileges by Business Rules team
3. Migration & Borders Technology Platform (MBTP) wide governance and monitoring processes apply
4. Cyber Security Operations Centre (CSOC) monitoring and alerting framework under development. This team primarily manages network security incidents on a 24/7/365 basis. This will apply to all MBTP platforms.

2.9 Where will the data be stored?

During a live facial recognition (LFR) pilot, the technology processes watchlist data in real time. The system stores an offline version of the watchlist data for the duration of the deployment, to operate as intended.

The system will capture and store data pertaining to matches against the watchlist. For up to 24 hours, after which it is deleted automatically.

In the event of a False positive anonymised match data will be retained by IE to assist with further investigation. This data will be acquired from GMP LFR systems and shared via an encrypted USB device owned by Immigration Enforcement.

During the deployment and in the event of a false match the LFR team will follow the agreed False Alert Procedure.

At the conclusion for the deployment any positive images will be shared with IE via the same encrypted USB device. In any case any positive matches, false positive matches, possible matches, false alerts and confirmed false alerts will be deleted within 24 hours.

Following deployments the LFR system is wiped of all watchlist data and reports, to allow a fresh watchlist to be uploaded for subsequent deployments.

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.

All data held is derived from Home Office systems such as the Person Centric Data Platform (PCDP), ATLAS, Immigration and Biometrics System (IABS), Central Reference System (CRS), Initial Status Assessment (ISA), and reflects data held in those live systems, being updated via a regular data-feed.

These systems have the means to meet these data subject rights where appropriate, by being fully searchable and having capabilities to update inaccurate information, and all requests will be assessed on a case-by-case basis.

Once shared with named police forces, the data will be stored in line with their data protection policies and deleted at the end of each deployment.

For this deployment Police CCTV cameras will be used to operate the LFR system. It is GMP policy to record CCTV footage, for the purpose of this deployment no footage will be retained following the deployment by Immigration Enforcement.

The LFR watchlist is generated from Home Office systems it will be curated in to a csv file which will be held on Home Office systems. The watchlist will be moved from a HO laptop in a secure building to an approved storage device to enable transfer of the watchlist to the LFR system laptop. If an alert is generated the

image will be held within the LFR laptop LFR system for up to 24 hours. The system and storage device will be wiped after 24 hours and all data deleted. We do not anticipate exceeding any storage capacity limitations with this data.

During a live facial recognition (LFR) pilot, the technology processes watchlist data in real time. The system does this by:

1. The watchlist data is securely loaded into the LFR system before deployment and remains encrypted throughout the operation.
2. The **Neoface M40 algorithm** creates a numerical biometric template for all images included within the database.
3. During deployment the LFR system captures facial images from live video stream of the Zone of Recognition. Using the **NEC HD5 Face Detector algorithm** to identify and capture facial images from the footage.
4. These images are converted into numerical biometric templates, again by the **Neoface M40 algorithm**, and immediately compared against a pre-defined watchlist.
    a. When the facial features from two images are compared, the LFR system generates a similarity score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity.
    b. A threshold value is set to determine when the LFR software will generate an alert to indicate that a possible match has occurred.
5. Matches are flagged instantly for operator review; the operator will conduct a review of both the captured and watchlist image to confirm that the match is correct. Ensuring that alerts are verified by trained personnel before any action is taken.
6. For the proof of concept, the police will operate the LFR equipment. When an alert is generated, the police officer will review the image and if matched, will refer to an Immigration officer who will review. If they agree they will then transmit the description of the person to an Immigration officer who will then approach the passenger and establish identity, nationality and lawful status. The approaching officer will then decide what action if any is then required.
7. No biometric data from non-matches is retained and is deleted immediately by the LFR system. Confirmed matches are retained by the LFR system for the purpose of reporting and quality assurance processes.
8. All processing occurs within strict legal and policy frameworks, and in accordance with this DPIA, to maintain compliance and protect privacy.

2.12 <u>For law enforcement processing only</u>: 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 <u>For law enforcement processing only</u>: 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?

The LFR technology captures images of all passengers entering the Zone of Recognition. It compares these images to a watchlist and triggers match alerts;

a) Where the LFR system does not generate an Alert that a person's biometric data is immediately automatically deleted; and

b) the data held on any encrypted storage device used to import the Watchlist is deleted as soon as practicable, and in any case within 24 hours, following the conclusion of the deployment.

c) Where the LFR system generates an Alert, all personal data is deleted as soon as practicable and in any case within 24 hours.

In the event of a False positive anonymised match data will be retained by IE to assist with further investigation. This data will be acquired from GMP LFR systems and shared via an encrypted USB device owned by Immigration Enforcement. During the deployment and in the event of a false match the LFR team will follow the agreed False Alert Procedure.

At the conclusion for the deployment any positive images will be shared with IE via the same encrypted USB device. In any case any positive matches, false positive matches, possible matches, false alerts and confirmed false alerts will be deleted within 24 hours.

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

Watchlist data will be retained within the LFR system for the duration of the deployment. All watchlist data held within the system will be deleted as soon as practicable following the end of each shift. Data relating to enforcement action will be retained for the use of IE and other enforcement agencies, in line with existing processes. Where a false alert is generated, IE will retain anonymised demographic data in order to investigate any potential bias.

The LFR system will process images captured for all individuals entering the Zone of Recognition including members of the public who are not included in the watchlist for deployment. In this event all images that result in a no match are deleted instantly and no data is retained.

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

In order to compile image data, the watchlist will be shared with colleagues within Home Office Biometrics and processed as per the below:

1. Watchlist data will be transferred to a secured SharePoint site. Accessible only by those who are required to access both the input and output data files.
2. HOB colleagues will extract the file using a Poise device and download to an encrypted USB storage device to transfer to the BAT system to process the extract.
3. The BAT System will process the extract and isolate images from the initial data received from IABs. This completed extract will be returned to the SharePoint via the USB drive as stated above.

Watchlist data will be shared via a secured encrypted USB device and manually uploaded to the LFR system. The Data Transfer process is as follows:

1. The pre-defined watchlist will be created within secure Home Office enterprise systems, by trained and cleared officers.
2. The list will be downloaded to an encrypted external encrypted USB device for transfer to the LFR vehicle and system. This will be conducted within a Home Office building using the same security protections
3. The encrypted USB device will be stored within a secured box, accessible only by agreed members of staff.
4. The data will be transferred a short distance to the LFR vehicle parked outside the deployment site's office.
5. Once transferred and uploaded, the encrypted USB device will be returned to a secured lockbox container and stored securely within the Home Office Building
6. An auditable record of data movement will be included in the data management plan. This record will capture:
    a. Personnel handling the data
    b. Dates and times of transfers
    c. Deletion records
    d. Secure storage records

Following each deployment, all data will be deleted from the LFR system. New data will be uploaded to the LFR system before the next deployment further protecting the data from any loss during the proof of Concept.

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

Specified SPOC identified as recipient of the data.

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:

The LFR system will process images captured for all individuals entering the Zone of Recognition including members of the public who are not who are not included in the watchlist for deployment. All images that result in a no match are deleted instantly and no data is retained.

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

OFFICIAL	☒
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?**

Click or tap here to enter text.

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.

Immigration Enforcement (IE) intend to pilot the use of Live Facial Recognition (LFR) as a precision tactic to locate people who are sought by IE for law enforcement purposes. An initial proof of concept is being planned in Holyhead for

Autumn 2025, focussing on individuals returning in breach of a deportation order. This constitutes a criminal offence.

The proof of concept is to take place over 3 days targeting arrivals throughout the length of the deployment. Ferry arrivals into Holyhead amount to 20 arrivals per day spaced throughout a 20-hour period. The LFR technology will only be active during disembarkation.

Recent intelligence indicates that Holyhead port is frequently used as an entry point by individuals with deportation orders. The purpose of the overt operation is to intercept those people who may be Returning in Breach of a deportation order in a legally compliant and ethical manner to enable the IE to achieve legitimate enforcement aims.

Deportation Orders (DO) principally involve Foreign National Offenders (FNO) who have often committed serious crimes. A DO requires a person to leave the UK and prohibits them from lawfully entering the UK while it remains in force. Entering in breach of a DO is a criminal offence under section 24(A1) of the Immigration Act 1971 that is currently punishable by up to five years imprisonment or a fine (or both).

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) ☐

Click or tap here to enter text.

Implied Statute power (list statute below) ☒

Implied power from the Immigration Act 1971 ("1971 Act"). Section 24(1A) of the 1971 Act provides that it is a criminal offence for a person to enter the UK in breach of the deportation order. An implied power exists to identify such persons, which the use of LFR falls within.

In the alternative, there is a common law power to use LFR to identify such persons.

The composition of the watchlist and use of images to support the LFR is based on an explicit power in regulation 4 of the Immigration (Collection, Use and Retention of
Biometric Information and Related Amendments) Regulations 2021.

3.4.a. **<u>General processing only</u>**: 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 ☐
Explicit Consent ☐
Employment, social security and social protection ☐
Vital Interests ☐
Not-for-profit bodies ☐
Made public by the data subject ☐
Legal claims or judicial acts ☐

Reasons of Substantial Public Interest	☐
Health or Social care	☐
Public health	☐
Archiving, research and statistics	☐

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

LFR technology will enhance the capabilities of border security personnel, within existing practices, to identify individuals of interest attempting to gain access to the

UK unlawfully.

This will be achieved by:

1. Once a camera used in a live context captures footage, the LFR software detects individual human faces.
2. Taking the detected face, the software automatically extracts facial features from the image, creating the biometric template.
3. The LFR software compares the biometric template with those held on the Watchlist.
4. When the facial features from two images are compared, the LFR system generates a similarity score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. A threshold value is set to determine when the LFR software will generate an alert to indicate that a possible match has occurred.

The LFR system will be operated by trained Police Officers during deployment, who will review the Alerts and decide as to whether any further action is required. If a match is confirmed they will then transmit that information to IE officers who will then approach the person to establish identity, nationality and lawful status. In this way, the LFR system works to assist IE to make identifications, rather than acting as an autonomous machine-based process devoid of user input.

IE will provide Authorising Officers (AO) to ensure correct deployment and usage of the system. AOs will be correctly trained to support operators and IE personnel to respond to alerts.

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?

Foot passenger arrivals at Holyhead total approximately 300 per day. The LFR system will process facial images for all foot passengers during the proof of concept. Further action will be taken by IE personnel only for those who match the pre-agreed watchlist.

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

Initial proof of concept will be one off activity to gather the benefits of the technology and inform the case for change. This will be clearly defined during a future pathfinder for the full delivery and this DPIA will be updated to reflect any new activity

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?

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 4.8.

If the yes answer is 'yes' and where the other party is external to the HO, please ensure section 5 is completed.

4.7.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:

Processors acting as part of the HO:

- South Wales Police (SWP)
- Greater Manchester Police (GMP)

The above processors will provide operators for the LFR system for the duration of the deployment. As per the deployment process operators will make decisions on whether to proceed with an alert and inform officers for further action. The Authorising Officer (AO) will observe the operators throughout the deployment and monitor matches for bias and to ensure correct procedure is being followed.

4.8 Will any personal data be transferred outside the UK?

☐ Yes ☒ No

If 'no' go to 4.9 If 'yes', provide brief details of the countries and complete Section 6.

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

The LFR will process personal data automatically with a view to identifying whether a person is entering in breach of a Deportation Order. The final decision will however be made by humans (Humans in loop). If the match is confirmed then this could lead to an arrest, investigation and a deprivation of liberty.

The alert generated by a facial match is assessed by officers before a decision is taken as to whether an encounter is necessary. IE have taken steps to ensure that the data used is as accurate and as up to date as is possible, watchlist data has been manually sampled and compared to existing records to ensure accuracy.

There remains a possibility that a false match could occur and that may mean someone is stopped or arrested. However, with the mitigation around data quality, the fact that we have humans in the loop who can check systems, fingerprints and verify information means we have taken steps to minimise any potential adverse effects.

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 4.12.

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

Whilst Live Facial Recognition (LFR) is not a new technology in the industry, it is however new to IE's operations.

The technology detects facial images by:

LFR cameras capturing live footage, the LFR software then detects individual human faces. Taking the detected face, the software automatically extracts facial features from the image, creating the biometric template. The LFR software compares the biometric template with those held on the Watchlist.

When the facial features from two images are compared, the LFR system generates a similarity score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater similarity. A threshold value is set to determine when the LFR software will generate an alert to indicate that a possible match has occurred. That match will then be reviewed by a human decision maker before any action is taken.

Police Colleagues will provide Facial Recognition technology for the proof of concept, supplied by NEC Software Solutions and verified by HO Biometrics, with the NPL report titled Facial Recognition Technology In Law Enforcement Equitability Study . Trained Police Officers will operate the LFR system on IE's behalf, referring all matches to IE & BF personnel for intervention.

IE will deploy trained Authorising Officers (AO) to manage and monitor matches and performance during the deployment.

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

It may be appropriate to pursue engagement opportunities with a number of stakeholders, including local authorities, and public consultative or ethical review bodies.

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

Click or tap here to enter text.

Section 5: Data Sharing/Third party processing

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

5.1 External contact details for data exchange/ processing

Name: Ben Gwyer
Grade: Inspector
Organisation: South Wales Police
Contact email: Ben.Gwyer@south-wales .police.uk

Name: Dominic Edgell
Grade: Sergeant
Organisation: South Wales Police & NPCC
Business Unit/Area: Click or tap here to enter text.
Contact email: Dominic.Edgell@south-wales.police.uk

Contact telephone: Click or tap here to enter text.

Name: Jon Middleton
Grade: Inspector
Organisation: Greater Manchester Police
Contact email: Jon.Middleton@gmp.police.uk

Name: Paul Lockett
Grade: Sergeant
Organisation: Greater Manchester Police
Contact email: Paul.Lockett@gmp.police.uk

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

Common law (list HO function/objective below) ☒

The pilot will look to match facial images from the deportation watchlist with those entering through Holyhead using LFR. This will assist in the identification of people who are returning in breach of their deportation order, a criminal offence contrary to section 24(A1) of the Immigration Act 1971 as amended by NABA 2022.

The purpose of the overt operation is to intercept those people who may be Returning in Breach of a Deportation Order in a legally compliant and ethical manner to enable the IE to achieve legitimate enforcement aims.

Royal Prerogative (HMPO only) ☐

Explicit Statute/power (list statute below) ☐

Click or tap here to enter text.

Implied Statute/power (list statute below) ☒

Implied power from the Immigration Act 1971 (”1971 Act”). Section 24(1A) of the 1971 Act provides that it is a criminal offence for a person to enter the UK in breach of the deportation order. An implied power exists to identify such persons, which the use of LFR falls within.

In the alternative, there is a common law power to use LFR to identify such persons.

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

***See 2.14**

Data will be held by the receiving organisation for the duration of the deployment. Data will be deleted daily from police LFR systems and reuploaded ahead of further shift sessions. Following the pilot all data transferred to police systems will be deleted, no data will be retained for any further amount of time.

Watchlist data will be retained within the LFR system for the duration of the deployment. All watchlist data held within the system will be deleted as soon as practicable following at the end of each shift. Data relating to enforcement action

will be retained for the use of IE and other enforcement agencies, in line with existing processes. Where a false alert is generated, IE will retain anonymised demographic data in order to investigate any potential bias.

The LFR system will process images captured for all individuals entering the Zone of Recognition including members of the public who are not included in the watchlist for deployment. In this event all images that result in a no match are deleted instantly and no data is retained

5.4 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

Click or tap here to enter text.

5.5 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 5.7

Click or tap here to enter text.

5.6 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.

Title: Overarching Umbrella Data Sharing Agreement V4.0

Between: The Secretary Of State For The Home Department, The National Police Chiefs' Council (on behalf of Police Forces of England & Wales), Police Service Of Scotland, Police Service Of Northern Ireland & The National Crime Agency

Published: July 2024

Title: Process-Specific Data Sharing Agreement V1.2

In respect of: Immigration Enforcement

Subject to: Overarching Umbrella Data Sharing Agreement V4.0

Published: April 2025

Contact Name: Jacki Rowson

Grade: Grade 7

Business Unit/Area: Data Protection Lead, Immigration Enforcement

Contact email: Jackie.Rowson@homeoffice.gov.uk

Contact telephone: 07717 546934

5.7 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.
NEC is considered a third-party processor to the Home Office as they are sub-processor acting on behalf of GMP and SWP.
NEC's access to IE data is limited to what is necessary to fulfil contractual obligations. Operationally, the data remains segregated and protected, with no direct access by NEC staff. GMP's contract includes strict data processing conditions aligned with UK GDPR and DPA 2018, ensuring NEC can only process data within the agreed scope and under their control.

Technical impact and viability

5.8 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.

5.9 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.
The following testing will be completed prior to use in a live environment to ensure rollout is workable:

1. Regression testing
2. Usability testing
3. Performance testing
4. Functional testing
5. Compatibility testing (on different browsers)
6. Accessibility testing
7. Security testing (the vulnerability scanner runs daily)

5.10 Confirm if development work is required to ensure systems are Data Protection compliant?

☐ Yes ☒ No

If yes, provide details including time frame

Click or tap here to enter text.

Security Checklist

5.11 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

5.12 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

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

Click or tap here to enter text.

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

☒ Yes ☐ No

5.15 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

Data stored on Amazon Web Services (AWS) in line with delivery partners existing security arrangements (MIDAS, DSA, DDaT). Data will be stored in South Wales and Greate Manchester Police's LFR systems databases for the purpose of the pilot.

Section 6: International transfers

Only complete this section if you have answered yes to question 4.8.

Note: The International Data Sharing/Transfers Guidance should be consulted for further guidance on how to complete this section.

I have read the guidance ☐

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

☐ Yes ☐ No (go to Section 7)

If 'yes', specify the country or countries.

6.2 Is the data transfer required for general processing (UKGDPR / Part 2 DPA) or law enforcement processing (Part 3 DPA)?

☐ General (go to 6.3) ☐ Law enforcement (go to 6.4)

6.3 General processing:

a) Does the country have a UK adequacy regulation for general processing?

☐ Yes ☐ No

b) If 'no', **will the transfer take place on the basis of appropriate safeguards?**

- Pursuant to a legally binding treaty with a public authority which contains enforceable appropriate safeguards for the rights of data subjects and includes effective legal remedies for those rights ☐

i.e. If relying on an existing treaty, **does it cover the purpose(s) for which you need to transfer data?**

☐ Yes ☐ No

- Pursuant to an administrative (non-binding) arrangement with a public authority which contains effective and enforceable appropriate safeguards for the rights of data subjects that has been approved by the Information Commissioner's Office ☐

  i.e. If relying on an existing arrangement, **does it cover the purpose(s) for which you need to transfer data?**

  ☐ Yes ☐ No

- Pursuant to a contract which contains Standard Contractual Clauses for data protection that have been approved by the Information Commissioner's Office ☐

- Pursuant to a contract which doesn't contain Standard Contractual Clauses for data protection but has been approved by the Information Commissioner's Office ☐

c) If not, **will the transfer take place on the basis of a derogation?**

- The data subject has explicitly consented to the transfer, and it has been approved by HOLA ☐

- The transfer is necessary for important reasons of public interest that are laid down in law ☐

- The transfer is necessary for the establishment, exercise or defence of legal claims ☐

- The transfer is necessary in order to protect the vital interests of the data subject or others, where the data subject is physically or legally incapable of giving consent ☐

- The transfer is from a register established by law that is intended for consultation by the public or persons with a legitimate interest ☐

Proceed to question 6.5

6.4 Law enforcement processing:

a) Does the country have a UK adequacy regulation for law enforcement processing?

☐ Yes ☐ No

b) If 'no', **will the transfer take place on the basis of appropriate safeguards?**

- Pursuant to a legally binding treaty with a 'relevant authority' which contains enforceable appropriate safeguards for the rights of data subjects and includes effective legal remedies for those rights ☐

  i. If relying on an existing treaty, **does it cover the purpose(s) for which you need to transfer data?**
  ☐ Yes ☐ No

- A conclusion based on an assessment of the circumstances that appropriate safeguards for the rights of data subjects exist, which has been approved by ODPO and notified to the Information Commissioner's Office ☐

c) If not, **will the transfer take place on the basis of special circumstances?**

- The transfer is necessary to protect the vital interests of the data subject or another person ☐

- The transfer is necessary to safeguard the legitimate interests of the data subject ☐

- The transfer is necessary for the prevention of an immediate and serious threat to public security in the UK or the third country ☐

- The transfer is necessary in an individual case for a law enforcement purpose, and a 'contemporaneous consideration' has been written explaining why the public interest is not overridden by the rights and interests of the data subject in this case ☐

- The transfer is necessary in an individual case for a legal purpose (in connection with legal proceedings; to obtain legal advice; or to establish, exercise or defend legal rights), and a 'contemporaneous consideration' has been written explaining why the public interest is not overridden by the rights and interests of the data subject in this case ☐

d) If the recipient is not a 'relevant authority', is the transfer strictly necessary for a law enforcement purpose?
☐ Yes ☐ No ☐ N/A

6.5 Is a process in place to keep a record of all international transfers?
☐ Yes ☐ No

6.6 If information is to be received from an international partner and retained in Home Office records, is a process in place to mark it as received from that partner?

☐ Yes ☐ No ☐ N/A

Note: The Overseas Security and Justice Assistance (OSJA) Supplementary Guidance should be consulted to determine whether an assessment of human rights, International Humanitarian Law, political and reputational risks is required.

I have read the guidance ☐

Section 7: Risks of the Processing

7.1 Identify and assess risks: Identify the risks and impacts to the rights and freedoms of individuals, the ability to comply with data protection legislation and any corporate risks.

At stage 1 of this DPIA you identified one or more high risk triggers that resulted in completion of a full (stage 2) assessment. Please include those high risks in the table below and complete all columns. Please also include any additional risks that have been identified during this assessment. **For more information about potential privacy risks see the DPIA guidance.**

NB: You should use the Home Office Enterprise Risk Management five-point risk severity scale to calculate the risk by combining scores for impact and likelihood of the risk. Risk management training is also available and should be completed by all staff.

Describe source of risk and nature of potential impact.	**Impact** (Very low/low/ medium/high/ very high)	**Likelihood** (Very low/low/ medium/high/ very high)	**Risk severity score** (Green/ amber/red/purple/ 1-25)
1. Risk of misidentification of individuals, leading to ICE offers intercepting innocent travelers incorrectly.	High	Low	16

2. Data quality issues leading to poor output from the LFR system.	High	Medium	19
3. Human error, an ICE officer decides to or not to intercept incorrectly based on the intelligence given to them by the LFR system	High	Low	16
4. Risk of individuals opposing systemic monitoring. A challenge may be brought by judicial review.	High	High	22
5. The expansion of LFR usage in more areas of the UK may lead to increased monitoring of individuals.	High	Medium	19
6. Processing activity involves mostly sensitive personal data, risk of data being leaked or lost.	High	Low	16
7. processing activity involves sensitive personal data being moved on an encrypted USB device. Risk of loss of the device of data writing failures.	High	Low	16
8. Processing activity involves large-scale data. A watchlist of thousands risks delays in processing.	Medium	Medium	14

7.2 Identify measures to reduce risk: NB If accepting any residual high risk, the ICO should be consulted before proceeding

Identify additional measures you could take to reduce or eliminate risks identified as medium, high or high risk				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** *(Eliminated reduced accepted)*	**Residual risk severity Score** (Green/amber/red /purple/1-25)	**Measure approved** (Yes/no)
1.	LFR technology used has been verified by HO biometrics and tested by SWP for accuracy.	Reduced	12	
2	Manual sweep of images for the watchlist will be conducted to eliminate poor quality	Reduced	10	
3	Clear SOPs will be drafted instructing staff on their powers during the pilot.	Reduced	10	
4	The public will be engaged prior to deployment and lines to respond to challenges will be prepared in advance	Reduced	15	
5	Future deployments will be coordinated centrally within IE, with established controls in place.	Reduced	10	
6	All data for LFR deployments will be handled within the secure Poise	Reduced	12	

	environment using official Home Office Networks.			
7	All encrypted USB device will be tested prior to deployment. During deployment, they will be securely stored and transported at deployment locations by trained personnel.	Reduced	11	
8	Watchlist sizes will be managed first by testing the quality of data images. If additional management is necessary, records within the list can be discounted as needed, based on relevant intelligence	Reduced	10	

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

☒ Yes ☐ No

If 'yes' provide details

It is recognised that LFR interferes with the privacy rights, Art 8 ECHR, of all persons captured by it. This interference is mitigated by the fact that the facial image/recording of persons who are not matched, are immediately deleted.

The use of LFR in this context is considered to be proportionate. Intelligence indicates Holyhead is a high-risk port for individuals entering in breach of a Deportation Order contrary to section 24(A1) of the Immigration Act 1971. Deployment of LFR technology shall contribute to the identification and prosecution of such offenders and shall aid border security. Additional justification for the deployment of LFR will be provided within the policy documents published on the Gov.uk website.

7.4 Are these risks included within a risk register?

☒ Yes ☐ No

If ‘yes’ provide details

All risks to the LFR pilot have been recorded on a central Risk register with clear escalation routes as required. This risk register also reports into central project management structures to effectively manage risk at a wider IE level.

7.5 Has an Equality Impact Assessment been completed?

☒ Yes ☐ No

Section 8: Referral to ODPO

8.1 Referral to the ODPO & DPC

Your DPIA must be referred to ODPO for review, you should email a SharePoint link of your DPIA to the ODPO. Once this is reviewed a SharePoint link of your DPIA must be sent to the data catalogue team for record keeping.

Appropriate links are required to be created for '*people in home office with link*'. Please see How to share DPIA links for guidance on how to do this.

Date referred to the ODPO	Reviewed by:	Date returned to the Author	Comments/ recommendations
18/07/2025	Gillian Brinton Nouch	25/07/2025	Please see comments throughout the document.
11/08/2025	Gillian Brinton Nouch	21/08/2025	Please see comments throughout the document.

8.2 ODPO Review complete

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
02/09/2025		Click or tap to enter a date.	Review complete. I note that this is a time limited proof of concept and as such I would recommend the results are subject to full and robust analysis at the end of the trial period to assess the value/ benefits of the activity before consideration is given to

			extending or repeating the trial. In the event the decision is taken to extend/ repeat the activity or move to BAU, then this DPIA will need to be updated to reflect that position and retuned this ODPO for further review. My only other observation would be that it is not standard practice or policy to publish DPIAs and as such if the intention is to publish this document, or a version there-of I recommend engaging with the Home Office Policy lead; please refer to section 9.1 below.

8.3 IAO sign-off

Date referred to IAO	Name of IAO or person signing on behalf of	Date returned to the Author	Residual risks and measures approved Y/N	Comment (including approved to proceed Y/N)
21/11/2025	Gordon Summers	21/11/2025	Y	Approved to proceed

Section 9: Referral to HO Data and Analytics Steering Committee

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

9.1 Criteria for referral to the Data and Analytics Steering Committee

Criteria	Met
ODPO have identified a risk that, in its opinion, requires escalation to the ICO (regardless of risk severity; guidance will be produced in due course once examples indicate how this might be revealed). The view of the Chair of the Data and Analytics Steering Committee will be sought in advance of any such escalation.	
ODPO reason for referral if not one listed below: [ODPO insert detail]	
There is a significant impact, either qualitative and/or quantitative, upon individual rights, this may be one or more of the following:	
An instance where the proposal will not meet the Home Office obligations to meet the individual rights and protections of data subjects as defined in UK GDPR and DPA18.	
An instance where the proposal is likely to result in any person(s) individual privacy/data protection rights being compromised.	
A particular concern is identified having regard to the purpose, method of processing and location of processing that in combination warrants further escalation or consideration.	
High sensitivity – the nature of the personal data itself is so sensitive, even though the rest of the risks around processing were low. The committee could be asked to scrutinize but equally the Board could determine that it did not need to do so.	
It is not possible to implement all recommended controls/mitigations. (Where controls and mitigations have been identified but result in a short period of heightened risk this **would not** warrant escalation).	
High likelihood of challenge or regulatory enforcement being brought, or a high likelihood of such a challenge or action being successful against the HO.	
Where a proposal resulted in advice that the processing would be unlawful, and the project has since revised (tweaked) the proposal this should be referred to the Committee.	
Specific referral circumstances:	
Data processing has been promised by a Minister/ the Cabinet, but there are questions as to whether there is a sufficient legislative/technical /administrative framework in place to enable this.	
A decision has been made to prefer specific safeguards over others or a riskier approach.	
An issue that is business critical emerges e.g. essential work to a business-critical system, that may mean that data subjects rights may not be met.	
Where processing is likely to attract significant controversy.	

Other: [add detail]	

9.2 Referred to the HO Data and Analytics Steering Committee.

Referred to Data and Analytics Steering Committee	Referred to Data and Analytics Steering Committee	Date of the Data and Analytics Steering Committee (if appropriate)	Date returned to the Author
Click or tap to enter a date.	Yes ☐ No ☐	Click or tap to enter a date.	Click or tap to enter a date.
Recommendations/ findings/ comments from the Data and Analytics Steering Committee			