Data Protection Impact Assessment (DPIA) Template

Proposal/ Project/Activity title	Facial Recognition
Information Asset Owner(s)	G. Summers

URN:105.25

Document Control

	Name	Job Title	Date
DPIA Drafted by	R Granger	**Project Manager**	**26/06/2025**
Reviewed by	P Warham	**Programme Manager**	**26/06/2025**
Lead DPP for business area	J Rowson	**IE Data Protection Lead**	**1 & 19 May 2025**
Lead business owner /project manager/policy owner	A 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
Final 3.1	15/12/2025	Submitted for ODPO Review
Final 4.0	02/02/2026	Sign off by SRO
Final 4.0	02/02/2026	Sign off by SRO
Final 4.1	19/02/2026	Sign off by SRO

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
R Cage	Deputy Director IE Strategic Services and Transformation	20 February 2026

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) will be deploying standard LFR enabled cameras attached to mobile vehicles or laptops with linked Live Facial Recognition (LFR) software attached.

   The LFR vans will capture images of all persons who walk within designated zones and extract a biometric template of the facial features which is then compared against a pre-populated watchlist of images of specific identified persons of interest.

   Any image scanned which does not flag a potential match is automatically and almost instantaneously deleted.

   The originating images are not retained by IE or police. IE and police forces have released extensive websites to ensure lawful and transparent processing

[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.

these are publicly accessible. The Police force supporting at each operation will be specified on the public facing website.

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
    - 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:	R Cage
Telephone Number:	Click or tap here to enter text.
Information Asset title:	IE Strategic Services and Transformation
Email:	Click or tap here to enter text.
Name:	F 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:	R Granger
Telephone Number:	Click or tap here to enter text.
Business Unit/Team:	Emerging Technology, Data and Innovation
Directorate:	Immigration Enforcement

1.5 Date DPIA commenced:

15/04/2025

1.6 Date processing activity to commence (if known):

06/10/2025

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):

To be allocated by the DC team

1.8 DPIA version:

Version 4.0

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

1. ATLAS
2. Data Services and Analytics (DSA)
3. Immigration and Asylum Biometric System (IABS)
4. Gov.uk DPIA
5. South Wales Police Force DPIA – lfr-dpia.pdf
6. Greater Manchester Police DPIA – IVRO - NineWorks - DPIA Screening Questionnaire
7. Sussex and Surrey Police Force DPIA - SxSy-DPIA_LFR_Deployments, surrey-and-sussex---dpia-lfr-software.pdf

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 a redacted version of 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. Updated versions of all documents will be prepared and similarly published for all subsequent LFR deployments that are led by IE.

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?

Immigration Enforcement (IE) will extract data from caseworking systems relating to individuals subject to a Deportation Order (DO), who are over 18 and have been removed from the UK and those wanted for an immigration-related criminal offence. The extracted data will be washed by Home Office Biometrics against the IABs database to obtain the corresponding image, which will then be used to finalise the watchlist for the deployment and to create an offline extract copy for sharing with law enforcement partners.

This extracted information will only be used for the purpose of a single deployment. For deployments, the data will be extracted as close to the deployment as possible to ensure the highest level of accuracy. A dip sample of 100 records will be conducted to ensure data quality, and, as a final safeguard, the NEC system will automatically check all images for quality.

The LFR system 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 or who are wanted for an immigration-related criminal offence. 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 Police colleagues act as the LFR operator on behalf of IE. All Police colleagues will be from an authorised LFR-equipped police force. They 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.

When encountering an individual who is subject to a match from the LFR system, Frontline IE officers will also have access to the immigration systems relevant to confirming the subject's identity & status (Atlas, CRS & Pronto). 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 procedures.

- 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, health or criminality
- Reporting Details
- Barriers to removal

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 capture 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 IE watchlist and therefore they should not lead to a match.

There will be signage, leaflets and officers on hand to address any concerns during the pilot deployment.

Anyone under 18 who is encountered linked to a subject within the watchlist. Standard IE protocol for handling minors in an encounter will be followed. All will be cognisant of their duty under section 55 of the Borders, Citizenship and Immigration Act 2009

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 Home Office 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) Authorising Officers,
c) 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
    e. In line with Home Office practices and dependant on location all signage and leaflets will be in Welsh and English and is consistent with NPCC LFR materials.

f. A uniformed officer is on hand to answer any questions for the duration of the deployment. Officers have access to interpretation services if required.

d) 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 biometric data and watchlist images are tightly defined. The generation of the watchlist is restricted to specific staff who, on clear instruction from the approved governance processes, will extract the watchlist data and associated images for controlled transportation to the deployment location.

The finalised offline watchlist will be stored on an encrypted USB stick that will be accessed by the LFR operator only at the deployment location. The watchlist data will be extract the watchlist directly into the LFR software in the van, at which point the watchlist will be deleted from the USB stick. The watchlist data is only retained for a short period of time, this being the active deployment as it is not anticipated that further use would be feasible.

Once imported, the watchlist and associated biometric templates will only be accessible to the LFR operator, therefore ensuring necessity of access to a restricted number of users.

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 employed staff and authorised police personnel working on this deployment will be security cleared to the appropriate level within their organisation, typically SC.

2.8a. How will access be controlled?

Systems and controls

System/ Data	Who has access	How is it controlled
Immigration System Data	Immigration Enforcement colleagues via role-specific profiles.	Individual password protected user profile dependant on role
Home Office Supplied Laptop	User assigned at distribution.	Enterprise secured data network Bit locker and password protected to individual user.
Watchlist Extract/ Encrypted USB stick	Authorised Home Office Employee supporting the deployment.	Password access to the HO supplied laptop. The USB stick is encrypted with a passcode only available to necessary staff.
LFR system on a standalone laptop	Authorised LFR trained operators	Force assigned system log-in.

Background

To share the required data. The LFR watchlist is generated from Home Office systems from Atlas and IABS. 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 IE deployments, Police cameras will be used to operate the LFR system. The 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 Police as soon as is practicable and in any case within 24 hours.

For this deployment no camera 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 individual 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.

All personnel assigned to the deployment will hold appropriate level of security clearance and system access will be regulated according to their role and clearance level.

2.9 Where will the data be stored?

The offline watchlist, once drawn from HO systems, will be stored in an access-controlled space only accessible by named members of the LFR team. For a deployment this data will be downloaded to a Home Office supplied secured, encrypted USB device. Which will be uploaded to the supporting police force's standalone secure police Live Facial Recognition (LFR) computer to enable the LFR system to function.

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.

The data to create the offline watchlist will be drawn from Home Office systems as close as is practicable to the LFR deployment. This data will be used for the purpose and duration of this deployment only and will be deleted within 24 hours of completion of deployment.

Ahead of any future deployments the data extraction steps will be conducted again to deploy using the most up to date data as is available at the time of extraction.

These systems have the means to meet these data subject rights where appropriate 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 cameras will be used to operate the LFR system. The LFR camera feed will not be stored, this will be real time processing only. Any biometric templates that do not generate a hit on the LFR system will not be stored. Any hits that generate a LFR potential match will be retained for a period of 24 hours only and manually deleted by the operator.

There is no necessity to retain the match data as it has been verified by the operator. Watchlist images uploaded to the system and transferred to the system via encrypted USB memory stick are deleted from the LFR system and USB stick within 24 hours of the conclusion deployment or at midnight each day of the day of deployment if the deployment if longer than 24 hours.

For LFR deployments, the Home Office can only generate one offline watchlist per deployment (regardless of the length of deployment) due to technical restrictions. The offline watchlist generated for the purpose of the deployment will be deleted from secured Home Office systems at the conclusion of the deployment.

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?

A deployment can be up to 3 days in length, unless extended by a further authorisation. 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) Any images captured by the police cameras and processed by the LFR system that do not generate a match will be automatically deleted from the LFR system.

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

c) With the police-controlled LFR laptop being used to operate the LFR system, where a deployment crosses over multiple days, the offline watchlist is deleted at the conclusion of each day and re-uploaded prior to the following days deployment.

d) Where the LFR system generates an alert report, all personal data is deleted within 24 hours of the completion of that day's deployment.

In the event of a False positive, anonymised match data will be retained by IE to assist with further investigation of system performance. This data will be acquired from Police 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. As per this procedure at the conclusion of the investigation all data will be deleted

At the conclusion for the deployment a match report 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 from the Police LFR system within 24 hours of the completion of the deployment.

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 each day of the deployment. All watchlist data held within the police LFR system will be deleted as soon as practicable following the end of each day of the deployment. Data relating to enforcement action will be retained for the use of IE and other enforcement agencies, in line with existing processes.

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 personal is retained.

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

Data Move	Method	Between	Safeguards
Finalised Watchlist to Encrypted USB Memory Stick	Physical file transfer	LFR Team Poise Secured laptop – Encrypted USB Memory Stick	Transfer will be conducted by agreed staff, using agreed HO equipment in a secured location
Transfer to Supporting Police Force's LFR System	Physical File Transfer	Encrypted USB Memory Stick – LFR System	Transfer will be conducted by agreed staff, using agreed HO equipment in a secured location

Offline 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 named nominated members of staff.
4. The encrypted USB will be transferred a short distance to the LFR system where the data is uploaded.
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

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 deployment.

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

Specified SPOC identified as recipient of the data. The USB is also encrypted and transported in a lock box and governed by outward and return procedures.

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?**

We are publishing anonymised quantitative data onto the Gov.uk website. No private information will be published as part of this. All published pages on the Gov.uk website are subject to the privacy policies below:

Gov.uk privacy Policy - Privacy notice - GOV.UK
Cookie Guidance Cookies on GOV.UK

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 deploy Live Facial Recognition (LFR) technology as a precision tactic to locate people who are sought by IE for law enforcement purposes. Focussing on individuals returning in breach of a deportation order, which is a criminal offence, or who are wanted for an immigration-related criminal offence.

LFR deployments will be authorised for up to 3 days targeting arrivals throughout the length of the deployment. Deployments will take place at UK ports. The LFR technology will only be active during disembarkation. Previous deployments have amounted to an average of 1000 faces seen per 24-hour period during a deployment. However, passenger arrivals will vary dependant on time of day and seasonal travel.

Recent intelligence indicates that CTA ports are frequently used as an entry point by individuals with deportation orders or to avoid detection if they are wanted in respect of an immigration-related criminal offence. The purpose of the overt operations is principally to intercept those people 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 as amended by Nationality and Border Act (NABA) 2022 that is currently punishable by up to five years imprisonment or a fine (or both).
Those that are wanted by Crime and Financial investigation teams who have been unable to be traced through traditional means will be included on the watchlist as they are wanted for an immigration-related criminal offence but remain at large.

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(A1) of the 1971 Act, as amended by Nationality and Border Act (NABA) 2022, 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.

Part 3 of the Immigration Act 1971 sets out a number of immigration-related criminal offences. It also provides the ability to obtain warrants to arrest and search premises in relation to such offences. Those that are wanted by Crime and Financial investigation teams who have been unable to be traced through traditional means will be included on the watchlist as they are wanted for an immigration-related criminal offence and remain at large. There is an implied power from the 1971 Act to identify such persons, which the use of LFR falls within.

Additionally, there is a common law power to use LFR to identify such persons. In Bridges v SWP [2019] EWHC 2341 (Admin), the High Court confirmed that common law powers were sufficient for the police to operate LFR. This finding was not disturbed on appeal. Further powers can be found in IE LFR Policy document.

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. **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 ☐
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: Images will have been provided principally for immigration purposes. The legal power for comprising the watchlist gallery is provided by Part 2 of the Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021, which permits such images to be used for law enforcement purposes whilst they are held for immigration purposes. In relation to IE LFR deployments, these are the legal powers used to take photographs of deportees prior to removal and for other defined circumstances, and which allow their use for immigration and law enforcement purposes (under Regulation 4).

The Policy document and SOP prepared for the LFR trial set out clear criteria for watchlist inclusion, including the intelligence-based rationale on which it is based and the validation and authorisation processes that must be observed in compiling and using the watchlist. To ensure compliance with the SOP, the deployment request must be sent to the Authorising Officer and the Record of Authorisation made by that officer should confirm that the deployment adheres to the principles within it around watchlist generation and compilation, including the criteria that applies to which images may be included on the Watchlist, in what circumstances and for what purpose, to ensure that the necessity and proportionality criteria for the Watchlist are satisfied.

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 lack of a routine immigration control on CTA routes provides a border security vulnerability which is being exploited by some to circumvent immigration controls.

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

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?

For the first two proof of concept deployments, we scanned approximately 7500 faces across the full deployment. However, this is subject to change due to timings of crossing and seasonal travel for future deployments. Although this is faces seen by the technology, we estimate at around 300 passengers per day will be subject to the LFR.

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

The first two proof of concept deployments focussed only on foot passengers using a LFR enabled Police vehicle housing the LFR system and cameras.

Further deployments are planned. The next one is intended to relate to foot passengers in the arrivals hall and vehicle lanes and shall take place in late February 2026.

.

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 on behalf of the HO as controller:

- Supporting Police Force
- National Police Chiefs Council (NPCC)

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.

The LFR NeoFace software is a siloed non-networked system which is subject to security measures, this includes restricted access and is only accessible to trained staff to upload and view the watchlist data.

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 the individual seeking to enter the UK is subject to an extant Deportation Order or wanted for an immigration related criminal offence. 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.

4.10 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, namely watchlist dip sampling, LFR system quality processing and 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.

4.11 Does the proposal involve automated decision-making?

☐ Yes ☒ No

If yes, provide details

Click or tap here to enter text.

4.12 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 law enforcement, it is however relatively 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 LFR deployments, supplied by NEC Software Solutions and verified by HO Biometrics, which is referenced within the NPL report titled Facial Recognition Technology in Law Enforcement Equitability Study.

Trained Police Officers will operate the LFR system on Home Office's behalf, referring all matches to IE personnel for intervention.

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

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

The following have already been informed in respect of our LFR deployments and invited to comment if applicable:

- Biometric Forensic Ethics Group (BFEG) now known as Science and Technology Advisory Committee (STEAC)
- ICO Biometrics and surveillance camera commissioner
- Office of the Data protection Officer
- Equalities and human rights commission
- National Police Chief's Council (NPCC)
- Police Liaison Unit Wales
- Welsh Office

This activity has ministerial backing and IE remain cognisant that there is an ongoing public consultation into the use of Facial recognition in the UK.

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: D Gallichan
Grade: Inspector
Organisation: Sussex and Surrey Police
Contact email:

Name: D Edgell
Grade: Sergeant
Organisation: South Wales Police & NPCC
Business Unit/Area: Click or tap here to enter text.
Contact email:
Contact telephone: Click or tap here to enter text.

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

Common law (list HO function/objective below) ☒

LFR deployments will look to identify persons returning in breach of a deportation order and those wanted in respect of an immigration-related criminal offence.

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(A1) of the 1971 Immigration Act as amended by Nationality and Border Act (NABA) 2022, provides that it is a criminal offence for a person to enter the UK in breach of the deportation order; knowingly entering without required entry clearance is an offence under section 24 (B1) potentially punishable by a four-year custodial sentence. An implied power exists to identify such persons, which the use of LFR falls within.

Part 3 of the Immigration Act 1971 sets out a number of immigration-related criminal offences. It also provides the ability to obtain warrants to arrest and search premises in relation to such offences. Those that are wanted by Crime and

Financial investigation teams who have been unable to be traced through traditional means will be included on the watchlist as they are wanted for an immigration-related criminal offence and remain at large. There is an implied power from the 1971 Act to identify such persons, which the use of LFR falls within.

Alternatively, there is a common law power to use LFR to identify such persons. In Bridges v SWP [2019] EWHC 2341 (Admin), the High Court confirmed that common law powers were sufficient for the police to operate LFR. This finding was not disturbed on appeal.

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**

The police are acting as processors for the Home Office, while the Home Office are the controllers. The Home Office is only providing data relating to individuals who are subject to a Deportation Order or an immigration related criminal offence, via an offline watchlist, to enable the supporting LFR-enabled police force to operate LFR on its behalf. There is no off-site data processing; the processors will only hold the information for the duration of the deployment, and upon completion of the tasks, the LFR system will be wiped.

Anonymised numerical 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 to investigate any potential bias.

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**

Watchlist data will be retained within the LFR system for the duration of the day of the deployment. All watchlist data held within the police LFR system will be deleted as soon as practicable following the end of each day of the deployment. Data relating to enforcement action will be retained for the use of IE and other enforcement agencies, in line with existing processes.

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 personal is retained.

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.

There is an overarching MoU between Policing and the Home Office in regards to data sharing. In the case of LFR, the Home Office is acting as the controller and the supporting police for as the processor. This is an unusual arrangement, and a separate data sharing agreement has been drafted to supplement the existing processes in place.

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 sub-processor acting on behalf of the supporting police force. In that fact they provide the technology to the authorised LFR equipped police force in support of image processing. However, any NEC access to this data is limited to the use of their technology only which has been licenced to the relevant LFR equipped police force.

Operationally, the data remains segregated and protected, with no direct access by NEC staff. The Home Office 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.

NEC will have no direct access to any Home Office data, and they are only providing the LFR software.

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

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. Usability testing
2. Performance testing
3. Functional testing
4. Accessibility testing

All testing has been completed during previous proof of concept deployments, and the results of the above testing have been covered within the post-deployment report.

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?

N/A

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

The offline watchlist will be downloaded and stored on the encrypted USB memory stick prior to being uploaded to the LFR system. The offline watchlist Data will be stored in the supporting Police's LFR systems for the purpose and duration of the day of the deployment.

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. Misidentification (false positive/negative) leading to incorrect interception or failure to intercept individuals.	High	Low	16
2. Poor quality or outdated watchlist data degrading LFR accuracy, quality or outdated watchlist data degrading LFR accuracy.	High	Medium	19
3. Human error by Police LFR operators or IE officers in interpreting alerts.	High	Low	12
4. Public or legal challenge regarding systematic monitoring use of LFR (Art. 8 ECHR, JR risk).	High	High	22
5. Future expansion of LFR deployments creating greater monitoring exposure.	High	Medium	19
6. Data breach or loss of highly sensitive biometric and immigration data.	High	Low	16
7. Loss or corruption of encrypted USB devices used to transport the watchlist.	High	Low	16
8. Large-scale processing reducing system performance or causing delays.	Medium	Medium	14

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)
9. Deleted police LFR laptop data being recoverable without forensic wipe.	High	Low	12
10. Bias or unequal system performance across demographic groups.	High	Low	16
11. Insufficient transparency to travellers if signage/leaflets are unclear or missing.	High	Medium	19
12. Match for children's facial image despite non-inclusion on watchlist.	High	Low	16
13. Zone of Recognition extending beyond operational necessity, risking excessive data capture.	Medium	Medium	14
14. Accidental retention of CCTV-like footage by Police cameras. -like footage by Police cameras.	High	Low	16
15. Chain of custody risks during manual movement of removable media.	High	Low	16
16. Risk of Police processors not strictly following HO deletion protocols.	High	Low	16
17. Inconsistent operator training between LFR-equipped forces.	Medium	Medium	14

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)
18. Out of date intelligence feeding watchlist composition.	High	Low	16
19. Conflict/escalation risk during passenger encounters following LFR alerts.	High	Low	16
20. Mishandling of vulnerable individuals whose ATLAS profiles include health/safeguarding markers.	High	Medium	19
22. Equality impacts not fully mitigated despite EIA completion (public sector equality duty).	High	Medium	19

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	Only use HO verified LFR systems (NEC) with human in the loop and secondary ID checks (ATLAS/CRS/fingerprints).verified LFR systems (NEC) with human in the loop and secondary ID checks (ATLAS/CRS/fingerprints).verified LFR systems (NEC) with human in the loop and secondary ID checks (ATLAS/CRS/fingerprints).-verified LFR systems (NEC) with human-in-the-loop and secondary ID checks (ATLAS/CRS/fingerprints).	Reduced	12	
2	Manual dip sampling of 1,200 images; NEC image quality checks; watchlist refreshed pre-deployment.	Reduced	10	
3	SOPs for decision making, structured operator training, AO oversight.	Reduced	10	
4	Pre-deployment public engagement; signage; GOV.UK notices; publication of DPIA/ ; adherence to ICO/SC Code.	Reduced	15	

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)
5	Central IE governance for any future deployments; strict scope control.	Reduced	10	
6	BitLocker encryption; secure SharePoint; restricted access; daily deletion cycle; no retention of non-matches.	Reduced	12	
7	Pre-tested encrypted USBs; chain of custody log; secure lockboxes; trained handlers.	Reduced	11	
8	Manage watchlist size; quality filtering; intelligence-led prioritisation; high-capacity Police LFR systems.	Reduced	10	
9	BitLocker encryption on Police laptops; mandatory deletion within 24h; no raw video retention.	Reduced	10	
10	Monitor demographic false alerts; AOs observe operator decisions; use of NPL findings; refine image thresholds.	Reduced	12	
11	Ensure signage/leaflets are visible, bilingual and consistent with NPCC materials; officer engagement on-site.	Reduced	10	
12	Officers trained in handling minors; minors excluded from watchlist; instant deletion of non-matches.	Reduced	11	

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)
13	Technical restriction of capture zone to operational necessity; camera placement review with Police.	Reduced	10	
14	Reinforce Police process to delete accidental footage immediately; audit checks.	Reduced	10	
15	Documented transfer steps; audit logs; secure containers; minimise movement between sites.	Reduced	11	
16	MoU with NPCC; clear deletion requirements; daily AO confirmation of deletion events.	Reduced	11	
17	Standardised operator and AO training package across all supporting forces.	Reduced	10	
18	Watchlist regenerated as close as possible to deployment; cross-check against ATLAS/IABS live data.	Reduced	10	
19	Clear encounter scripts; officer safety and de-escalation guidance; presence of bilingual/interpretation services.	Reduced	12	
20	SOPs for vulnerable persons; access to ATLAS vulnerability markers; safeguarding referral options.	Reduced	12	
21	Commitment to update DPIA before any BAU rollout; ODPO engagement.	Reduced	10	

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)
22	Monitoring for bias during deployment; reference to EIA; AO oversight for protected characteristics.	Reduced	12	

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

The Home Office has considered the risks of deploying LFR technology in regard to the public against the legitimate aims of the Home Office as follows:

Home Office Mission	Impact on Public	Benefit
Safer streets	Negligible to none, current deployment activities are focussed within the port environment and won’t encroach on the public during day-to-day life.	LFR deployments are aimed at those subject to a DO or who are wanted for immigration-related criminal offences attempting to re-enter the UK. Therefore, supporting the Home Office’s safer streets mission.
Integrity of the border	Limited – passengers within the port environment may experience minor delays when LFR is operational. Within a port or border environment the public expect a heightened level of security In the event of an alert, the subject will be stopped and their identity confirmed, accompanying passengers will be stopped alongside the subject. Members of the public captured by the LFR camera who do not match to the watchlist will have their image deleted within 1 second. Additional IE officers to the normal port operations will be present to act upon intelligence from the LFR system. Creating a high presence, but allowing members of the public to seek support due to higher visibility	LFR deployments are aimed at those subject to DO or who are wanted for immigration-related offences. Building confidence and resilience with the UK Border. Introducing an effective intelligence-led system to identify those who are persons of interest will contribute to IE’s strategic aims.
Immigration enforcement aims and Objectives		Introducing an effective intelligence led system to identify those who are persons of interest will contribute to IE‘s strategic aims. This system builds into the Protect mission, as we are preventing high harm individuals from re-entering the UK and thus protecting the UK public.

Home Office Mission	Impact on Public	Benefit
Protection of individuals at risk	Limited – passengers within the port environment may experience minor delays when LFR is operational. Within a port or border environment the public expect a heightened level of security Additional IE officers to the normal port operations will be present to act upon intelligence from the LFR system. Creating a high presence, but allowing members of the public to seek support due to higher visibility	The aim of the processing is to assist in the identification of subjects attempting to enter the UK in breach of DO or wanted for immigration criminal offences. By this nature we are assisting with the protection of individuals at risk.
Government priority for restoring governance and control		The principal aim of the processing is to assist in the identification of subjects attempting to enter the UK in breach of DO or whilst wanted for immigration criminal offences. These individuals may have previous convictions from UK courts, and preventing their return to the UK works towards this objective.

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 chances or erroneously arresting a subject are low.

The use of LFR in this context is considered to be proportionate. Intelligence indicates CTA ports are high-risk locations for individuals entering in breach of a Deportation Order contrary to section 24(A1) of the Immigration Act 1971 as amended by Nationality and Border Act (NABA) 2022, or for evading attention if they are wanted for immigration-related criminal offences.

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 project Risk Register with clear escalation routes through IE’s chain of command as required. This risk register also reports into central project management structures to effectively manage risk at a wider IE level. These risks are owned by the project SRO Gordon Summers as listed on this DPIA.

7.5 Has an Equality Impact Assessment been completed?

☒ Yes ☐ No