

Data Protection Impact Assessment (DPIA) Template

Proposal/ Project/Activity title	Immigration Enforcement – Live Facial Recognition Hardware, Software and Deployment Processing
Information Asset Owner(s)	Gordon Summers

URN: 184.26

Document Control

	Name	Job Title	Date
DPIA Drafted by	R Granger	Project Manager	15/04/26
Reviewed by	M Wilkinson	Programme Manager	17/07/26
Lead DPP for business area	Nicola Allen Jackie Rowson	IE Data Protection Lead	13/07/26
Lead business owner /project manager/policy owner	Andy Clark	IE Business Rules Programme Manager	17/07/26

Version/Change history

Version	Date	Comments
Draft 4.2	14/07/2026	Draft 4.2 – DPO review amendments.
Draft 4.3	15/07/26	DPO review comments incorporated.
Draft 4.4	27/07/2026	IAO comment incorporated
Version 5.1	05/08/26	Approved version following ODPO review

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 Rob Cage	IE ICE ROM North Director Head of Strategic Delivery Command	20/07/2027 27/07/2027

Contents

<u>DPIA Stage 1</u>	<u>4</u>
DPIA Stage 2	8
Section 1: Background and contacts	8
Section 2: Personal data.....	10
Section 3: Purpose of the processing	26
Section 4: Processing activity	31
Section 5: Data Sharing/Third party processing	37
Complete this section if you have answered 'yes' to question Q.4.7.	37
Technical impact and viability	42
Security Checklist	43
Section 6: International transfers	44
Only complete this section if you have answered yes to question 4.8.	44
Section 7: Risks of the Processing	47

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.**

Redraft note: This DPIA is a redraft of the original DPIA prepared for the Live Facial Recognition proof of concept. The programme has now moved into a formal delivery phase. To simplify governance, clarify processing boundaries and support clearer assurance, the previous single DPIA has been separated into two linked assessments: one covering the Facial Recognition Watchlist Generator, including the creation and management of deployment-specific watchlists; and this DPIA, which covers the LFR software, hardware and associated operational processing used during deployments.

DPIA Stage 1

Summary of the processing

1. **Does the proposal/project/activity involve the processing¹ 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.]

Live Facial Recognition (LFR) supports officers in identifying individuals where human recognition alone may be insufficient, such as in crowded transport hubs. It compares faces in real time against a controlled watchlist using settings informed by supplier guidance, National Physical Laboratory testing outcomes where applicable, and relevant policing guidance. Trained officers/operators always review system

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.

alerts before any action is taken. LFR is used only where necessary and proportionate, with safeguards, oversight, transparency and ongoing review to uphold data protection and human rights standards.

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 Hardware, Software and Deployment Processing

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

1.3 Information Asset Owner(s) (IAO):

Email: Gordon.summers2@homeoffice.gov.uk
Name: Gordon Summers
Telephone Number: 07990 798716
Information Asset title: IE - ICE North

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

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

Email: Matthew.wilkinson10@homeoffice.gov.uk
Name: Matt Wilkinson
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:

15/04/2026

1.6 Date processing activity to commence (if known):

01/11/2026

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 UK GDPR and will require an incident report.

Processing has not commenced under the programme phase. A proof of concept was previously undertaken under a separate DPIA.

The DPIA is being completed in advance of planned deployment activity.

1.7 Information Asset Register reference (if applicable):

To be allocated by the Data Catalogue team and linked to the relevant IABS information asset record before approval.

1.8 DPIA version

Draft 4.4 – DPO review amendments

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)
GOV.UK DPIA
4. IE Facial Recognition Watchlist Generator (FRWG) URN:

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

01/09/2026 (tbc)

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

IE will publish a redacted version of this LFR DPIA to support transparency, subject to operational, security, legal professional privilege and law enforcement sensitivity considerations. IE will also consider any request for this DPIA under the Freedom of Information Act 2000, taking advice from the ODPO, Legal Advisers and/or the ICO where appropriate.

IE has also prepared supporting documentation for the LFR programme, including policy, operational guidance, deployment documentation, equality assessment and risk assessment material. Redacted versions of relevant documents will be published on a dedicated webpage for LFR deployments where publication does not undermine operational effectiveness, public safety, legal obligations or the rights and freedoms of individuals.

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.

This section describes the personal data processed by the LFR hardware and software during authorised deployments. It does not repeat the full assessment of the upstream creation of the watchlist, which is covered by the linked IE Facial Recognition Watchlist Generator DPIA, or the full operation of underlying Home Office source systems, which are covered by their own DPIAs.

2.1 What personal data is being processed?

Immigration Enforcement (IE) will extract data and related facial images from case working systems relating to individuals of interest as defined within the IE LFR policy document. The extracted data will be used to create an offline extract for sharing with IE Live Facial Recognition (LFR) teams and/or law enforcement partners.

This extracted information will only be used for the purpose of authorised LFR deployments. 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 system will automatically check all images for quality.

Watchlists

Watchlists are deployment-specific, time-limited and purpose-specific. They are created only for an authorised LFR deployment and are limited to individuals who meet the eligibility criteria set out in the IE LFR Policy and the defined enforcement purpose for that deployment. They are not compiled for general intelligence gathering, speculative monitoring or exploratory use.

The creation of the watchlist is covered by the linked Facial Recognition Watchlist Generator DPIA. This DPIA focuses on the subsequent use of that watchlist within the LFR software and hardware during deployment. Once the watchlist has been approved through the required governance and authorisation process, it is securely transferred to the LFR system for use during that deployment only.

The watchlist contains limited information required to support identification and officer review, such as the individual's name, date of birth, nationality and facial image. The LFR system converts the facial image into a biometric template for comparison against live probe images captured during the deployment. Inclusion on a watchlist does not itself result in any enforcement action. Any alert generated by the system is reviewed by a trained officer/operator, and any subsequent engagement or enforcement decision is made by officers following further human checks and the exercise of lawful powers.

Watchlist data is subject to strict access controls. It is handled only by trained and appropriately cleared personnel, transferred using approved secure methods, and retained only for the period necessary to support the deployment. Data relating to non-matches is deleted immediately by the LFR system. Watchlist data and associated biometric templates are deleted from the LFR system and any transfer media within the approved retention period following the conclusion of the deployment.

For joint deployments, any sharing of watchlist data with police forces or other partners will be governed by a deployment-specific data sharing arrangement. This will set out the purpose of the sharing, legal basis, controller or processor roles, watchlist criteria, security arrangements, retention and deletion requirements, and audit responsibilities.

Hardware, software and joint deployment arrangements

The hardware and software used to support an LFR deployment may be provided and operated by Immigration Enforcement, a police force, or both, depending on the nature, location and operational lead for the deployment. For example, some deployments may use IE-owned or IE-managed LFR equipment, while joint deployments with policing partners may involve police-provided LFR hardware, software, vehicles, cameras or trained operators. In all cases, the deployment model, equipment owner, operator roles and access arrangements will be identified and recorded in advance as part of the deployment authorisation and data management process.

Where IE and a police force jointly determine the purposes and means of processing personal data for an LFR deployment, the parties will enter into a specific data sharing agreement covering processing under Part 2 and/or Part 3 of the Data Protection Act 2018, as applicable to the purpose of the deployment. The agreement will set out the respective roles and responsibilities of the parties as joint controllers, including the purpose of the sharing, applicable legal basis, watchlist criteria, use of any IE or police hardware and software, access controls, security arrangements,

retention and deletion requirements, audit responsibilities, handling of data subject rights, and procedures for managing incidents or breaches.

Where one party provides technical capability or operational support without determining the purposes and means of the processing, the data sharing agreement or associated deployment documentation will make clear whether that party is acting as a processor, sub-processor or controller in its own right. The final controller/processor position will be confirmed for each deployment before processing begins, reflecting the operational model and the applicable Part 2 and/or Part 3 processing regime.

The LFR supplier is not expected to have routine access to live deployment data, watchlist data, biometric templates, match alerts or retained reports. If supplier access to personal data is required for maintenance, support, troubleshooting, testing or assurance, this will be limited to what is necessary, authorised in advance, recorded, and governed by a legally binding contract or equivalent written agreement. The contract or agreement will set out the supplier's role, the Home Office's documented instructions, security and confidentiality requirements, restrictions on sub-processing, audit and assurance arrangements, incident reporting, retention and deletion requirements, and the return or secure destruction of personal data at the end of the service. Further detail is provided in response to Q4.7a and Section 5.

The LFR system operates as a standalone deployment system and is not connected to wider Home Office infrastructure during live operation.

When reviewing alerts, the LFR operator will have access to the following information for individuals on the approved watchlist. The operator will use this information to assess whether the alert should be referred to IE officers for possible engagement.

- Name
- Date of birth
- Nationality
- Image
- Immigration references – Home Office (HO) reference, personal identity reference

- Immigration case types

Where an alert is reviewed and referred for officer engagement, frontline IE officers may carry out follow-up checks on existing Home Office systems to confirm identity, immigration status and the appropriate lawful response. Those systems are covered by their own DPIAs and access is governed by existing role-based access controls and 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) ☒

Processing Regime Determination

IE undertakes both administrative immigration functions and criminal law enforcement functions. For each deployment, the applicable processing regime is determined by the primary purpose of the deployment:

- Part 2 (UK GDPR / Part 2 DPA 2018) applies where LFR supports administrative or civil immigration activity (e.g., administrative detention or removal activity under Immigration Act powers).
- Part 3 DPA 2018 applies where LFR supports the prevention, detection, investigation or prosecution of criminal offences, or the execution of criminal penalties.

The applicable regime, legal basis, necessity and proportionality assessment, and safeguards are recorded and authorised in advance for each deployment.

A deployment regime determination record will be completed for every deployment and approved by the Authorising Officer before processing commences. Where both Part 2 and Part 3 purposes arise, the deployment documentation will identify how the respective processing activities are separated and governed.

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

For clarity, biometric data is processed by the LFR system for the purpose of uniquely identifying individuals. Criminal conviction, offence or criminality information

may be relevant to watchlist eligibility where it is necessary to identify individuals wanted in connection with immigration-related criminal offences or other authorised enforcement purposes.

Such information may also be visible to IE officers through existing Home Office caseworking systems during follow-up checks, for example where ATLAS special conditions include criminality markers. The LFR hardware and software do not process full criminal records as part of the biometric matching process. Any offence-related information included in the approved watchlist extract will be limited to what is necessary and proportionate to support officer review and must be authorised as part of the deployment governance process.

Health data may be visible to IE officers only through existing Home Office caseworking systems during follow-up checks, for example where ATLAS special conditions include vulnerability or health markers.

Individuals with a facial difference, disfigurement, injury, medical condition or other visible facial characteristic may be affected differently by facial recognition processing. This is recognised as a fairness and equality consideration and will be addressed through trained human review, officer discretion, reasonable adjustments where required, and monitoring of outcomes.

Religious or philosophical belief data is not used as a criterion for watchlist inclusion or LFR matching. The LFR system does not intentionally process religious belief data. However, some individuals may wear religious or cultural clothing or coverings, including head coverings or face coverings, which may affect image capture or the individual's experience of officer engagement. This is recognised as an equality and fairness consideration and will be mitigated through human review, officer discretion, reasonable adjustments where required, clear public information and monitoring of outcomes.

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.

The primary safeguard is that individuals under the age of 18 will not be included on an IE LFR watchlist.

Although the LFR system may transiently process facial images of children who enter the Zone of Recognition, those images are used only for real-time comparison.

Because individuals under 18 will not be included on the IE LFR watchlist, children are not expected to generate a true watchlist match. Any system alert would still require trained human review before any officer engagement or action.

Images of children, including those aged 13 or under, that do not generate an alert are processed only for real-time comparison, deleted immediately by the LFR system, and are not retained.

Additional safeguards will be applied through the deployment model. LFR deployments will be overt, with clear signage, leaflets and visible uniformed officers available to answer questions.

Where possible and consistent with the operational objective, documentation explaining the purpose, location, timing and safeguards for the deployment will be published in advance.

If a person under 18 is encountered in connection with a subject on the watchlist, officers will follow standard IE protocols for encounters involving minors. Officers will be mindful of the duty under section 55 of the Borders, Citizenship and Immigration Act 2009 to safeguard and promote the welfare of children. Any child-related issues arising during deployment will be recorded and considered as part of the post-deployment review.

Any learning relating to the incidental processing of children's images or engagement with children during deployment will be captured through the deployment review process and used to inform future authorisations, signage, briefing and operational safeguards.

Where operationally possible, camera positioning and zone design will seek to minimise the unnecessary capture of children.

2.6 Will data subjects be informed of the processing?

☒ Yes

☐ No

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

Not applicable.

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, LFR-specific notification will be provided for deployments. IE will ensure that:
- LFR deployments are, where possible without undermining the objectives of the deployment, notified to the public in advance using the Home Office website. Notifications will explain the purpose of the deployment.
- Signage advising the use of LFR will be placed before the entrance to the Zone of Recognition and will be clear, visible and appropriately sized.
- Deployment notifications will be published on GOV.UK in line with the IE LFR Policy, where this will not have a detrimental effect on the deployment objectives.
- Officers supporting the LFR deployment will wear IE-branded uniform and remain visible to members of the public to support engagement.
- Leaflets and supporting literature will be made available to explain the purpose of the deployment, how LFR works, the safeguards in place and how individuals can exercise relevant rights.
- In line with Home Office practice, and dependent on location, signage and leaflets will be provided in Welsh where required and in English, and will be consistent with NPCC LFR materials.
- A uniformed officer will be available to answer questions for the duration of the deployment. Officers will have access to interpretation services if required.
- Literature will be prepared for persons who may be engaged following an alert, including information consistent with the relevant privacy notice.

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

Access to biometric data and watchlist images is tightly controlled. The generation of the watchlist is restricted to specific staff who, on clear instruction from the approved governance process, will extract the watchlist data and associated images for controlled transfer to the deployment location. The rationale, proportionality, legality and necessity of the watchlist are determined by the Authorising Officer, who must approve its use before the watchlist is created. Processing activities to generate the offline watchlist are covered under the linked Facial Recognition Watchlist Generator DPIA.

The finalised offline watchlist will be stored and transferred using approved secure methods, including encrypted storage media where required. Access to the watchlist and associated biometric templates will be restricted to authorised personnel and recorded in the deployment data management plan.

Once imported, the watchlist and associated biometric templates will only be accessible to authorised LFR operators, ensuring access is limited to trained personnel with a need to know. IE will provide Authorising Officers to ensure correct deployment and use of the system. Authorising Officers will be trained to support operators and Home Office personnel in responding to alerts.

All Home Office personnel working on the deployment will be security cleared to the appropriate level for their role, typically SC.

Access will be limited to trained and authorised personnel with a need to know for the specific deployment. This may include Home Office staff responsible for generating and transferring the approved watchlist, the Authorising Officer and staff supporting deployment governance, authorised LFR operators, frontline Home Office and IE officers responsible for engagement following an alert, police operators or police support staff where the deployment uses police capability or is a joint deployment, supplier or technical support staff only where access is necessary, authorised, recorded and governed by a legally binding contract or equivalent written agreement, and information security, audit or assurance staff where required for oversight, incident response or compliance review.

2.8a. How will access be controlled?

Systems and controls

System/Data	Who has access	How is it controlled
Immigration System Data	Immigration Enforcement and Home Office colleagues via role-specific profiles.	Individual password protected user profile dependent on role
Home Office Supplied Laptop	User assigned at distribution.	Enterprise secured data network BitLocker 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

The LFR watchlist is generated from Home Office systems into a file held on secure Home Office systems. The watchlist will be transferred from a Home Office device in a secure building to approved encrypted storage media to enable transfer to the LFR system. If an alert is generated, any associated data held within the LFR system will be retained only in accordance with the deployment data management plan and applicable retention period.

Cameras will be used only to operate the LFR system and not for general CCTV purposes. No camera footage will be retained by IE following the deployment. If any footage is generated during the deployment in error, this will be deleted by the LFR operators as soon as practicable and in any case within 24 hours.

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

2.9 Where will the data be stored?

The offline watchlist will be created and stored within secure Home Office systems before deployment. For deployment, the approved watchlist will be transferred using approved secure methods, including encrypted storage media where required, and uploaded to the standalone LFR system.

During deployment, the LFR system processes live camera images within the authorised Zone of Recognition. Non-match images and biometric templates are deleted immediately and are not retained. Watchlist data and associated biometric templates are retained within the LFR system only for the authorised deployment period and are deleted from the LFR system and transfer media as soon as practicable after each deployment day, and in any event within 24 hours.

Images and biometric templates that do not generate an alert are deleted immediately and are not retained

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

Not applicable.

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.

The data used to create the offline watchlist will be drawn from Home Office systems as close as practicable to the LFR deployment. This data will be used only for the purpose and duration of the authorised deployment and will be deleted in accordance with the deployment data management plan.

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

Data subject rights will be supported through the underlying Home Office source systems and any operational records where personal data is retained. Requests will be assessed on a case-by-case basis. Where images or biometric templates relate to non-matches and have been immediately deleted by the LFR system, there may be no retained data against which some rights can practically be exercised.

Cameras will be used only to operate the LFR system and not for general CCTV purposes. No camera footage will be retained by IE following the deployment. If any footage is generated during the deployment in error, this will be deleted by the LFR operators as soon as practicable and in any case within 24 hours.

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

There is no operational need to retain match data within the LFR system once it has been reviewed by the operator and any required report has been transferred in accordance with the data management plan. Watchlist images uploaded to the system, and any data transferred using encrypted USB storage, are deleted from the

LFR system and transfer media within 24 hours of the conclusion of each deployment day.

Where a deployment continues over more than one day, the watchlist will be deleted and refreshed before use the following day. Any material change to the watchlist during an authorised deployment will require appropriate governance, authorisation and documentation before use. 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

The LFR system and associated deployment data management process will maintain records of key processing events, including upload of watchlist data, operator access, alert review, export or transfer of any match report, deletion of data from the LFR system and deletion of data from transfer media. Where any element is not automatically logged by the system, a manual deployment log will be maintained. The deployment log will be retained and reviewed in accordance with the data management plan and post-deployment review process.

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

Not applicable.

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

Watchlist inclusion criteria will identify the category of individual and the lawful purpose for inclusion. Deployment documentation will record whether the individual is included for administrative immigration purposes, law enforcement purposes, or another authorised enforcement purpose. Where information is derived from Home Office systems, officers will distinguish between verified factual information, case markers, allegations, intelligence and operational assessments in line with existing system rules, operational procedures and the applicable Part 2 or Part 3 processing regime.

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

Not applicable.

2.14 What is the retention period for the data?

A deployment may be authorised for up to 28 continuous days, subject to the necessity and proportionality assessment, operational requirement and any conditions set by the Authorising Officer. The LFR technology captures images of individuals entering the Zone of Recognition. It compares these images to a deployment-specific watchlist and triggers match alerts for operator review.

- Any images captured by the cameras and processed by the LFR system that do not generate an alert will be automatically deleted from the LFR system
- 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.

Where a deployment operates over extended periods, watchlist data held within the LFR system will be deleted as soon as practicable following the end of each deployment day and, in any case, within 24 hours. Where the same authorised deployment continues, the same updated approved watchlist may be re-uploaded before the next day's operation. Any material change to the watchlist during an authorised deployment will require appropriate governance, authorisation and documentation before use.

Where the LFR system generates an alert, any associated data required for operational, evidential, audit or performance review purposes will be transferred in accordance with the deployment data management plan and retained under the applicable retention schedule. Any remaining alert data held within the LFR system will be deleted within 24 hours of the completion of the relevant deployment day. Where false alert data is required for performance analysis, IE will retain only the minimum data necessary. Wherever possible, data used for performance analysis will be anonymised or aggregated so that individuals are not identifiable. If any personal data is retained for performance review, it will be subject to an identified retention period, access controls and deletion process.

At the conclusion of the deployment, any match report required by IE will be transferred using approved secure methods in accordance with the deployment data management plan. Positive matches, false positive matches, possible matches, false alerts and confirmed false alerts will be deleted from the LFR system within 24 hours of the completion of the relevant deployment day unless a shorter deletion period applies.

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

The LFR system will process images captured of individuals entering the Zone of Recognition, including members of the public who are not included on the deployment watchlist. Images that do not generate an alert are deleted immediately and no personal data relating to non-alerts is retained.

Deletion will be carried out in accordance with the deployment data management plan. The LFR operator or other named responsible officer will delete watchlist data, biometric templates, non-required alert data and data held on transfer media within the required timescales. Completion of deletion will be recorded in the deployment log. The deployment log will record the date and time of deletion, the person completing the deletion, the system or media deleted from, and any issues identified. The Authorising Officer or nominated deployment lead will confirm that deletion has been completed as part of the post-deployment review.

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

Where data is physically transferred outside secure Home Office systems, this will be done only where necessary for an authorised deployment and in accordance with the deployment data management plan. Transfers will use approved encrypted media or other approved secure transfer methods, with named personnel, recorded handling, secure storage and deletion controls. Where data is transferred to or accessed through police-provided LFR capability, the transfer method, access arrangements, controller/processor roles, retention requirements and deletion process will be set out in the deployment-specific data sharing agreement or equivalent written arrangement before processing begins.

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 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
--	--	--	---------------------------------

Where encrypted USB media is used, offline watchlist data will be transferred using an approved encrypted device and manually uploaded to the LFR system. The data transfer process for this model 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 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:
 - Personnel handling the data
 - Dates and times of transfers
 - Deletion records
 - Secure storage records

All deployment data held within the LFR system and transfer media will be deleted in accordance with the deployment data management plan. Any match report transferred to an approved Home Office or partner system will be retained only under the applicable retention schedule.

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

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.

A named SPOC will be identified for the receipt, handling and return or deletion of any transferred data. Where encrypted USB media is used, the device will meet Home Office encryption requirements, be stored in an access-controlled safe or lockbox, and be signed in and out by authorised personnel only.

Regarding the physical USB devices, the following controls have been discussed and approved by Information Security for the deployment of LFR:

- The Watch List USB stick devices are encrypted in line with HO requirements.
- The Watch List USB stick will be stored in an access-controlled safe with a sign-in sheet;
 - Operator signs out USB stick from secured safe
 - Operator downloads the watchlist to the USB
 - Operator uploads the watchlist to LFR system
 - The operator then wipes the watchlist from the USB device.
 - Operator puts USB back in a HO Secured safe.
- Devices must have watchlists deleted at the end of deployment (either before leaving the deployment, or when back at base).
- Devices will be forensically wiped once retired from use to prevent any data loss.

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 of individuals entering the Zone of Recognition, including members of the public who are not included on the deployment watchlist. Images that do not result in a match are deleted immediately and no personal data relating to non-matches 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.

The purpose is to improve IE's ability to identify individuals who may otherwise be difficult to locate or recognise through conventional checks alone, while reducing unnecessary interventions against people who are not on the watchlist.

IE uses Live Facial Recognition (LFR) to support lawful immigration enforcement by helping officers identify individuals who are lawfully sought for a defined and active enforcement purpose in public operational settings.

LFR operates by capturing live facial images within an authorised Zone of Recognition, creating biometric templates, and comparing them against a strictly defined, deployment-specific watchlist. The system generates alerts only; it does not make decisions about identity, immigration status, arrest, detention, removal or any other legal outcome. All alerts are reviewed by trained officers or operators, and any engagement or enforcement action is based on further human checks and the exercise of lawful powers.

LFR is used only where it is assessed as necessary and proportionate for the specific deployment. Less intrusive alternatives, such as database checks, intelligence-led tasking, visits to known addresses, surveillance or warrants, must be considered. LFR may be justified where those alternatives are unlikely to be effective within a reasonable timeframe or would create greater overall intrusion, including repeated interventions at residential premises or disproportionate impact on uninvolved third parties.

Each deployment must be authorised in advance by a senior Authorising Officer and must be limited to the approved purpose, location, duration and watchlist. Deployments are overt, time-limited, subject to transparency measures, and may last for up to 28 continuous days where justified by the operational requirement and authorisation.

This DPIA covers the LFR hardware and software and the associated deployment processing. Where processing is for law enforcement purposes within section 31 of the Data Protection Act 2018, Part 3 of the DPA applies, including the sensitive processing requirements for biometric data used to uniquely identify individuals. Where processing supports administrative or civil immigration functions, Part 2 of the DPA and UK GDPR may apply.

A deployment regime determination record will be completed for every deployment and approved by the Authorising Officer before processing commences. Where both Part 2 and Part 3 purposes arise, the deployment documentation will identify how the respective processing activities are separated and governed.

Watchlists and data sharing

Watchlists are deployment-specific, time-limited and purpose-specific. Individuals are included only where they meet the eligibility criteria in the IE LFR Policy and the defined enforcement purpose for the deployment. Watchlists are not compiled for general intelligence gathering, speculative risk assessment or exploratory monitoring.

For joint deployments, any sharing of watchlist data with police forces, or receipt of watchlist data from police forces where relevant, will be governed by a deployment-specific data sharing arrangement. This will set out the purpose, lawful basis, controller or processor roles, watchlist criteria, security arrangements, retention and deletion requirements, audit arrangements, data subject rights handling, and incident management responsibilities.

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

General processing (UK GDPR/Part 2 DPA) ☒ - go to question 3.2.a.

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

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

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

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

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

- Consent ☐
- Necessary for a law enforcement purpose ☒

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

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

Common law (list HO function/objective below) ☐

Click or tap here to enter text.

Royal Prerogative (HMPO only) ☐

Explicit statute/power (list statute below) ☐

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 Borders 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 Criminal 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.

Paragraph 17, Schedule 2 – Immigration Act 1971

17(1) A person liable to be detained under paragraph 16 above may be arrested without warrant by a constable or by an immigration officer.

17(2) If—

(a) a justice of the peace is by written information on oath satisfied that there is reasonable ground for suspecting that a person liable to be arrested under this paragraph is to be found on any premises; or

(b) in Scotland, a sheriff, or a magistrate or justice of the peace having jurisdiction in the place where the premises are situated is by evidence on oath so satisfied, he may grant a warrant authorising any constable acting for the police area in which the premises are situated (or, in Northern Ireland, any constable), at any time or times within one month from the date of the warrant, to enter, if need be by force, the premises named in the warrant for the purpose of searching for and arresting that person

Paragraph 16 of Schedule 2 to the Immigration Act 1971 provides the statutory power to detain individuals liable to examination or removal, forming the legal basis upon which arrest and entry powers under paragraph 17 may subsequently be exercised.

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 force 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.

The exercise of these powers is subject to compliance with Article 8 ECHR and the requirements of strict necessity and proportionality, including consideration of whether less intrusive means could reasonably achieve the same purpose.

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 individuals of interest prior to removal and for other defined circumstances, and which allow their use for immigration and law enforcement purposes (under Regulation 4).

The LFR Policy document and SOP 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

LFR technology will enhance the capabilities of Immigration Enforcement, 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 IE LFR Operators during deployment. Operators will review alerts and decide whether any further action is required. If the operator assesses an alert as a possible match suitable for referral, they will pass the relevant information to IE officers for further checks and any appropriate engagement. IE officers will then undertake any necessary checks to establish identity, nationality and immigration status before any decision or action is taken. In this way, the LFR system assists IE to make identifications and does not operate as an autonomous decision-making process.

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.

Authorising Officers are responsible for providing senior, independent scrutiny of each proposed LFR deployment before it takes place. Their role is to review and approve the deployment rationale, including the necessity and proportionality case, the defined operational purpose, the location, duration, watchlist criteria, legal basis, data protection considerations, and the safeguards that will apply. The Authorising Officer must be satisfied that the deployment is lawful, necessary and proportionate, that less intrusive alternatives have been considered, and that the proposed use of LFR is consistent with the IE LFR Policy, SOP and any relevant data sharing or deployment documentation. Authorising Officers also ensure that deployments are properly recorded, that any conditions or limitations on the authority are clear, and that post-deployment review, audit and learning are completed.

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?**

During the initial proof-of-concept activity, approximately 7,500 faces were scanned, averaging around 1,250 per deployment day. The programme has now moved into formal delivery and IE plans to deploy LFR regularly throughout the year, subject to enforcement need, authorisation and deployment-specific necessity and proportionality assessments. Deployment volumes are expected to be approximately two to three times per week, with a projected watchlist containing between 6,000 and 15,000 entries. These figures will be kept under review and updated as further operational deployments are completed.

The size of any watchlist will be determined by operational necessity and may be significantly lower than the upper projected limit depending upon the deployment objective

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

IE intend to use LFR technology regularly to enhance the capabilities to supplement existing operational activity, to identify those stated in the watchlist. In addition to assisting with the delivery of IE's key operational aims.

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 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:

Summary of third-party roles

Policing partners may act as joint controllers where they jointly determine the purpose and means of an LFR deployment with IE. The LFR technology supplier is separate from that arrangement and acts only as a processor, or sub-processor where applicable, when providing software, technical capability or support services under contractual controls.

LFR technology supplier

The LFR technology supplier provides the software and associated technical support used by IE to support image processing during authorised deployments. The supplier does not determine the purpose of the deployment, the watchlist criteria, the deployment location, the operational response to alerts or any enforcement decision. Those matters remain for IE and, where relevant, any policing partner under the applicable deployment documentation.

Where supplier access to personal data is required for maintenance, support, troubleshooting, testing or assurance, the supplier will act as a processor, or sub-processor where applicable, under contractual controls. Any such access will be authorised in advance, limited to what is necessary, time-bound, recorded and subject to confidentiality, security, audit, incident reporting, retention and deletion requirements.

System access and security controls

The LFR software operates as a standalone, non-networked deployment system and is subject to security controls. Access to the system, watchlist upload functions and any visible watchlist data is restricted to trained and authorised personnel with a need to know. The supplier is not expected to have routine access to live deployment data, watchlist data, biometric templates, match alerts or retained deployment records.

Potential joint-controller arrangements with police

Where an LFR deployment involves IE and a police force, personal data may be processed jointly where both parties determine the purpose and means of the processing. This may include circumstances where IE provides or shares a deployment-specific watchlist and the police provide or operate the LFR technical capability, including hardware, software, cameras, vehicles, trained operators or supporting infrastructure.

Where IE shares a watchlist with police and the police provide or operate the LFR capability for a deployment, the arrangement will be treated as potential joint-controller processing unless the deployment documentation clearly demonstrates that one party is acting only as a processor or technical provider.

The respective roles and responsibilities will be confirmed in advance through a deployment-specific data sharing agreement covering processing under Part 2 and/or Part 3 of the Data Protection Act 2018, as applicable to the purpose of the deployment. The agreement will set out the lawful basis, purpose of sharing, watchlist criteria, controller, joint controller or processor roles, access controls, security arrangements, retention and deletion requirements, audit arrangements, data subject rights handling, incident management and post-deployment review. Where both parties jointly determine the purposes and means of processing, the agreement will record the parties as joint controllers. Where one party only provides technical capability or operational support without determining the purposes and means of processing, the agreement or deployment documentation will record that party's role as processor, sub-processor or technical provider, as appropriate.

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.

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 system processes biometric data automatically to generate similarity scores and alerts against a defined, deployment-specific watchlist. It does not make decisions about identity, immigration status, arrest, detention, removal or any other legal outcome. All alerts are subject to trained human review and secondary verification before any engagement or enforcement action is considered.

Where an alert is assessed as a possible match, IE officers must undertake further checks, which may include engagement with the individual, checks against Home Office systems, identity information and, where required, biometric checks such as fingerprints. Any legal or similarly significant effect arises only from subsequent human decision-making and the exercise of lawful powers.

Profiling is marked "yes" because LFR automatically compares biometric characteristics to identify whether a person may correspond to a watchlist entry. The

risk of adverse impact is mitigated through strict watchlist criteria, senior authorisation, threshold controls, data-quality checks, trained human review, secondary verification, immediate deletion of non-alert data, audit and post-deployment review.

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 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.

Trained IE officers/operators will operate and manage the LFR system, provided by an approved supplier, verified by HO Biometrics, and referenced within the NPL report titled Facial Recognition Technology in Law Enforcement Equitability Study.

In all cases IE will deploy trained officers/operators 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

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
- Equality and Human Rights Commission
- National Police Chiefs' 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.

This is an ongoing responsibility and further engagement will be held as we move into a more formal programme phase.

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: TBC

Grade:
Organisation:
Contact email:

Name:
Grade:
Organisation:
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) ☒

Immigration Enforcement (IE) is a statutory public authority whose functions derive from the Immigration Acts. The use of Live Facial Recognition (LFR) technology is undertaken in support of those statutory public task functions and is not reliant on common law as a source of power. However, the exercise of those functions is constrained by established common law, public law principles, including legality, necessity, rationality, and proportionality, and must be compatible with Article 8 ECHR as given effect by the Human Rights Act 1998.

The deployment of LFR involves the processing of biometric data and engages the right to respect for private life. Accordingly, LFR use must pursue a legitimate aim, be necessary and proportionate, and be carried out within a clear and foreseeable legal framework, with defined purposes, limited discretion, meaningful human oversight, and robust safeguards.

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 Borders 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 Criminal

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.

Personal data processing is carried out under the **Data Protection Act 2018**. Where IE acts for general immigration functions, processing is undertaken under **Part 2 (UK GDPR)** on the basis of a public task. Where processing supports law-enforcement purposes, including joint working with police, **Part 3** applies. Information sharing with police forces is limited to what is strictly necessary for the stated purpose, is proportionate, and is subject to documented governance, retention, and audit arrangements.

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**

When deploying LFR, data is uploaded to the system for the purpose of the deployment. This system is standalone and there is no off-site data processing and upon completion of the tasks, the LFR system will be wiped as soon as practicable and in any event within 24 hours

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 deployment. All watchlist data held within the LFR system will be deleted as soon as practicable and in any event within 24 hours. 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 immediately and no personal data 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

Data sharing agreements with policing partners expressly cover processing under both Part 2 and Part 3 of the Data Protection Act 2018, where applicable. The agreements should confirm the respective controller, joint controller or processor roles for each deployment, including where IE shares watchlist data and/or where police provide LFR hardware, software, operators or technical capability. They should also set out the lawful basis, purpose, watchlist criteria, security arrangements, retention/deletion requirements, audit arrangements, data subject rights handling and incident management responsibilities. (To be finalised)

The supplier provides software and technical support services and will only act as a processor where access to personal data is required. If supplier access to personal data is required for maintenance, support, troubleshooting, testing or assurance, this will be limited to what is necessary, authorised in advance, recorded, and governed by a legally binding contract or equivalent written agreement. Further detail is provided in response to Q4.7a and Section 5 of this DPIA.

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.

tbc

There is an overarching MoU between Policing and the Home Office in regards to data sharing.

Compliance will be assured through a combination of contractual controls, deployment-specific data sharing arrangements, operational governance and post-deployment review. Any external party involved in an IE LFR deployment, including a police force or technical supplier, will have its role and responsibilities confirmed before processing begins. This will include whether the party is acting as a controller, joint controller, processor or providing limited technical support.

Where IE shares or receives personal data for a joint deployment, a deployment-specific data sharing agreement or equivalent written arrangement will be in place. This will set out the purpose of the sharing, lawful basis, controller/processor responsibilities, permitted use of the data, access controls, security requirements, retention and deletion periods, audit arrangements, data subject rights handling, and incident or breach reporting requirements.

External parties will only receive or access the minimum personal data necessary for the authorised deployment. Watchlists will be deployment-

specific, time-limited and purpose-specific. Data will be transferred using approved secure methods, including encrypted media where required, and access will be limited to trained and authorised personnel with a need to know.

Compliance will be monitored through deployment records, data movement logs, deletion records, post-deployment review, audit where required, and escalation of any incident, breach or non-compliance through Home Office information assurance, data protection and operational governance routes. Supplier access to personal data is not expected routinely; if required for support or maintenance, it must be authorised in advance, recorded, limited to what is necessary, and governed by a legally binding contract or equivalent written agreement.

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.

Yes. The relevant third party/processor arrangement is the LFR technology supplier, which provides the LFR software and, where required, limited technical support services under a Home Office contract. The supplier does not have routine direct access to Home Office data processed during deployments, including watchlist data, biometric templates, live deployment data, alert data or retained deployment records.

Where supplier access to Home Office personal data is required for maintenance, support, troubleshooting, testing or assurance, access will be authorised in advance, limited to what is necessary, time-bound, recorded and subject to contractual data protection clauses consistent with UK GDPR and the Data Protection Act 2018. The supplier may only process Home Office data on documented Home Office instructions and within the agreed contractual scope. The identity of the LFR technology supplier, its role as processor or sub-processor as applicable, the nature and purpose of any processing, permitted access, security requirements, confidentiality obligations, restrictions on onward sharing or sub-processing, audit arrangements, breach reporting requirements, retention and deletion requirements, and arrangements for return or secure destruction of data will be included in the relevant formal written arrangement between the Home Office and the receiving or processing organisation.

For joint deployments with UK police forces, the deployment-specific DSA, MoU, operational agreement or processor clauses will confirm the controller/processor roles, lawful basis, data flows, access arrangements, security controls, retention and deletion responsibilities, and any permitted processor or sub-processor involvement before processing begins. No onward sharing of Home Office data with any third party or processor will be permitted unless it is necessary for the authorised deployment and expressly documented in the relevant written arrangement.

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

This is limited to anonymised/aggregated deployment assurance and performance analysis.

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:

- Usability testing
- Performance testing
- Functional testing
- 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

Yes, but only where necessary for an authorised deployment. The offline watchlist may be transferred from secure Home Office systems to approved encrypted media and uploaded to the standalone LFR system at the deployment location. The data will not be stored in cloud or off-site supplier systems as part of live deployment processing. It will be held only for the authorised deployment period and deleted in accordance with the deployment data management plan.

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

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)
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
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

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)
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.	High	Low	16
15. Chain of custody risks during manual movement of removable media.	High	Low	16
16. Risk of operators not strictly following HO deletion protocols.	High	Low	16
17. Inconsistent operator training between IE LFR teams.	Medium	Medium	14
18. Out of date intelligence feeding watchlist composition.	High	Low	16

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)
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
21. 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 (<i>Eliminated reduced accepted</i>)	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	Reduced	12	
2	Manual dip sampling of 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	
5	Central IE governance for any future deployments; strict scope control.	Reduced	10	

Risk	Options to reduce or eliminate risk	Effect on risk (<i>Eliminated reduced accepted</i>)	Residual risk severity Score (Green/ amber/ red/ purple/1-25)	Measure approved (Yes/no)
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 LFR systems.	Reduced	10	
9	BitLocker encryption on LFR enabled 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 (<i>Eliminated reduced accepted</i>)	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 Authorising Officer.	Reduced	10	
14	Reinforce IE 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	Daily AO confirmation of deletion events. All operators are trained to the same standard.	Reduced	11	
17	Standardised operator and AO training package across all IE LFR operators.	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	

Risk	Options to reduce or eliminate risk	Effect on risk (<i>Eliminated reduced accepted</i>)	Residual risk severity Score (Green/ amber/ red/ purple/1-25)	Measure approved (Yes/no)
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	
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
Stop: Prevent people from entering the UK illegally, ensure compliance and disrupt the organised crime groups	Increased public confidence that individuals who are subject to Deportation Orders or who pose a known risk are less able to re-enter the UK via the Common Travel Area. Minimal impact on the vast majority of passengers, whose data is immediately deleted where no match occurs.	Enables enhanced, targeted checks at CTA-linked ports, supporting the identification of individuals seeking to re-enter the UK unlawfully. LFR acts as a precision capability that strengthens border security and has a potential deterrent effect on opportunistic attempts to circumvent immigration control using false documents or indirect travel routes.
Manage: Identify those in the UK without status, maintain contact with them and bring their cases to conclusion	Reduced disruption to the wider public compared to repeated enforcement visits at residential addresses or workplaces. More timely resolution of immigration cases, increasing fairness and certainty for individuals and communities.	Supports quicker identification and lawful engagement with individuals who are without status and cannot otherwise be located through less intrusive means. Enables more effective re-engagement with immigration casework processes, helping bring longstanding or complex cases to a conclusion.

Home Office Mission	Impact on Public	Benefit
Remove: Remove those with no right to be here, especially high-harm individuals	Reassurance to the public that Immigration Enforcement has effective, proportionate capabilities to locate and deal with individuals who pose higher harm or risk, without resorting to broad or indiscriminate measures.	Enhances IE's ability to identify and locate individuals subject to removal action, including higher-harm cohorts. The visible, overt nature of LFR deployments provides reassurance about enforcement capability while remaining subject to strict safeguards,
Protect: This underpinning mission recognises the vital role IE plays in protecting the UK public and economy, maintaining the integrity of the immigration system, and safeguarding vulnerable individuals	Improved public safety and confidence in the integrity of the immigration system, balanced against privacy protections through immediate deletion of non-matches, overt deployment, and transparency. Protection of vulnerable individuals from repeated or intrusive enforcement activity.	By enabling targeted, intelligence-informed deployments, LFR supports the prevention and detection of immigration-related criminality while minimising unnecessary intrusion. The use of LFR contributes to protecting the public and economy by strengthening system integrity and reducing reliance on more intrusive enforcement measures that can impact third parties and vulnerable individuals.

It is acknowledged that the deployment of Live Facial Recognition (LFR) constitutes an interference with the private life rights of individuals whose facial images are processed, engaging Article 8 of the European Convention on Human Rights. This interference arises from the real-time capture and comparison of facial images in publicly accessible locations. However, the interference is limited in both scope and duration and is mitigated by the operational design of the system, including the immediate and automatic deletion of biometric data relating to individuals who do not generate an alert, and the absence of any retention or onward use of such data.

The interference pursues a **legitimate aim**, namely the prevention and detection of crime, the enforcement of immigration law, and the protection of the integrity of the United Kingdom's border. In particular, intelligence and operational assessments indicate that Common Travel Area (CTA)-linked ports, including locations with direct and indirect connections to the UK, present a heightened risk of individuals seeking to enter in breach of a Deportation Order, contrary to section 24(A1) of the Immigration Act 1971 (as amended by the Nationality and Borders Act 2022), or of individuals who are otherwise sought in connection with immigration-related criminal offences attempting to evade detection.

Live Facial Recognition (LFR) may be deployed in-country only where its use supports a clearly defined and lawful immigration enforcement purpose and where strict safeguards are in place to ensure compliance with data protection and human rights obligations. In-country use of LFR is not routine and is not used for general monitoring, exploratory activity, or broad compliance checks. Its deployment is restricted to specific operational circumstances where individuals are lawfully sought for enforcement or criminal proceedings and cannot reasonably be identified or located through less intrusive means.

All in-country deployments of LFR are subject to senior authorisation, deployment-specific necessity and proportionality assessments, and adherence to the eligibility criteria set out in the Immigration Enforcement LFR Policy. Watchlists are narrowly constructed, time-limited, and purpose-specific, and may only include individuals who fall within defined policy categories and have been approved by an Authorising Officer. Intelligence may inform the location and timing of a deployment but does not, of itself, justify inclusion of individuals on a watchlist.

LFR deployments in-country are conducted overtly and are supported by clear signage, public information, and the presence of trained officers. The technology does not make enforcement decisions: all system alerts are subject to immediate human review and verification, including secondary identity checks, before any engagement or action is taken. Biometric data relating to individuals who do not generate an alert is automatically and immediately deleted, and data relating to alerts is retained only for the minimum period necessary in accordance with approved retention schedules.

In-country use of LFR is subject to ongoing oversight, audit, and post-deployment review to ensure that safeguards remain effective and that the use of the technology continues to be necessary and proportionate in the specific operational context. Where these safeguards cannot be met, or where the enforcement objective can reasonably be achieved by less intrusive means, LFR will not be deployed.

The use of LFR in this context is assessed as **necessary** having regard to less intrusive means. Alternative methods of identification and location—such as database checks, intelligence-led tasking, physical surveillance, visits to known addresses, or execution of warrants—have been considered. In the specific operational contexts in which LFR is deployed, these measures are assessed as unlikely to achieve the enforcement objective effectively within a reasonable timeframe, or as likely to result in greater overall intrusion, including repeated interventions at residential premises and disproportionate impact on uninvolved third parties. LFR is therefore deployed only where less intrusive measures are assessed as insufficient to meet the operational need.

The deployment of LFR is further assessed as **proportionate**. Its use is tightly constrained by strict watchlist eligibility criteria, senior pre-authorisation, time-limited deployments, overt operation, human review of all alerts, and robust governance and audit arrangements. LFR does not make enforcement decisions, and the likelihood of erroneous arrest is mitigated by conservative system thresholds, human-in-the-loop verification, and secondary identity checks prior to any action being taken.

In these circumstances, the interference with Article 8 rights is considered justified and proportionate to the legitimate aims pursued. The deployment of LFR contributes to the effective identification and enforcement action against individuals lawfully sought for immigration-related and criminal matters, supports border security, and does so in a manner designed to minimise intrusion, prevent arbitrary decision-making, and protect the rights and freedoms of the wider public. Further detail on the operational safeguards and justification for LFR use is set out in the Immigration Enforcement LFR Policy and associated documents published on GOV.UK.

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

Section 8

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

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
27/07/2026	Gillian Brinton Nouch	05/08/2026	Review complete however please note that Q5.1 Q5.5 and Q5.6 will need to be update pre deployment if any 3rd parties involved.

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)
Click or tap to enter a date.		Click or tap to enter a date.		

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			