# Data Protection Impact Assessment (DPIA)

| DPIA Information | |
|---|---|
| Name (and or project number) | SxSy-DPIA_LFR_Software:<br>NEC Software Solutions – Neoface Facial Recognition Technology (FRT) |
| Forces involved in Project | Joint |
| Operational Contact | |
| Information Asset Owner | |
| Business Contact | |
| Information Governance Contact | |

| Document Review Information | | | |
|---|---|---|---|
| ***Version History*** | ***Version Date*** | ***Requestor of Change*** | ***Summary of Change(s)*** |
| *1.0* | *24/05/2018* | *Regional Feedback* | *Agreed final version* |
| *2.0* | *02/09/2024* | *Audit Feedback* | *Updates to format* |

**Introduction**

The **Data Protection Impact Assessment (DPIA)** process is an important tool to help you identify and minimise the data protection risks of a project that involves processing personal data.

The DPIA process is relevant to initiatives involving the use of personal data and is particularly important when a new business process or technology initiative involves the collection, recording, sharing or retention of personal data.

The DPIA enables privacy and data protection considerations to be made in the early stages of a project where any identified problems can be easier to resolve rather than late or retrospective consideration where solutions can be more costly or delay implementation. A DPIA, can also identify whether the project should be continued when balanced with the rights and interests of persons affected.

The DPIA process will consider privacy in the way the forces use individual's personal data. This can involve privacy about: the integrity of the individual, the person, their personal information, their personal behaviour and their personal communications.

When carried out early the DPIA process can provide the following benefits:

- identify any privacy or information risks concerning the processing of personal data
- determine any mitigations necessary to bring those risks down to an acceptable level
- provide a record of those mitigations and the decision by Business Lead whether to accept and adopt them
- provide a record of the Data Protection Officer's views on the initiative.

**Who is responsible for carrying out a DPIA?**

The Project Manager will be responsible for ensuring that the DPIA is completed. In the absence of a Project Manager it will be the relevant specified Business Lead. The Information Governance team will assist you and explain how the DPIA should be completed.

**The DPIA will require authorisation by:**

- Information Asset Owner and Senior Responsible Officer
- Information Governance team or the Data Protection Officer
- Senior Information Risk Officer – where the DPIA has identified 'high' residual risks and referral to the Information Commissioner is require

**Freedom of Information Act & Information Security**

This document (including attachments and appendices) may be subject to an FOI request.

In compliance with the Government's Security Policy Framework's (SPF) mandatory requirements, please ensure any onsite printing is supervised, and storage and security of papers are in compliance with the SPF. Dissemination or further distribution of this document is strictly on a need-to-know basis and in compliance with other security controls and legislative obligations.

**Data Protection Impact Assessment Report**

**1. Outline of the project, objectives and benefits**

It has been agreed at a National level that the Live Facial Recognition (LFR) vans will deploy with NeoFace software provided by NEC. This is currently deployed in the vans owned by the Metropolitan Police Service (MPS) and South Wales Police (SWP).

The LFR software 'matches' using an import from a custom Watch List (see Deployments DPIA for further details). The Watch List is made up of biometric templates, this is where the 'facial features' associated with a subject is expressed as numerical values.

NeoFace is the NEC's high performance, highly scalable facial recognition algorithm, providing fast and accurate results for the most demanding real-time or post-event facial recognition use cases. The software performs consistently by combining the best feature-matching and AI technologies. It's built-in safeguards support privacy and proportionate use, with auditing and reporting as well as automatic and manual data retention tools.

NEC's Live Facial Recognition uses real-time video feeds to scan and match faces against a pre-determined police Watch List. This will be standalone software in the vans, it will not be connected or accessible across Force networks nor will any LFR data be processed by the Supplier.

If a match is found, officers receive an instant alert allowing for quick identification of persons of interest while reducing unnecessary interventions. All alerts will be subject to human review prior to any deployment of officers to interact with the data subject, this is not an automated process and all engagements will be risk assessed by the operator.

The NEC NeoFace software has built-in privacy features to enable compliance with the UK data protection laws, including the UK GDPR and the Data Protection Act 2018. It operates under strict legal and ethical guidelines, ensuring necessary and proportionate use supported by Sussex and Surrey operating procedures to ensure safe and ethical deployment of the software.

MPS and SWP tested Facial Recognition Technology (FRT) with the National Physical Laboratory (NPL). The NPL is a world-leading centre of excellence that provides cutting-edge measurement in science, engineering and technology. The aim of the testing was to develop an in-depth understanding of the performance of the algorithms when it was being used in an operational environments. The NPL test plan was specifically designed to help identify any impact this technology may have on any protected characteristics, in particular race, age and sex.

The NPL report gives an impartial, scientifically underpinned and evidence-based analysis of the performance of the facial recognition algorithm currently used by the MPS and SWP. Its findings revealed that there was no demographic performance variation for LFR.

**2. Describe the intended use of personal data:**

Neo Face technology will compare the Watch List to persons passing through a designated area of LFR deployment. The 'SxSy DPIA LFR Deployments' DPIA fully details the restrictions placed on the Watch List and its application for live deployments. Please review this DPIA if more details are needed in relation to this subject matter.

**SxSy DPIA LFR Deployments – DPIA Extracts**:

*The LFR application requires a Watchlist of reference images. These are processed so that the 'facial features' associated with their subjects are extracted and expressed as numerical values (a Biometric Template). The watchlist is then a collection of those biometric templates that are processed during the LFR deployment. Deployments will involve a real time capture of the Biometric Templates of any individuals who cross the path of the camera therefore that particular cross section of the general public will have their image and biometric template data processed (i.e. both personal data (the image) and sensitive/special category data (the biometric template).*

*Categories of data subjects in relation to the watchlist processing could therefore fall under the below categories:*

- *wanted by the courts; and/or*
- *suspected of having committed an offence, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or*
- *subject to bail conditions, court order or other restriction that would be breached if they were at the location at the time of the Deployment; and/or*
- *missing persons deemed increased risk; (subject to specific parameters) ; and/or*
- *presenting a risk of harm to themselves or others.*
- *police orders such as football banning orders, stalking prevention orders- police imposed orders as well as court-imposed orders.*

*The Watchlist is bespoke for every Deployment and the rationale for the make-up of the Watchlist must be intelligence-led, justified, proportionate and necessary, with the nature of the Watchlist recorded prior to each Deployment. The Candidate Images and related Biometric Templates for the watchlist are required to be deleted as soon as possible post Deployment and in any case within 24 hours.*

*The criteria for Watchlist constructs must be approved by the Authorising Officer (the 'AO') and be specific to an operation or to a defined policing objective. The AO will be the rank of Superintendent or above to ensure resilience in deployment of this resource. Full guidance on this process and necessary criteria will be detailed in the SOP.*

*Images are typically imported into the LFR application for each Deployment from local Force systems. Data may also be provided by other police forces and agencies associated with law enforcement and also from the general public. Where police originated images other than custody images are considered for use, consideration regarding the legality and necessity of the inclusion of such images is needed.*

*Non-police originated images should only be included in a Watchlist with the authorisation of the AO. The AO should also consider all the circumstances pertaining to the image and in particular the factors above.*

*The Watchlist is created via a CSV file and corresponding Candidate Images which are saved in a secure folder with the force ICT domain. The content of the folder is extracted into the LFR application prior to Deployment via an encrypted USB drive. This device is plugged into the vans whilst on Police premises, the disk does not leave the police site. This mitigates the concerns for loss.*

*The LFR application will create Biometric Templates of the faces in the Watchlist. This will then use a live camera feed to scan faces of individuals in a designated area creating Biometric Templates of each to compare against those in the Watchlist.*

*The collection of personal information is via CCTV cameras connected to the standalone laptop/server. The laptop is not connected to the force ICT infrastructure and can be considered a 'black box' solution (an independent system to the current technical architecture).*

*The application 'extracts' a face from CCTV footage (known as a Probe Image) creates a Biometric Template and then compares it against a pre-defined Watchlist, every Candidate Image in the Watchlist will also have a Biometric Template created. In doing so, the application does not save the live CCTV feed, only a particular face if a Possible Match is made against a Candidate Image along with a wider CCTV frame from which the Probe Image was extracted.*

With regards the physical USB devices, the below has been discussed and approved by Information Security for the deployment of LFR:

- The Watch List USB stick devices are encrypted with BitLocker;
- The Watch List USB stick will be attached to and stored with van/car keys.
  - Operator downloads the watchlist to the USB
  - Operator uploads the watchlist to the van, on police premises
  - Operator then then wipes the watchlist from the USB
  - Operator puts van keys and USB back on the designated hook back in the FCC
- Stored in access controlled key safe with sign-in sheet;
- Devices must have watchlists deleted at the end of deployment (either before leaving the van, or when back at base).

The NeoFace software in the vans will be standalone, it is not networked to the Force infrastructure or to allow access by the Supplier. NEC do not have remote access to the vans while deployed or back on site. If there are any software / technological concerns then technical support will attend the local Force site.

NEC Software – NPL Testing Summary:

The full results are presented in the National Physical Laboratory (NPL) commissioned report: Facial Recognition Technology in Law Enforcement Equitability Study from March 2023. Relevant extracts to support the deployment of this software have been provided below but it is recommended that whole document is reviewed using the above link prior to DPIA sign off.

The LFR technology tested was NEC HD5 Face Detector. This is the version of algorithm being deployed in the Sussex and Surrey vans, it is also the facial detection and recognition algorithms currently used by MPS and SWP for LFR (these Forces supported the equitability study testing).

The accuracy of LFR is measured in terms of:

- True-Positive Identification Rate (TPIR) – the rate of successful recognition when subjects on the watchlist pass through the zone of recognition
- False-Positive Identification Rate (FPIR) – the rate of incorrect recognition (i.e., false positives or false alerts) when subjects not on the watchlist pass through the zone of recognition.
- TPIR is sometimes referred to as the True Recognition Rate, and FPIR as the False Alert Rate.

To ensure accuracy for multiple Forces, the performance figures were compared for two different watchlist sizes: (i) a watchlist of 10,000 reference images (MPS LFR deployments) and (ii) a watchlist of 1000 reference images (SWP LFR deployments).

Given the observations identified in the report regarding the demographic variation in FPIR, it is recommended that Forces use the face match compliance setting of 0.64 or above to minimise the likelihood of any false positive and adverse impact on equitability. This threshold of 0.64 has been determined by the ACC for Sussex and Surrey, this will form the standard threshold for deployments. There will be flexibility to lower this if specific intelligence is received, in these circumstances a full rationale will be detailed in the LFR Application / Written Authority Document.

The below statistics support the decision to set 0.64 as the default threshold.

At a face-match threshold of 0.64, the software produced no false positives against the watchlist of 178,000 Filler images. At threshold 0.62, two non-mated recognition opportunities (by the same individual) gave a false positive. At threshold 0.60, ten non-mated recognition opportunities generated false positives (increasing to twelve with the revised face detection settings).

| Face-match threshold | Face detection settings | Observed TPIR | Observed FPIR | FPIR anticipated under operational measures: Watchlist 10k | FPIR anticipated under operational measures Watchlist: 1k |
|---|---|---|---|---|---|
| T | | TPIR 178400, 1, T | FPIR 178000, T | FPIR 10000, T | FPIR 1000, T |
| 0.64 | (a) | 79 % | 0.00 % | < 0.004 % | < 0.001 % |
| 0.62 | (a) | 82 % | 0.05 % | < 0.004 % | < 0.001 % |
| 0.60 | (a) | 85 % | 0.25 % | 0.014 % | 0.002 % |

The number of cohort subjects with false positive by gender, ethnicity and age at a face-match threshold of 0.64 identified no false positives. At face-match thresholds of 0.62 and 0.60 the number of subjects with a false positive is small, and a statistically significant imbalance between demographics is not shown.

| Face-match threshold Face-detection settings | FPIR | Female | Male | Asian | Black | White | Age <21 | Age 21-30 | Age 31-42 | Age >42 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0.64 (a) | 0.00 % | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0.62 (a) | 0.05 % | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 0.60 (a) | 0.25 % | 2 | 4 | 2 | 4 | 0 | 0 | 5 | 1 | 0 |

Testing ethnicity and gender at a face-match threshold of 0.64, the ethnicity-gender group with the best TPIR was the Asian-Female group, and the poorest TPIR was for the Black-Female group. However, the observed differences in TPIR by gender, by ethnicity, and by ethnicity & gender combined were not statistically significant at the 0.05 significance level.

In the below table we see that for the size 10,000 (MPS) watchlist at thresholds above 0.64 the extent of demographic variation in FPIR is limited.

**Table 9 – Selectivity and estimated FPIR by probe demographic for notional MPS Watchlist**

| | Asian Female | Asian Male | Black Female | Black Male | White Female | White Male |
|---|---|---|---|---|---|---|
| Face match threshold: 0.66 | 0<br>< 1 in 10,000 | 0<br>< 1 in 10,000 | 0<br>< 1 in 10,000 | 0<br>< 1 in 10,000 | 0<br>< 1 in 10,000 | 0<br>< 1 in 10,000 |
| Face match threshold: 0.64 | 0<br>< 1 in 10,000 | 0<br>< 1 in 10,000 | 0.00003<br>< 1 in 10,000 | 0<br>< 1 in 10,000 | 0<br>< 1 in 10,000 | 0<br>< 1 in 10,000 |
| Face match threshold: 0.62 | 0<br><1 in 10,000 | 0.00011<br>1 in 9,200 | 0.00003<br>< 1 in 10,000 | 0<br><1 in 10,000 | 0<br><1 in 10,000 | 0<br><1 in 10,000 |
| Face match threshold: 0.60 | 0<br><1 in 10,000 | 0.00022<br>1 in 4,600 | 0.00021<br>1 in 4,700 | 0.00023<br>1 in 4300 | 0<br><1 in 10,000 | 0<br><1 in 10,000 |

This is supported in performance changes for the demographic profile and size of the SWP watchlist.

**Table 10 – Selectivity and estimated FPIR by probe demographic for notional SWP Watchlist**

| | Asian Female | Asian Male | Black Female | Black Male | White Female | White Male |
|---|---|---|---|---|---|---|
| Face match threshold: 0.66 | 0<br><1 in 100,000 | 0<br><1 in 100,000 | 0<br><1 in 100,000 | 0<br><1 in 100,000 | 0<br><1 in 100,000 | 0<br><1 in 100,000 |
| Face match threshold: 0.64 | 0<br><1 in 100,000 | 0<br><1 in 100,000 | 0.000000<br><1 in 100,000 | 0<br><1 in 100,000 | 0<br><1 in 100,000 | 0<br><1 in 100,000 |
| Face match threshold: 0.62 | 0<br><1 in 100,000 | 0.000002<br><1 in 100,000 | 0.000000<br><1 in 100,000 | 0<br><1 in 100,000 | 0<br><1 in 100,000 | 0<br><1 in 100,000 |
| Face match threshold: 0.60 | 0<br><1 in 100,000 | 0.000003<br><1 in 100,000 | 0.000002<br><1 in 100,000 | 0.000003<br><1 in 100,000 | 0<br><1 in 100,000 | 0<br><1 in 100,000 |

The NPL test identified the optimum threshold settings at 0.64 which has been adopted by both Forces.

## 3. Consultation:

Whilst Forces have autonomy to determine deployment thresholds (as above), the decisions on software provider and version have determined by the National working group. Therefore there has been limited consultation other than in the National working group to ensure the best most reliable software is deployed. The deployment of NeoFace ensures consistency across policing which is essential to build trust from the public during deployments.

An issue has been raised Nationally regarding the threshold settings for the Police National Database (PND) Retrospective Facial Searches. It is essential to evidence that this does not impact on the NEC software deployed in the LFR vans. The PND is separate to this project and whilst the thresholds for the Facial Searches will cause concern, it is not to be considered for LFR. The threshold issue for PND will be detailed in a separate DPIA – DPIA SQ Facial_Rec_PND_v1.1.

**Data protection compliance – assessment of necessity and proportionality of personal data processing.**

**Principle 1: Use of personal data is fair and lawful:**

a) Lawful basis for the processing of personal data is stated as follows:
Personal and Special category / Sensitive data will be processed under the UK GDPR (High Risk / Vital Interests only in relation to Missing Persons) and Part 3 of the Data Protection Act for a Law Enforcement purpose. In relation to Missing Persons, this will only be in instances where there is a serious perceived threat to life (vital interests) under Article 2 of the European Convention on Human Rights (ECHR).

For this reason, the below list of potential processing covers all potential data processing.

- **Personal Data (Article 6 (1) of the UK GDPR):**
  (e) **Public task**: processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
  (d) **Vital interests**: processing is necessary to protect someone's life.

- **Special Category Data (Article 9 (2) of the UK GDPR) to include Article 10 (Criminal Data):**
  (c) Processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
  (g) processing is necessary for reasons of **substantial public interest** (see below for the conditions), on the basis of Domestic Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The following conditions apply to this processing:
    - Administration of justice and parliamentary purposes
    - Preventing or detecting unlawful acts
    - Safeguarding of children and individuals at risk (as defined at Section 18 of Schedule 1 DPA 2018)

- **Lawful basis for processing sensitive data for law enforcement purposes:**
  Sx/Sy police will process Personal / Sensitive Data under Police's legal functions and where processing is necessary for the performance of a task carried out for that purpose by a competent authority. The images processed through the LFR software are identified as biometric data (sensitive data). The ICO defines this as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm someone's unique identification of that natural person, such as facial images data".

  The definition of a function for 'law enforcement purposes' covers activities that are for the 'purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

  In addition, the police will only process sensitive data under Part 3 of the UK GDPR where the processing is strictly necessary for the law enforcement purpose and the processing meets at least one of the conditions in Schedule 8, Part 3 Data Protection Act 2018 namely:
  - Judicial and statutory purposes/administration of justice; the sensitive processing must be necessary for the administration of justice, or the exercise of a function conferred 'on a person' by enactment. This covers a constable and other competent authorities. In addition, in order to satisfy this condition, you must be able to demonstrate that the processing is necessary for reasons of substantial public interest.
  - Safeguarding of children and of individuals at risk; this condition is met in cases where consent is not appropriate because the individual is under 18 or at risk, but the processing is necessary for reasons of substantial public interest and is to protect them from harm or to protect their well-being.

**Principle 2: Use of personal data is for a specified, explicit and legitimate purpose and not re-used for a purpose that is in-compatible with the original purpose:**
LFR vans will be deployed under UK GDPR for a Public Task and/ or under Part 3 of the Data Protection Act for a Law Enforcement purpose. They are not to be used in the same way as conventional CCTV surveillance. On deployment, a bespoke and approved Watchlist will be created and imported into the vans.

The NEC software will be standalone and not networked. The default 0.64 threshold will not be customisable by operators, this will be an administrative function by pre-determined superuser.

Neither the biometric template (generated from the images on the Police Watchlist) or the images processed through the LFR CCTV will be retained. The biometric template will be deleted within 24 hours of the end of deployment, and it has been confirmed in the 'LFR Deployments DPIA' that no images will be retained within the NEC software. As the biometric template and CCTV feed footage data are not retained, there will be no further processing of this data.

There may instances where retention of data is necessary and required to fulfil legal obligations such as those under CPIA 1996 or Police Conduct Regulations. Given the use of LFR as an intelligence product rather than an evidential one, it is anticipated that the need for such retention will arise rarely.

**Principle 3: Use of personal data is adequate, relevant and no more than necessary:**
NeoFace software will not be networked and any processing will be limited to the stipulations outlined in the LFR Deployments DPIA. This being that CCTV footage will not be saved and will be used for real time identification of nominals only. There will be no further processing of captured data on the NeoFace software.

**Principle 4: Personal data must be accurate and kept up to date:**
For members of the public passing through, the processing will be real time. With regards the watchlist, checks must be made to ensure that the images uploaded to the watchlist are the most recent and up-to-date image of the individual. Watchlists uploaded to NeoFace will not be more than 24 hours old to provide increased assurance that those on the list remain of interest. A new Watchlist is generated for every LFR Deployment.

During the Deployment there will not be any additional identifiers created or attached to the biometric templates of members of the public captured by LFR.

**Principle 5: Personal data must be kept in an identifiable format for no longer than necessary:**

- **Biometric Templates – no matches**
  Any Biometric Templates which do not match those on the Watchlist are automatically deleted immediately following the comparison process.
- **Possible Matches**
  Where there is a Possible Match, this will generate an Alert, which is displayed to the LFR Operator. If a Possible Match is made three thumbnail images will be saved within the LFR application along with the related metadata. The first is the Candidate Image from the watchlist, the second is the face extracted from the CCTV and the third being the CCTV frame from which the Probe Image was extracted. The maximum retention period for Possible Match images and the related Biometric Templates is 24 hours although generally this information is deleted immediately post Deployment finishing.
- **Watchlists and associated metadata**
  Deleted immediately after Deployment or at latest within 24 hours
- **LFR Operator and Engagement logs**
  Retained in line with MOPI retention periods.
- **CCTV Footage**
  CCTV footage generated from LFR Deployments is deleted at the end of the deployment (or within 24 hours where not possible at the end of the deployment), except where retained:
  - in accordance with the UK GDPR, Data Protection Act 2018, MoPI or the Criminal Procedures and Investigations Act 1996;
  - in accordance with Sx / Sy Police's complaints / conduct investigation policies.

**Principle 6: Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction:**

There are two types of access available on NeoFace, 'user' and 'administrator' access levels. All operating staff will all be vetted and cleared to at least MV/SC level. These are fully discussed in the LFR Deployment DPIA and have been signed off by DPO and SIRO.

The use of LFR technologies (NeoFace) is governed by a number of codes of practice including those applying to the police such as PACE. The governance and authority for an LFR Deployment is contained in the LFR Policy. No Deployment is permitted without Superintendent authorisation (this is fully detailed in the SoP) and the criterion for deployment is provided in the Policy. During Deployment command teams are required to monitor and review data processing to ensure that it remains lawful. A post Deployment debrief and review is used to identify lessons for the future and periodic audits will be conducted to provide assurance.

The authorising Superintendent must ensure that all issues have been adequately identified, documented, and mitigated to ensure that the Deployment is not only necessary, but also proportionate to the specified law enforcement purpose.

Following the conclusion of any Deployment the force will apply learning including evidence of effectiveness in similar operational scenarios and to carry it forward to subsequent Deployments to ensure the use of LFR on each successive occasion is truly beneficial, in particular to the public.

Watchlist images are transferred onto the LFR application via a USB using an AES-CBC 256-bit full disk hardware encryption engine that is further protected by pass number access. Access to the USB stick containing the Watchlist is limited to those with a need to use it. Full details of access (update and read only) will be detailed in the LFR Standard Operating Procedures and will be the responsibility of the business leads to ensure compliance.

Despite the encryption on the USB stick, any loss will be processed as a potential data breach using the SABR form. This follows standard Sx / Sy Police processes. However, it is important to note that the encryption and fact that the USB stick will be wiped before leaving police premises. The Watch List USB stick will be attached to and stored with van/car keys.

- Operator downloads the watchlist to the USB
- Operator uploads the watchlist to the van, on police premises
- Operator then then wipes the watchlist from the USB
- Operator puts van keys and USB back on the designated hook back in the FCC

**7. Personal data will be processed in accordance with the individual's data protection rights:**

As this will be an overt tactic and signage deployed, individuals will be able to avoid the area in which the Deployment is located. Each Deployment will have a compelling, legitimate grounds which are documented beforehand.

- Right to be informed – members of the public will be informed prior to a Deployment. Post Deployment and dependent on the passage of time it will depend on whether an individual was identified as a match as to whether this right can be exercised although individuals can be provided with the details of the time, date and location of the Deployment to determine the likelihood that their data was processed. Watchlists could be re-engineered therefore it is possible that individuals on a Watchlist may be able to exercise this right where appropriate.
- Right to rectification – individuals will be able to challenge the processing where a Possible Match has been identified by LFR and the LFR Operator/LFR Engagement Officer.
- Rights of Access – CCTV footage and the Watch List will be manually deleted at the end of the deployment (and in worst case within 24 hours), there is unlikely to be any requests for this data within this period.
- Right to erasure – a request can be submitted where a match has been made and individuals are challenging the outcome. It is acknowledged that this right is not likely to be exercised as personal information relevant to the LFR application is deleted with 24 hours.
- Right to data portability – not applicable.
- Right to object – not applicable under Part 3 DPA 2018. Sx/Sy Police will assess any right to object requests it receives on a case-by-case basis if a request is received and the processing in question does fall under Part 2 of the DPA 2018.
- Right to object to automated decision-making including processing – no automated decision making will be taking place without any human involvement. All decisions will have manual intervention.

**8. Personal data will not be transferred outside the European Economic Area (EEA) without guaranteed adequate privacy protections:**
Data will not be processed outside of the UK.

**9. The force must be able to demonstrate how they are complying with the Data Protection Act 2018 & GDPR:**
Sx/Sy Police has a mature Information Governance Strategy and Structure in place. It incorporates the requirements of the Police to be open and transparent (wherever appropriate and possible) about how data is processed. To this end and having considered the risks to this right posed by the use of LFR, Sx/Sy Police has adopted a number of measures to ensure that the right to be informed is upheld.

A key measure is the publication of Sx/Sy key LFR Documents on the Sx/Sy Police website. Whilst Sx/Sy Police is not required to publish a number of these documents, it has elected to do so. This is an important measure to inform our communities including the public passing an LFR deployment and those who may be placed on a Watchlist to understand the standards Sx/Sy Police, as a public body, operates to. In this way, Sx/Sy Police use of LFR is both foreseeable and assessable. The published documents are detailed in the LFR Deployment DPIA.

## 4. Identifying and assessing risks

The main focus of the risk assessment within the DPIA is to consider the risks to the interests of the individuals whose data will be processed. Risks may also be intangible (significant social or economic disadvantage) such as the risk of losing public trust. The identified risks are listed below and scored using a standardised risk assessment matrix. The listed 'agreed actions' have been identified as a way to either **reduce or eliminate** risks identified as **medium or high**. Agreed measures will be factored into implementation plans and will be the responsibility of either the Project Manager or Information Asset Owner to ensure they are completed.

| | **Describe the source of the risk, the problem it creates and the potential impact on individuals.** | **Likelihood** | **Severity** | **Risk** | **Agreed action** | **Action Owner** | **Risk score** |
|---|---|---|---|---|---|---|---|
| 1 | As a result of limited availability of images for testing the software there is a risk that bias may not be sufficiently eliminated in the algorithm deployed resulting in a disproportionate number of individuals with protected characteristics being identified in False Alerts leading to potential legal challenge, financial claims and an increase in complaints. | Remote | Significant | Medium | Assurances around the testing conducted by the software supplier are required in the contract and will be continually monitored to ensure that any potential bias in the use or development of the technology is identified and rectified Watchlists will also be checked to ensure that gender or ethnicity is not unfairly represented. Equality Impact Assessments will be completed and regularly reviewed against legal developments and deployment outcomes. The force will monitor performance in this regard and having ongoing obligation to consider whether other algorithms should be used instead.<br>**Progress Update:**<br>Despite the confirmation of a 0.64 threshold, there is always the risk that the deployment could identify a false match which leads to a wrongful arrest. This will continue to be monitored across all deployments and also at briefings. | IAO / IAA | Medium |
| 2 | Consideration needs to be recorded in relation to software version updates and assurances that they are tested by the NPL prior to any upload onto Police LFR systems. | Possible | Significant | Medium | This will need to be monitored locally and nationally to ensure any new versions of the software area properly tested to ensure there is no organisational damage if the thresholds are not functioning.<br>**Progress Update:**<br>This will need to be continually monitored by the IAO / IAA and ensure testing has been completed before any upload to our systems. | IAO / IAA | Medium |

**6. Information Management – Comments**

Whilst this DPIA is focused on the deployment of the NeoFace software, it is essential to include and reference decisions agreed in the Deployments DPIA to ensure consistency across our use of this software. Whilst there was little consultation with Sussex / Surrey over the supplier, this decision was essential at a National level to ensure a consistency of processing across all Forces LFR deployments. This offers stronger reassurances to the Police Forces and to members of the public with regards the processing of their biometric data and any actions the Police take.

It has been confirmed that the software is stand alone and no access is granted to the supplier. This ensures compliance with LFR deployment documentation and also reinforces the protection of data for the public. It has also been agreed that the CCTV footage processed through the software will be real time only and will not be retained and re-purposed by Sussex or Surrey Police.

Concerns have been raised regarding software version control, as in this is already 2 years old and V5 updates must be tested by the NPL prior to any installation, including testing as a pilot Force. It is recommended that Sussex and Surrey should not engage with the software until it is tried and tested as it could lead to false hits and irreparable damage to the reputation of LFR deployment.

Based on the NPL testing, it has been agreed that Sussex and Surrey will only apply the 0.64 threshold unless there is an operational requirement / justification for a targeted deployment. I agree this is the best option and fully support this from a governance compliance.

| Threshold Setting | Observed True Positive Identification Rate (TPIR) | Observed False Positive Identification Rate (FPIR) | Anticipated FPIR with Watchlist 10k | Anticipated FPIR with Watchlist 1k |
|---|---|---|---|---|
| 0.64 | 79% | 0.00% | < 0.004% | < 0.001% |
| 0.62 | 82% | 0.05% | < 0.004% | < 0.001% |
| 0.60 | 85% | 0.25% | 0.014% | 0.002% |

| 7. Authorisation of DPIA: |
|---|

DPIA will be retained by the Information Governance team. This will be reviewed by the parties listed below with consideration then given for signatory by the Senior Information Risk Owner (SIRO), Senior Responsible Officer (SRO) and Information Commissioners Office (ICO) if required.

| | Name | Date |
|---|---|---|
| **Force Lead** | | *19/09/2025* |
| **Force Lead** | | *22/09/2025* |
| **Project Lead** | | *19/09/2025* |
| **Information Management Sussex** | | *19/09/2025* |
| **Data Protection Officer Sussex** | | *22/09/2025* |
| **Summary of DPO advice:** | *This DPIA is specific to the deployment of NeoFace software as the nationally preferred option to enable Live Facial Recognition. General principles governing LFR have previous been addressed in an overarching DPIA on LRF deployment which has been reviewed and approved by me and my Surrey Police counterpart.*<br><br>*Initial iterations of this document placed a degree of reliance on testing carried out by an American Federal Agency which is not subject to UK/ EU DP standards. These references have been removed, and clarity offered that risk is assessed based on the findings of the UK National Physical Laboratory.*<br><br>*It is imperative that the Forces recognise that this software has not eliminated bias. Instead, software settings have been agreed which balance a reasonable degree of reliability against operation effectiveness. Whilst this is a nationally agreed position approved by the NPCC lead, it is imperative that the Forces remain aware and continue to review impact. Processes built into the SoPs minimise high-impact error by removing automated decision-making; any arrest will always be based on a human decision following further checks. Nonetheless, I would advocate periodic reporting back to the Ethics Committee. It is also imperative that an EIA is submitted; I am not sighted on that document at present.*<br><br>*It is also essential that a full submission is made to the Biometric and Surveillance Camera Commissioner before deployment commences.* | |
| **Data Protection Officer Surrey** | | *18/09/2025* |
| **Summary of DPO advice:** | *I have no further comments or concerns that have not already been addressed.* | |
| **Senior Information Risk Owner** | | *29/09/2025* |
| **SIRO Comments** | *I support the logic and approach in adopting a face-match threshold of 0.64* | |

**Referral to the ICO (if required)**

| Refer Name | Date | Comments |
|---|---|---|
| | | |

**DPIA Review History**

| Date | IGO - Force | Comments |
|---|---|---|
| | | |