# Data Protection Impact Assessment Report (DPIA2)

| Information | |
|---|---|
| Name | Thames Valley Police's Overt Use of Live Facial Recognition Technology |
| Forces involved | Thames Valley Police |
| Business Area/s Affected | Joint Operations Unit and Intelligence Command |
| Information Asset Owner | D/Chief Supt. for Crime & Intelligence - Craig Kirby<br>Head of Digital, Digital Transformation (RMS) - Tom Kempster |
| Senior Responsible Officer | D/Chief Supt. for Crime & Intelligence - Craig Kirby |
| Project Manager | Abbie Newnham |
| Information Governance - JIMU Contact | Senior Information Governance Manager - Sharon Warwick |

| Document Ownership | |
|---|---|
| Author(s) | Legal Consultant |
| Document Owner | Joint Information Management Unit - Sharon Warwick |

# Data Protection Impact Assessment Report

## 1. Outline of the objectives, benefits and purpose

TVP proposes to deploy Live Facial Recognition (LFR) technology, commencing late December 2025.

LFR is a real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined 'watchlist' in order to locate persons of interest by generating an alert when a potential match is found.

TVP considers, based on the experience of other police forces (and its own consideration of the technology), that LFR is a highly effective and valuable tool that would support TVP in protecting our communities. As of November 2025, thirteen police forces have used or are using LFR. The Home Office published a consultation on 4 December 2025 which identified a number of benefits of the use of LFR[1]:

- An LFR alert helped the Metropolitan Police locate a man wanted for two outstanding rapes and an offence of indecent assault. The indecent assault was committed in 2017.
- Deployments of LFR in London, from January 2024 to September 2025, led to over 1,300 arrests of individuals wanted for a variety of serious crimes, such as rape, domestic abuse, aggravated burglary, grievous bodily harm, robbery, drug supply, animal cruelty, aggravated harassment, cruelty to children and criminal damage.
- The deployments in London also led to other positive outcomes, such as allowing the police to ensure that registered sex offenders were complying with court-imposed conditions. This led to over 100 arrests during the same period.
- South Wales Police used LFR to help locate and subsequently arrest individuals wanted for a variety of serious crimes, such as grievous bodily harm with intent, robbery, intentional strangulation, actual bodily harm, breach of sex offender notification conditions, domestic violence-related malicious communications, breach of a court order relating to a swelling burglary, vehicle interference and drugs.
- A high risk missing 14-year old girl with significant concerns relating to child sexual exploitation and criminal exploitation was identified following South Wales Police's use of LFR.
- Suffolk Police's use of LFR led to four people being located and arrested for failing to appear before court and a fifth person for theft.

The consultation also recognised that technology, such as LFR, can have a key role to play in addressing violence against women and girls and knife crime.

[1] Police use of facial recognition: factsheet - GOV.UK

The technical operation of LFR comprises of the following six stages:

Compiling/using existing database of images**:** the LFR application requires a Watchlist[2] of reference images against which to compare facial images from the video feed. In order for images to be used for LFR, they are processed so that the 'facial features' associated with their subjects are extracted and expressed as numerical values (a Biometric Template).

The TVP LFR Policy outlines considerations relevant to lawfully compiling a Watchlist including determining the persons who may be on a Watchlist and the sources of Watchlist imagery.

Facial image acquisition**:** a CCTV camera takes digital pictures of facial images in real time, capturing images as a person moves through the Zone of Recognition and using it as a live feed. The siting of the CCTV cameras, and therefore the LFR Deployment location is important to the lawful use of LFR. The TVP LFR Policy and Standard Operating Procedure ("**SOP**") provide considerations relevant to selecting the locations to deploy the cameras when using them for LFR.

Face detection**:** Once a CCTV camera used in a live context captures footage, the LFR software detects individual human faces.

Feature extraction**:** Taking the detected face the software automatically extracts facial features from the image, creating a biometric template.

Face comparison**:** The LFR software compares the biometric template with those held on the Watchlist.

Matching**:** When the facial features from two images are compared the LFR application 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. Trained members of the police personnel will then review the Alerts and make a decision as to whether any further action is required. In this way, the LFR application works to assist police personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input. TVP's LFR Policy and SOP sets out the threshold value that will be used and the independent human review required on any facial matches indicated by the LFR system.

Out of scope: There are other forms of facial recognition technology (FRT) that are not subject of this guidance. This includes Retrospective Facial Recognition (RFR). RFR is also often referred to as post-event, which relates to non-real time searching of images against a database. An emerging variant of FRT is Operator Initiated Facial Recognition (OIFR) where an officer takes a picture of a subject via a mobile device and submits it for an immediate search. This is fundamentally different from LFR in that a human

[2] Terms used in this DPIA are as defined in the LFR Policy Document.

operator has made the decision to submit a particular Probe Image for analysis and is also out of scope for this guidance.

The Chief Constable of TVP will be the data controller for deployments conducted by TVP, for the purpose of TVP's policing objectives in the TVP geographical area. The LFR deployments will be delivered using specialist equipment operated by the TVP and Hampshire & Isle of Wight Constabulary collaborated Joint Operations Unit, LFR Team. During the preparation and delivery of a specific TVP LFR deployment the LFR Team will be acting under the direction and control of the TVP Chief Constable and will in practice be responsible for direction and management of the deployment, according to the arrangements set out in their own LFR Policy and Standard Operating Procedure and other associated LFR impact assessments and documents.

This Data Protection Impact Assessment (DPIA) forms part of a suite of documents which detail the approach and assessment of various risks and mitigations in relation to the deployment of LFR. The TVP LFR Documentation including this DPIA should be read in conjunction with those documents, in particular the TVP LFR Legal Mandate, TVP LFR Policy, TVP LFR Standard Operating Procedure (SOP), TVP LFR Appropriate Policy Document (which includes the TVP LFR Retention Schedule), TVP LFR Privacy Notice, TVP LFR Human Rights Impact Assessment, TVP LFR Equality Impact Assessment, TVP LFR Surveillance Camera Code Self-Assessment as well as the specific TVP LFR Deployment Application and Authorisation.

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

**a) Describe the nature of the processing:**

LFR is a real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined 'watchlist' in order to locate persons of interest by generating an alert when a possible match is found.

Biometric data used to uniquely identify an individual is considered to constitute sensitive processing when used for law enforcement purposes. The sensitive data processed utilising LFR is the biometric facial template data, created from images of individual's faces, for the purpose of uniquely identifying an individual together with the watchlist and CCTV images in so far as they are capable of revealing racial or ethnic origin and/or religious beliefs.

The watchlist for LFR will usually be comprised of a copy of a subset of the TVP custody image dataset but may also include other lawfully held images. These custody images, to be included on a watchlist, have been previously collected by TVP when an individual has been arrested and detained. All watchlist images will have a biometric template created at the point of enrolment to the LFR system.

All images of faces collected via the live LFR cameras will have a biometric facial template created for comparison against the biometric facial templates of persons on the watchlist.

Where the comparison of the LFR live camera images does not generate an alert of a potential match against an image on the watchlist, the biometric template will not be further processed and biometric data of the individual will be automatically and permanently deleted once this comparison has been completed, which is an almost instantaneous process. No other personal identifiers are collected from the live cameras in addition to the image and biometric template.

The categories of personal data processed in the course of an LFR deployment will comprise:

- Images of individuals for inclusion in the watchlist;
- Basic metadata of persons included on the watchlist;
- Extracted biometric templates of individuals included in the watchlist;
- CCTV images of individuals passing through the zone of recognition;
- Extracted biometric templates of individuals passing through the LFR zone of recognition;
- Flagged matches;
- Logs and records pertaining to consideration of matches and any engagement undertaken with individuals.

Categories of special category personal data that may be processed/sensitive processing that may be undertaken in the course of an LFR deployment comprise:

- Racial or ethnic origin;
- Religious or philosophical beliefs;
- the processing of biometric data for the purpose of uniquely identifying a natural person; and
- data concerning health.

Processing will also include criminal conviction and offence data.

Statistical analysis may be carried out to analyse and develop the accuracy, efficacy and equitability of TVP's use of LFR systems. Any processing of images and LFR data for this reason would not involve the need to identify or locate persons. Such analysis would be subject to the additional safeguards such as de-personalisation and would not result in any decisions with respect to a particular individual.

Personal data of police officers and staff may also be processed

**b) Describe the scope of the processing:**

<u>Individuals Affected by the Deployment</u>

The individuals who may be affected by the deployment will be:

- Individuals whose image is included in the LFR deployment Watchlist and whose personal data is processed;
- individuals who avoid entering the zone of recognition and whose personal data is not processed (affected only due to the need to re-route to avoid the zone of recognition);
- individuals who enter the zone of recognition but whose image is not captured by the LFR system and whose personal data is not processed;

- individuals who enter the zone of recognition and whose image is captured and ingested into the LFR system but are not the subject of an alert and whose personal data, including biometric data (comprising special category data/sensitive processing) is processed;
- individuals who enter the zone of recognition and whose image is captured and ingested into the LFR system who are the subject of an alert representing a potential match which is discounted as false by the LFR operator and whose personal data is processed, including biometric data (comprising special category data/sensitive processing);
- individuals who enter the zone of recognition and whose image is captured and ingested into the LFR system who are the subject of an alert which is affirmed by the LFR operator and referred to the LFR engagement officer on the ground but no contact is made and whose personal data is processed, including biometric data (comprising special category data/sensitive processing);
- individuals who enter the zone of recognition and whose image is captured and ingested into the LFR system who are the subject of an alert which is affirmed by the LFR operator and referred to the LFR engagement officer on the ground with contact being made but the officer confirms the individual is not the wanted individual, and personal data is processed, including biometric data (comprising special category data/sensitive processing);
- individuals who enter the zone of recognition and whose image is captured and ingested into the LFR system who are the subject of an alert which is affirmed by the LFR operator and referred to the intervention officer on the ground with contact being made and the LFR engagement officer confirms the individual is the wanted individual and arrests or otherwise disposes of the matter, and personal data is processed, including biometric data (comprising special category data/sensitive processing).

<u>Watchlists</u>

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 Template are deleted immediately post Deployment and in any case within 24 hours.

The criteria for construction of Watchlists for use with LFR must be approved by the Authorising Officer and be specific to an operation. Watchlists, and any images of persons of interest for inclusion on a Watchlist, must be limited to the following categories:

(a) For the purpose of locating persons currently wanted for offences who have an outstanding warrant for their arrest issued by a court or are sought for recall to prison.

(b) Where there are reasonable grounds to suspect the individual of having committed a criminal offence. Both the seriousness of the suspected criminal offence and the prevalence and local impact of the criminal offence should be considered.

(c) Subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the deployment.

(d) For the purpose of locating individuals who are designated as a current High Risk Missing Person. A High Risk Missing Person is where the risk of harm to the subject is assessed as both likely and serious. A missing person should only be included in a watchlist in response to an individual intelligence case, and should be a proportionate response to the need to manage the risk of harm, taking into account the individual's own expectation of privacy, including the impact it may have on the missing person and their expectations of privacy.

Images

Images will typically be obtained from existing police and law enforcement records, and in particular custody images. Custody images are taken in circumstances where the individuals are aware of the collection of their personal data and its retention and use is already subject to various laws and regulations. While this processing is not based on consent, and individuals may not have been aware of the potential for their images to be used in the context of a TVP LFR Deployment, due to the novelty of the technology, the use of their custody images for further law enforcement purposes including the investigation and prosecution of crimes would have been within their reasonable expectation. Section 64A(4) of the Police and Criminal Evidence Act allows for the photographs of detained persons to be used for the prevention and detection of crime, the investigation of offences or the conduct of prosecutions.

There will be occasions, where no image is held by TVP particularly for high risk missing persons, or if one is held, its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of a non-police originated image. Non-police originated images should only be included in a Watchlist with the authorisation of the Authorising Officer. The Authorising Officer should also consider all of 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, limited access, 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.

The TVP Documentation provides that the composition of Watchlists;

- must be based on the intelligence case, authorised by the Authorising Officer and once generated reviewed before each Deployment by the LFR Team to apply additional safeguards in respect of protected characteristics ensuring that Watchlists should not be excessive for the purpose of the LFR Deployment;
- the most up-to-date custody images or non-police sourced images of a person who meets the criteria for inclusion on the watchlist will be extracted for LFR use; and
- ensured that the correct image settings have been used, i.e. those that have proved to be reliable in connection with the LFR system.

Matching

Biometric templates are extracted from the images once the data is uploaded to the LFR System. Watchlists will not be uploaded more than 24 hours prior to a deployment to ensure that the Watchlist is as current as is reasonably possible. The collection of personal information at the LFR recognition zone 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. The LFR system '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. If a Possible Match is made against a Candidate Image, a match report is recorded along with a wider CCTV frame from which the Probe Image was extracted.

Biometric templates of individuals who are flagged as a potential match are deleted within 24 hours of the conclusion of the deployment.

Where the comparison of the LFR live camera images does not generate an alert of a potential match against an image on the watchlist, the biometric template will not be further processed and biometric data of the individual will be automatically and permanently deleted once this comparison has been completed, which is an almost instantaneous process. No other personal identifiers are collected from the live cameras in addition to the image and biometric template.

The CCTV live feed capture of members of the public passing through the recognition zone is deleted after 31 days unless by exception it is required to be kept retained for longer:

- Retained in relation to investigate a complaint about officer conduct; or
- Retained as evidence for a criminal offence investigation / prosecution.

All Watchlist images uploaded to the LFR system are deleted within 24 hours of the conclusion of the deployment.

Not every person walking through the LFR recognition zone that is captured via the CCTV will be enrolled into the application. The face has to be of sufficient 'quality' to enrol into the application. The level of enrolment rate will be dependent on many factors, the significant of these include;

- crowd density,
- individual movements,
- face angle; and
- lighting.

TVP will have a:

- LFR Authorisation Process Guidance Flowchart which clearly sets out the decision-making steps to use LFR which is captured in the LFR SOP; and
- LFR Policy and SOP, which should include details of: factors to consider relating to use case and policing priorities for LFR; criteria for watchlists and sources of

imagery; guidance when an Alert is generated, actions to be taken following an Alert, the resourcing of deployments to respond to alerts, and relevant policing powers; factors to consider when deciding on deployment location and camera placement; arrangements to ensure that the deployment is overt, including considerations regarding any prior notification and signage; responsibilities of officers and staff involved in deployment;

- LFR Appropriate Policy Document details the retention periods for data processed during LFR deployments.

Individuals whose personal data is processed may be more likely to be locally based but processing is not restricted to individuals who reside within the jurisdiction of TVP.

It is difficult to estimate the anticipated scale of processing but it is likely to be a high volume. This DPIA proceeds on that basis. However, for the vast majority of individuals the processing will last no longer than the time it takes them to traverse the LFR Zone of Recognition before their personal data is deleted and the impact on them is considered to be negligible.

Steps have been taken to minimise the duration of processing of personal data. In respect of the most sensitive biometric data, in respect of individuals who are not flagged as a potential match for a watchlist image, this data is deleted automatically and almost instantaneously. In relation to biometric templates of individuals who are flagged as potential matches, the biometric template is deleted no later than 24 hours following the conclusion of the deployment. The CCTV live feed capture of members of the public passing through the recognition zone is deleted after 31 days unless by exception it is required to be kept retained for longer:

- Retained in relation to investigate a complaint about officer conduct.
- Retained as evidence for a criminal offence investigation / prosecution

The geographical area will be determined by the purpose of the Deployment, however the intention is to focus LFR overtly over a distinct geographically limited location or event. The Authorising Officer will define the date, time, location and duration the Deployment is authorised for based on the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the intelligence case behind the Deployment, as set out by the applicant and recorded on the application document.

The proposed processing activities will be conducted pursuant to Part 3 Data Protection Act 2018 and/or, particularly in connection with high risk missing persons, the UK GDPR.

While all of these categories of individual are considered in the Human Rights Impact Assessment and Equality Impact Assessment, which have been conducted contemporaneously with this Data Protection Impact Assessment (DPIA), only those categories of individual whose personal data may be processed in the course of the deployment are addressed in this DPIA.

The Chief Constable of TVP will act as data controller in respect of personal data processed in the context of its LFR Deployments at all times.

**c) Describe the bigger picture in which the processing is taking place:**

It is acknowledged that the processing of personal data in the context of LFR Deployments will involve the use of novel technologies, and in particular the use of artificial intelligence in the form of the extraction and comparison of biometric templates of still and moving images.

This has been the subject of considerable public debate, and has been considered by the Courts. The Home Office has recently stated that "*whilst it is clear there is a legal framework within which facial recognition can be used now … confident, safe and consistent use of facial recognition and similar technologies at significantly greater scale requires a more specific legal framework*".[3] However, pending the introduction of bespoke legislation governing LFR, currently the use of LFR is subject to a range of laws and regulations which are detailed in this DPIA and the LFR Documentation, including the Legal Mandate.

Individuals included in Watchlists will be individuals suspected of criminality and who are wanted by the courts and police, individuals who may pose a risk to themselves and others, and individuals who may be vulnerable. These individuals will not have consented to the processing of their personal data. Nevertheless, there is strong public interest in identifying these individuals and enabling them to be subject to appropriate action. There is a reasonable expectation that personal information will be processed for the fulfilment of operational police duties including: protection of life; preserving order; preventing the commission of offences; and bringing offenders to justice. It is likely, then, to be within these individuals expectations that their personal data could be processed for these purposes. In relation to high-risk missing persons, the need to safeguard their interests outweighs any reasonable expectations they might have in relation to the privacy of non-police images.

There are also concerns that the software algorithm may contain inherent bias, including with regard to the protected characteristics of race, age and gender. The specific technology to be used in the LFR Deployments has been subject to scientific testing both as to its efficacy and the potential for bias and discrimination. The National Physical Laboratory's scientific testing found that at a setting of 0.64 (algorithm threshold) there was equitability of facial matching accuracy across all demographics. In TVP's consideration of the threshold setting it will adopt, it has reviewed the LFR deployments made by South Wales Police where (at the time of writing this document) no inaccurate matches were experienced at a threshold setting of 0.64. TVP will deploy LFR with an accuracy setting of 0.64 and carry out its own equitability evaluation after each deployment.

During any policing operation where LFR is deployed, signs publicising the use of the technology will be prominently placed in advance around the Zone of Recognition. These measures are to alert members of the public of the presence of LFR technology and allow them sufficient time to exercise their right not to walk into the Zone of

[3] https://www.gov.uk/government/consultations/legal-framework-for-using-facial-recognition-in-law-enforcement/consultation-on-a-new-legal-framework-for-law-enforcement-use-of-biometrics-facial-recognition-and-similar-technologies-accessible

Recognition. In advance of the Deployment, TVP will use social media and its website to publicise details of the Deployment.

There will be processing of the personal data of children or vulnerable groups in LFR Deployments due to their walking through the Zone of Recognition. However, if their Biometric Template does not generate a Possible Match no other details will be processed and this information will be deleted immediately. Where there is a Possible Match, the LFR Operator will be alerted and further manual checks will be carried out to identify whether that person is on the Watchlist.

**3. Data Subject Views:**

Careful consideration has been given to the views of the general public in relation to the deployment of LFR. Surveys indicate a high level of public support for the use of facial recognition technology in policing. In a study published by the Home Office in December 2025, 2 in 3 support the use of facial recognition technology in policing, while 1 in 10 were opposed. The reporting found that: *"[r]espondents recognised benefits such as helping the police to catch criminals, enhance public safety, and locate missing or vulnerable individuals. However, concerns included the potential for misuse or hacking, risk of false identification and issues around data privacy*." There are concerns that Deployments will limit or contravene the right to privacy or deter members of the public from exercising their right to freedom of assembly and freedom of expression. TVP is mindful of these concerns, as well as the concerns expressed by the Courts in R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058, and the judgment of the European Court of Human Rights in Glukhin v Russia (Application No. 11519/20). TVP has addressed those concerns in the development of safeguards applicable to the deployments.

In the police force area of TVP, the following consultation has been undertaken, and is ongoing, in respect of TVP's decision to deploy LFR as a policing tactic in appropriate circumstances.

- The TVP "Think Tank", is independently chaired and has been consulted and been given an opportunity to ask questions and challenge thinking. The group is made up of both internal and external stakeholders from a variety of backgrounds and with a variety of specialist interests and experiences. The objectives of the "think tank" are:
    - To consider, provide advice and guidance on and challenge the interpretation of legitimacy and implications of external statutory, regulatory requirements or policy guidance relating to legitimacy matters for both policing and non-policing agencies.
    - To review and provide advice on cases, circumstances and activities which have significant or novel and/or wider-ranging ethical considerations and which fall within any of the legitimacy principles.
    - To oversee the development of a legitimacy framework/strategy to enable corporate and institutional matters to be consistently, fairly and proportionately assessed, and receive assurance on the effectiveness of its strategy.

- Highlight any significant risk to or opportunity and share good practice and good news stories.
- Share knowledge and provide guidance on how legitimacy impacts on partnerships and Organisational Development.
- Advise on contemporary policing issues and matters of emerging interest to policing.

- Separately, the TVP "Chairs of Independent Advisory Groups" has been consulted. This group is made up of the chairs of the various local IAGs from across the different areas of TVP. Again, this group has been briefed and given an opportunity to ask questions and challenge, but also invited to cascade information about TVP's plans to deploy LFR technology in communities to local IAGs, who, in turn, are invited to engage with tactical and strategic LFR leads accordingly.

The Information Commissioner's Office was notified of TVPs first LFR Deployment, in advance.

Through on the ground engagement by officers with members of the public during the course of deployments it is anticipated that unsolicited feedback will be provided which will further inform our view of public attitudes.

Individuals likely to be included as part of watchlists have not been the subject of explicit pro-active consultation because it would be impossible to carry out that consultation, or because it would defeat the purpose of the deployment to do so.

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

Information is being processed under Law enforcement / UK GDPR / UK GDPR & Law Enforcement rules.

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

**Lawful basis** for the processing of personal data is stated as follows:

- Personal data:
  - TVP will not rely on an individual's consent to process their personal data for LFR purposes and therefore where processing takes place pursuant to Part 3 Data Protection Act 2018, i.e. for the law enforcement purposes, the processing of personal data takes place in accordance with section 35(2)(b) Data Protection Act 2018, i.e. the processing is necessary for task carried out for the law enforcement purposes by TVP, which is a competent authority for the purposes of the Act;
  - the "law enforcement" purpose, defined in section 31 Data Protection Act 2018, is: the prevention, investigation, detection, and prosecution of criminal

offences; the execution of criminal penalties; and the safeguarding against and the prevention of threats to public security;

- TVP's processing of personal data for LFR must also be 'authorised by law' which is met by the 'policing purpose' set out in the Statutory Code of Practice on Police Information and Records Management; and
- where processing takes place pursuant to the UK GDPR (e.g. for the location of high risk missing persons, or the evaluation of efficacy and equitability of LFR), the processing meets one or more of the following requirements: processing is necessary for compliance with a legal obligation to which the controller is subject [Article 6(1)(c) UK GDPR]; processing is necessary to protect the vital interests of the data subject or another natural person [Article 6(1)(d) UK GDPR]; and/or processing is necessary for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller [Article 6(1)(e) UK GDPR].

- Special Category / Sensitive data:
  - TVP will not rely on an individual's consent to process their sensitive data for LFR purposes and therefore TVP relies on the following conditions from Schedule 8 of the DPA 2018 and has an Appropriate Policy Document in place:
    - Statutory etc. purposes (Schedule 8(1)): processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest);
    - Administration of justice (Schedule 8(2)): processing is necessary for the administration of justice);
    - Protecting individual's vital interests (Schedule 8(3)): processing is necessary to protect the vital interests of the data subject or another individual);
    - Safeguarding of children and of individuals at risk (Schedule 8(4)): processing is necessary to protect individuals, under 18yo or over 18yo and at risk form neglect or physical, mental or emotional harm; or protecting the physical, mental or emotional wellbeing of an individual);
    - Personal data already in the public domain (Schedule 8(5)): processing relates to personal data which has been manifestly made public by the data subject); and
    - Legal claims (Schedule 8(6)): processing is necessary for in connection with legal proceedings, obtaining legal advice, or establishing / exercising / defending legal rights).

  - TVP will not rely on an individual's consent to process their special category data for LFR purposes and therefore TVP relies on the following conditions from article 9(2) of the UK GDPR and Schedule 1 of the DPA 2018 and has an appropriate policy document in place:

- Article 9(2)(c)): processing 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;
- Article 9(2)(e)): processing relates to personal data which are manifestly made public by the data subject;
- Article 9(2)(g)): processing necessary for reasons of substantial public interest provided for in domestic law. The substantial public interest conditions require a condition from Part 2 of Schedule 1 of the DPA 2018 to be satisfied, as follows:
    i. Schedule 1, Part 2(6) Statutory and government purposes: processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest.
    ii. Schedule 1, Part 2(8) Equality of Opportunity or Treatment: Processing is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained.
    iii. Schedule 1, Part 2(18) Safeguarding of children and of individuals at risk: processing is necessary to protect individuals, under 18yo or over 18yo, and at risk form neglect or physical, mental or emotional harm; or protecting the physical, mental or emotional wellbeing of an individual.

- Criminal data:
    - TVP will process criminal offence data during LFR deployments and under Article 10 of the UK GDPR and section 10(5) of DPA 2018 the processing must satisfy a condition from Parts 1-3 of Schedule 1 of the DPA 2018. TVP meets the following conditions:
        i. Schedule 1, Part 2(6) Statutory and government purposes: processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest.
        ii. Schedule 1, Part 2(8) Equality of Opportunity or Treatment: Processing is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained.
        iii. Schedule 1, Part 2(18) Safeguarding of children and of individuals at risk: processing is necessary to protect individuals, under 18yo or over 18yo, and at risk from neglect or physical, mental or emotional harm; or protecting the physical, mental or emotional wellbeing of an individual.

- Wider lawfulness:

  The wider lawfulness of the processing of personal data in the context of the deployment of LFR is set out in detail in the TVP Legal Mandate, which should be read together with this DPIA.

  In summary the position is:

  - LFT for law enforcement purposes is not currently subject to dedicated primary legislation. Rather, LFR is governed or informed by existing laws and guidance, including the Data Protection Act 2018, UK GDPR, Human Rights Act 1998, Equality Act 2010, Protection of Freedoms Act 2012, the Amended Surveillance Camera Code of Practice, the Surveillance Camera Commissioner's 'Facing the Camera: Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales', Information Commissioner's Opinion on 'The use of live facial recognition technology in public places', and the College of Policing Authorised Professional Practice on Live Facial Recognition, and jurisprudence.
  - Section 64A(4) of the Police and Criminal Evidence Act allows for the photographs of detained persons to be used for the prevention and detection of crime, the investigation of offences or the conduct of prosecutions.
  - In addition to complying with the specific requirements of data protection legislation, steps have been taken to ensure that the proposed processing meets wider legal obligations, including under the Human Rights Act 1998 and Equality Act 2010.
  - The Court of Appeal in *Bridges* recognised that while there is an existing legal framework in which to regulate the use of LFR, which does contain sufficient safeguards, care must be taken to ensure that LFR is deployed in a way which does not leave too much discretion to individual police officers.
  - The European Convention on Human Rights and the Human Rights Act 1998, which incorporates Article 8 of the Convention into UK law, protects the right to respect for private and family life. TVP has separately considered the way in which the deployment of LFR impacts on the human rights of both those on the Watchlist, and those who pass through the Zone of Recognition, in the TVP Human Rights Impact Assessment.
  - s.149 Equality Act 2010 imposes an obligation on public authorities, in the exercise of their functions, to have due regard to the need to eliminate discrimination, harassment, victimisation and any other prohibited conduct, advance equality of opportunity between those who share a protected characteristic and those who don't and, to foster good relations between such groups.
  - Sections 13 and 19 of the Equality Act 2010 prohibit direct (that is to say the less favourable treatment of a person compared to another based on a protected characteristic (i.e. age, disability, gender reassignment, pregnancy

and maternity, race, religion or belief, sex and/or sexual orientation)) and indirect (the application of a provision, policy or practice to an individual discriminates against them based on a relevant protected characteristic).

- In support of meeting the public sector equality duty (PSED), and ensuring that LFR Deployments are not discriminatory, TVP has carried out an LFR Equality Impact Assessment (EIA) which shall be reviewed at least annually and kept under periodic monitoring throughout the period during which LFR Deployments are undertaken to ensure that any learning or trends can be identified and addressed at an early stage. That EIA should be read in conjunction with this DPIA and the Human Rights Impact Assessment in particular.
- Consideration has also been given to any potentially discriminatory impact of the operation of the LFR system, in connection with the processing of personal data. The specific technology to be used in the LFR Deployments has been subject to scientific testing both as to its efficacy and the potential for bias and discrimination. The National Physical Laboratory's scientific testing found that at a setting of 0.64 (algorithm threshold) there was equitability of facial matching accuracy across all demographics. In TVP's consideration of the threshold setting it will adopt, it has reviewed the LFR deployments made by South Wales Police where (at the time of writing this document) no inaccurate matches were experienced at a threshold setting of 0.64. TVP will deploy LFR with an accuracy setting of 0.64 and carry out its own equitability evaluation after each deployment.

- Explain how individuals will be made aware of the processing.

  Several methods are proposed to make affected individuals, and the wider community, aware of the processing of personal data.

  TVP already publishes a privacy notice which addresses its processing of personal data, including in connection with the processing of custody images etc. Those individuals who have already had contact with the police will be aware of the taking of their custody image and the processing of their personal data,

  This is supplemented in relation to the deployment of LFR with the publication of an LFR specific privacy notice and LFR specific Appropriate Policy Document.

  In advance of all proposed deployments, TVP will issue an alert on its website and via social media. It is anticipated that this will be the subject of further coverage, for example in local print and broadcast media.

  Where considered necessary and appropriate, businesses and other organisations in the vicinity of the deployment will be engaged with both in advance and on the day.

  LFR deployments will be overt. Appropriate signage will be placed at the perimeter of the LFR deployment location to ensure that individuals are alerted to the LFR deployment. These measures will be supplemented by officers and staff

who are able to provide further information to members of the public, including leaflets on how to ascertain further information regarding the deployment and exercise any right of recourse. Individuals will be able to exercise a choice as to whether to enter the LFR deployment zone of recognition or seek to take steps to conceal their face.

To supplement the LFR Privacy Notice, TVP is also publishing other documentation pertaining to LFR to assist in advancing public understanding of the technology, its use and the compliance measures and safeguards that are in place.

**Necessity**

TVP recognises that the use of LFR is novel and can constitute a material interference with an individual's privacy. However, TVP considers that LFR can deliver considerable policing benefits.

The Home Office published a consultation on 4 December 2025 which identified a number of benefits of the use of LFR[4] including locating individuals wanted for serious criminal offences, leading to arrests for criminal offences, assisted with ensuring registered sex offenders were complying with court-imposed sanctions, and locating high-risk missing children.

In relation to high risk missing persons, the nature of these incidents is often such that locating the individual is an urgent priority given the risk they pose to themselves or others.

Therefore, while alternative, less intrusive measures of locating wanted individuals, suspects and/or high risk missing persons are available, TVP considers that the option of appropriate use of LFR is more likely to protect the rights of individuals, particular having regard to the fact that those other methods require higher ratios of police officers and staff. Further, as explained herein, a number of safeguards have been adopted to ensure that LFR is used in a proportionate manner.

**Proportionality**

The individuals whose images can be included on a Watchlist include individuals wanted for offences who have an outstanding warrant for their arrest issued or are sought for recall to prison; where there are reasonable grounds to suspect the individual of having committed a criminal offence; and those in breach of bail conditions, court orders, or similar. In these circumstances, and for these individuals, TVP considers that, having regard to the law enforcement purposes which are strongly engaged, when balanced against the rights of affected individuals and taking into consideration the safeguards which are in place, an interference with individual rights is subject to appropriate safeguards considered to be proportionate to the aim pursued.

[4] Police use of facial recognition: factsheet - GOV.UK

In relation to high risk missing persons, the risk posed by those individuals to themselves and/or others, and the need to safeguard them and the general public, when balanced against the interference with individual rights is subject to appropriate safeguards considered to be proportionate, in the round.

The above assessments take into account the processing of the personal data of members of the public who are passing through the Zone of Recognition. The impact on those rights is extremely limited (and has been characterised by the Court of Appeal as "negligible"). The use of LFR requires matching data, and therefore the processing of the personal data of members of the public who pass through the Zone of Recognition is required as part of an LFR Deployment. Taking into account the negligible impact on their rights, the fact that each LFR Deployment is overt and transparent, that there are safeguards in place, the processing is considered to be proportionate to the pressing social aim pursued.

**Fairness**

In order to ensure fairness TVP will:

- adopt the transparency and educational measures for the general public detailed above; and
- the efficacy and performance of the system has been considered together with scientific research on potential bias and/or discrimination in the system, as detailed.

**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:**

Where a police custody image (collected for a law enforcement purpose) is used on an LFR watchlist to locate a high risk missing person (a non-law enforcement purpose), the processing will be subject to the provisions of the UK GDPR and must satisfy section 36(4) of the DPA 2018 and be 'authorised by law'. Its use is 'authorised by law' by satisfying the 'policing purpose': protecting life and property, as set out in the Statutory Code of Practice on Police Information and Records Management.

In relation to custody or other police sourced images, it would be within the reasonable expectations of individuals that such personal data would be re-used for law enforcement purposes. Section 64A(4) of the Police and Criminal Evidence Act allows for the photographs of detained persons to be used for the prevention and detection of crime, the investigation of offences or the conduct of prosecutions.

The personal data which is collected (biometric templates) will not be used for any other purpose. The data will be retained for a limited period, as set out in the retention policy.

**Principle 3: Use of personal data is adequate, relevant and no more than necessary:**

TVP ensures that the use of personal data is adequate, relevant and no more than necessary:

- It is necessary to utilise images in order to obtain a biometric template;
- All personal, sensitive and criminal data processed by TVP for LFR is retained only in accordance with Appendix 1 – Table of Retention Periods for LFR Data, appended to the Appropriate Policy Document (published on the TVP LFR website).
- For members of the public passing through the LFR recognition zone, where the comparison of the LFR live camera images does not generate an alert of a potential match against an image on the watchlist, the biometric template will be automatically and permanently deleted once this comparison has been completed, which is an almost instantaneous process. No other personal identifiers are collected from the live cameras in addition to the image and biometric template.
- The CCTV live feed capture of members of the public passing through the recognition zone is deleted after 31 days unless by exception it is required to be kept retained for longer:
  - Retained in relation to investigate a complaint about officer conduct.
  - Retained as evidence for a criminal offence investigation / prosecution
- The retention and deletion custody images stored on TVP's crime recording system, from which the watchlist images are sourced, will be managed outside of the LFR processing; in accordance with the retention guidance set out in the Statutory Code of Practice on Police Information and Records Management and associated College of Policing's Authorised Professional Practice on Information Management
- The images on the LFR watchlist will be deleted within 24 hours of the completion of the LFR deployment.

**Principle 4: Personal data must be accurate and kept up to date:**

For members of the public, the processing of their personal data (biometric template) will be in real time.

In terms of the Watchlist, technological safeguards have been put in place to ensure that the images uploaded to the watchlist are the most recent and up-to-date police held image of the individual. Watchlists must be compiled no more than 24 hours in advance of the deployment. TVP has put in place steps to ensure that image quality and suitability for comparison will be considered as part of the process of creation of a Watchlist.

Consideration has also been given to any potentially discriminatory impact of the operation of the LFR system, in connection with the processing of personal data. The specific technology to be used in the LFR Deployments has been subject to scientific testing both as to its efficacy and the potential for bias and discrimination. The National

Physical Laboratory's scientific testing found that at a setting of 0.64 (algorithm threshold) there was equitability of facial matching accuracy across all demographics. In TVP's consideration of the threshold setting it will adopt, it has reviewed the LFR deployments made by South Wales Police where (at the time of writing this document) no inaccurate matches were experienced at a threshold setting of 0.64. TVP will deploy LFR with an accuracy setting of 0.64 and carry out its own equitability evaluation after each deployment. Additionally, TVP will consider, on an ongoing basis, the accuracy and efficacy of the LFR system, including through post-Deployment reviews and evaluation.

LFR is a tool that assists police officers to locate persons of interest. A LFR match does not qualify as formal identification and LFR software does not make decisions that result in any person being spoken to. It provides a guide to officers about which people passing through the Zone of Recognition may be of interest to them. LFR Operators then consider the alert using their experience and training, before the Engagement Officer makes any decision to engage with a person. This includes consideration about whether age is a factor in generating an alert. Even where an engagement occurs, further action is not an automatic consequence, the officer would need a lawful basis to take any further action (such as an arrest).

Law enforcement specific accuracy requirements (DPA 2018, Part 3):

- Section 38(2) of the DPA 2018 requires that for any of the law enforcement purposes that personal data based on fact must be distinguished from personal data based on personal assessments, so far as possible. The LFR system achieves this by effectively indicating its confidence in the potential match through the match score and the LFR system operators and Engagement Officers contextually understand that any potential match alerts produced by the LFR system are not fact but are a technical assessment that helps supplement the officers' human assessment.
- Section 38(3) of the DPA 2018 requires that for any of the law enforcement purposes a clear distinction must be made, where relevant and as far as possible, between personal data relating to different categories of data subject. The images of persons included on the watch list will be categorised and labelled as per the policing objective of their inclusion.

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

All personal, sensitive and criminal data processed by TVP for LFR is retained only in accordance with Appendix 1 – Table of Retention Periods for LFR Data, appended to the Appropriate Policy Document (published on the TVP LFR website).

Where the LFR system does not generate an alert a person's biometric data derived from the live LFR CCTV feed it is immediately automatically deleted. Where the LFR system does generate an alert, that person's biometric data derived from the live LFR CCTV feed is deleted within 24 hours following the conclusion of the deployment.

Watchlist data held on an encrypted USB memory stick used to import the watchlist onto the LFR system is deleted within 24 hours following the conclusion of the deployment.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

- due to its relevance in a criminal investigation and is then held in accordance with the Data Protection Act 2018, UK GDPR, MOPI and the Criminal Procedures and Investigations Act 1996; and /or
- in accordance with TVP's complaints / conduct investigation policies or other legal obligations.

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

TVP comply with the relevant parts of the legislation relating to security, and seek to comply with the College of Policing - Information Assurance Authorised Practice and relevant parts of the ISO27001 Information Security Standard.

TVP standard operating procedures and policies make clear what use may be made of any sensitive data contained within them. Our security measures are designed to protect against unauthorised or unlawful processing, accidental loss, destruction or damage. The security of the LFR system has been assessed by the TVP ICT department.

The LFR System is subject to the following security measures:

Technical:

- The application is non-networked and not configured to extend to the cellular network as an additional geographical protection.
- The LFR application is 'closed' and not connected to other TVP systems or the internet.
- The TVP watchlist is transferred from the TVP crime recording system by encrypted USB to the closed LFR System where it is uploaded.
- The Dashboard and RESTful API are secured with SSL and TLS by default.
- All connections are directed through HTTPS.

Organisational:

- Two types of access will be available to the application – 'user' and 'administrator' access levels.
- Passwords are security protected.
- LFR System operating staff will have police vetting clearance.
- Role- based access controls.
- LFR System access is only granted to users following completion of training.
- The LFR system is staffed when in use and therefore physical protections are in place.
- The physical encrypted USB remains the responsibility of a specified member of the LFR Team during the LFR deployment.

Audit:

- The LFR System has an inbuilt audit file.
- Audit data enables 'logging data' to be retained regarding user activity that enables user and system auditing to be conducted.

In relation to TVP officers and staff, these individuals will have been subject to appropriate police vetting and are subject to statutory and contractual obligations of confidentiality and have received general data protection and information security training as well as LFR specific training.

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

Where possible and appropriate individuals will be able to avoid the area in which the Deployment is located. Members of the public will be informed prior to a deployment.

TVP already publishes a privacy notice which details individuals' data protection rights, including providing details of the Data Protection Officer and rights of recourse. A specific supplementary privacy notice has been prepared and published in relation to TVP's LFR Deployments, providing further detail of the specific application of these rights.

Both of these privacy notices will be available online. They will also be highlighted to individuals at the perimeter of the Zone of Recognition and via QR codes. For those individuals who are engaged with by an LFR Engagement Officer further to a potential Watchlist match being flagged by the LFR system, the LFR Policy and SOP require those individuals to be pro-actively offered LFR information leaflets that will deliver key messages about how LFR works and signpost to further information on the TVP LFR website about their rights and mechanisms to seek recourse.

In terms of specific rights, where personal data is retained:

- Right to rectification – individuals will be able to challenge the processing where a Possible Match has been identified by LFR and the LFR Engagement Officer/Officer;
- 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 object – not applicable under Part 3 of the Data Protection Act 2018. TVP 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 Data Protection Act 2018.

In fulfilment of its obligations under s.81 of the Data Protection Act 2018:

- As part of the ongoing review and oversight arrangements, complaints and concerns will be considered; and
- It will be emphasised to all officers and staff engaged in LFR Deployments, through operational briefings, that any perceived infringement of the rights of

individuals, or failure to comply with the requirements of LFR documents, should be reported to the LFR Silver Commander.

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

The Data Protection Act 2018 restricts the transfer of personal data processed for law enforcement purposes outside the UK and the UK GDPR imposes safeguards on the transfer of personal data to countries which fail to provide adequate protections for personal data.

The LFR System is a siloed, non-networked, on-premise application, which does not involve the transfer of personal data outside of the UK.

**9. The force must be able to demonstrate how they are complying with the Data Protection Act 2018 & UK GDPR:**

TVP demonstrates how its use of LFR meets the requirements of the DPA 2018 (Part 3 in particular) and UK GDPR with the following measures which will be reviewed and updated when required:

- Conducting and publishing a Data Protection Impact Assessment, reviewed by the Data Protection Officer.
- Publishing a LFR specific privacy notice and appropriate policy document.
- Publishing a retention schedule for the different types of personal data processed during LFR.
- Designing LFR processes to take into account data protection requirements.
- Carrying out a security assessment of the LFR system and implementing appropriate security measures.
- Having an Information Management Policy and LFR Policy.
- Having written contracts with any data processors.
- Recording LFR activity in TVP's Record of Processing Activities.

An audit trail will demonstrate how personal data is processed, and decisions are taken, for each deployment. That audit trail will consist of the LFR Application, Written Authority Document, Operational Risk Assessment, LFR Cancellation Report and the Deployment Logs.

If any future TVP statistical analysis to develop the accuracy and efficacy of our use of LFR systems, is carried out on our behalf by a third party, this relationship will be governed by a data processing contract (if necessary).

**5) Data protection risks and actions required to mitigate them:**

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.

However, although not detailed below in the risk table, non-compliance with the legislation will have a detrimental impact on the organisation resulting in additional scrutiny from the Information Commissioner's Office and the potential to receive significant fines.

The below listed 'agreed actions' have been identified as a way to either **reduce or eliminate** risks identified as **medium or high**. Agreed measures will need to 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 problem that is the risk, the vulnerability that creates the problem and the potential impact on individuals.**<br>Focus mainly on the impact on the data subject. Mention corporate risks only as necessary. | **Likelihood of harm**<br>Remote, possible or probable. | **Severity of harm**<br>Minimal, some impact, or serious. | **Risk score**<br>Low, medium or high. | **Agreed action**<br>Detail to action that will reduce the risk | **Action Owner**<br>Name & date | **Residual Risk score**<br>Low, medium or high. |
|---|---|---|---|---|---|---|---|
| 1 | Vulnerability when data in transit: Watchlist Transfer.<br><br>As a result of the Watchlist being downloaded onto USB, the USB could be lost or intercepted by threat actors. This would result in a data breach whereby personal data and images of | Remote | Serious | Low | The USB memory stick utilised for transfer will be encrypted. The time period during which personal data is stored on the encrypted USB memory stick is minimised by the watchlist only being created no more than 24 hours prior to the deployment and being required to | LFR Operator – routine LFR activity | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | persons who were sought on the Watchlist, including the reasons they were sought, could be released to members of the public who are not authorised to have access. | | | | be deleted within 24 hours of the deployment.<br><br>The USB drives are provided to the LFR Operators at the start of the Deployment and returned at its conclusion. During that time, they are the personal responsibility of the LFR Operator they are provided to. Operators are appropriately vetted to ensure they are suitable persons to have access to such data. | | |
| 2 | Vulnerability when data in transit: Camera Feeds.<br><br>Threat actors could intercept the feeds through the wireless network of cameras and compromise police data or interfere with feeds coming into cameras. This could lead to data being intercepted and confidentiality, availability and data integrity concerns. | Remote | Some Impact | Low | The rapid deployment cameras used by TVP for this purpose do not collect or retain any personal information nor do they undertake any biometric processing. The feeds from the cameras are transmitted via an encrypted VLAN to the van, where the feeds are compared by the LFR Software. The LFR system itself is a siloed non-networked system, which is subject to security measures. | Automated system mitigation | Low |
| 3 | Vulnerability when data at rest: Police information, including personal information, images and Watchlist data could be | Remote | Serious | Low | All computers utilised for LFR by TVP have password access requirements for the computer and also for LFR software. Personal | Automated system mitigation | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | intercepted or interfered with from LFR computers on board LFR vans.<br><br>Threat Actors could gain access to data that has been uploaded to the computers on board LFR vans in public places and intercept or interfere with police held data, leading to a compromise of the data and/or threat to police systems which in turn could affect the confidentiality, availability and integrity of all police held information | | | | and biometric data utilised for the purposes of LFR are not retained within the computer itself and are stored within the LFR software whilst it is in operation. The LFR application is staffed when in use to ensure the security of the LFR system. At the conclusion of the Deployment, data is erased from the LFR system and associated USB drives and cannot be recovered. The application is non - networked and non - configured to extend to the cellular network – essentially an additional geographical protection. The LFR application is 'closed' and not connected to other TVP systems or the internet. | | |
| 4 | Vulnerability when data at rest: Wireless cameras deployed could be damaged for the purpose of intercepting personal data contained within the cameras.<br><br>Threat actors could target the wireless cameras whilst they are not attended and obtain personal data held within the camera which may provide them with | Remote | Some Impact | Low | The cameras have no internal memory and will not receive any personal information through data transfer. No biometric processing will be undertaken in the cameras nor will it be stored within. | Automated system mitigation | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | personal information of individuals | | | | | | |
| 5 | Physical security: A device with LFR software and data may be stolen and utilised by an individual who may gain unauthorised access to information held on the LFR system which may pose a risk to persons included in those Watchlists. | Remote | Serious | Low | Whilst LFR is in operation, an LFR Operator must be in attendance at all times. LFR Operators are warranted police officers and are trained to manage their own protection should an individual try to take a device with LFR capability by force. At the conclusion of an LFR Deployment, all devices and USB drives are accounted for the by Authorising Officer. Further, the LFR system does not retain any biometric templates other than those who have generated an alert. Those Biometric Templates are retained for the duration of the deployment and then deleted with no means of recovery by the LFR Operator.<br><br>All computer devices capable of LFR have a password access requirement for the computer and a second for the LFR system. | LFR Operators – routine LFR activity | Low |
| 6 | Personnel security: There is a risk that TVP officers or staff may access or interfere with data used by the LFR System which | Remote | Serious | Low | The LFR data is uploaded onto and held securely on TVP systems accessible to only a small team of vetted LFR operators and officers. | Vetting Team, automated system | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | may lead to a risk to individuals or affect the confidentiality, availability and integrity of the LFR data. | | | | The LFR system is fundamentally permission based. The data held on TVP systems is not specific to LFR (it provides LFR with the information needed to compile and generate a Watchlist and relates to policing information generated following LFR Alerts). | activity, LFR Team Lead. | |
| 7 | Commercial Service Providers/ Suppliers: There is a risk that the supplier of the algorithm may fail to ensure that any bias or discrimination is eliminated as far as possible resulting in inaccurate identification of individuals leading to false Alerts, unlawful arrests, unlawful interference with Article 8 rights, and targeting of minorities unfairly. | Remote | Serious | Low | The algorithm was tested by National Physical laboratory (NPL) to determine the most appropriate settings to mitigate or eliminate bias towards any demographic. Whilst this testing attempted to replicate the realism of operational environments, it is recognised that there are variables such as lighting etc in the operational environment that cannot be controlled and could not be tested in a non - operational environment. TVP have accepted the guidance of the NPL and the TVP LFR Policy prescribes a 0.64 threshold setting that deems bias highly unlikely. A LFR Operator will provide an independent human review of the matched images to oversee the likeness of any match. TVP will monitor Deployment data and outcomes to determine the Threshold setting remains appropriate. This will include a | LFR Operator | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | review of the number of Alerts confirmed as Positive matches, those returning False Positive matches, the circumstances, System Factors, and Environmental Factors that may have impacted on the performance of the LFR algorithm. TVP has carried an Equality Impact Assessment which will be kept under review. | | |
| 8 | Accidental Disclosure: as a result of the LFR Operator identifying an incorrect match there is a risk that third party data may be disclosed leading to a loss of confidentiality | Remote | Serious | Low | The LFR Operator will not solely rely on the generation of an Alert to confirm the identity of the Subject. The LFR Engagement Officer will then decide whether to engage with the LFR Operator's confirmed matched person. LFR is a policing tool to assist TVP in locating persons sought by TVP for policing purposes. It supports decision making with any results providing an indication which is considered only as intelligence. | LFR Operator & Engagement Officer | Low |
| 9 | Information provision: Where LFR is deployed, there is a risk that fair processing information may not be widely available to members of the public resulting in them not being informed of the processing of their personal data | Possible | Some impact | Medium | TVP publishes a general privacy notice online and a LFR-specific privacy notice which is accessible to data subjects; published online.<br><br>In addition to this, TVP will ensure that website and social media | LFR Team and LFR Engagement Officers | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | resulting in a potential data breach, increased complaints, court cases, enforcement action and reputational damage. | | | | messaging includes information about LFR Deployments. It is anticipated that this will result in further coverage, including in traditional news media at a local level.<br><br>LFR Deployments will be conducted overtly. Zones of Recognition are clearly identified with specific signage. Information is provided (including QR codes) that will direct individuals towards the TVP LFR webpage which provides access to the LFR privacy notice and also the LFR documents that provide them with more information.<br><br>All Engagement Officers deployed in support of LFR will have access to informational material that can be distributed to members of public and those subject of Alerts (whether correct or False Positive). Engagement Officers will be present at the locations of the Zones of Recognition to respond to any Alerts but also to engage and inform the public and make information available to them in order that they can make informed | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | decisions regarding entering a Zone of Recognition. | | |
| 10 | Freedom of expression/assembly: As a result of LFR being deployed, there is a risk that it may impact the right to privacy of individuals or may deter members of the public from exercising their right to freedom of assembly and freedom of expression afforded by the Human Rights Act and that any limitation on these rights is not in accordance with the law resulting in potential legal challenge, financial claims and increase in complaints | Possible | Some impact | Medium | The Deployment Application and Written Authority Document will include an assessment of potential impacts broadly across the locations within the Zone of Recognition and members of public who may be lawfully accessing that area. There will also be consideration as to whether there may be specific groups or communities to whom the impact may be more significant. These issues will be brought to the attention of the Authorising Officer as part of the decision - making process. Wherever possible, if the Deployment is authorised, engagement should occur with groups which are potentially impacted. The Officer submitting the LFR Application and Written Authority Document will include consideration of potential impact upon human rights, potential mitigations and whether the impact is justified in achieving the policing purpose. This will also include consideration of less intrusive policing tactics to LFR and also | LFR Team and Authorising Officer | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | whether LFR could be deployed but in a less intrusive way to achieve the same policing objectives. | | |
| 11 | Threshold value: There is a risk that intervention may take place as the result of a False Alert due to the Threshold value for a Similarity Score being set too low or too high resulting in reputational damage, potential enforcement action and financial penalties, loss of public trust and increased volumes of complaints. | Remote | Serious | Low | The TVP LFR Policy & SOP prescribe an accuracy setting of 0.64. This Threshold Setting is based on the guidance provided in the National Physical Laboratory Equitability Study. There are two human fail safes in the LFR process:<br>• LFR Operator: should monitor the conditions throughout the Deployment to ensure that conditions remain suitable to maximise Positive Alerts and minimise the risk of False Alerts. Where an Alert is generated, the LFR Operator must consider if they believe the Alert to be correct and accurate;<br>• LFR Engagement Officer: following an Alert being confirmed by the LFR Operator, the Engagement Officer will then decide whether to engage with the Subject of the LFR Alert. The purpose of this Engagement is to undertake | LFR Operators and Engagement Officers | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | further checks in order to confirm if the Alert is correct through other enquiries. If the Alert is confirmed, the Engagement Officer is then responsible for determining the most appropriate outcome to dispose of the Engagement.<br><br>An individual who chooses not to enter a Zone of Recognition does not constitute a criminal offence nor does it directly trigger the use of any powers such as stop search or arrest.<br><br>The risk here is no more prevalent than in current police practices when interrogating police indices. LFR does not involve autonomous decision making. The purpose of LFR is to support TVP by locating persons in a crowd who may be sought by TVP or other law enforcement agencies, for the purpose of making further enquiries. | | |
| 12 | Excessive Watchlist: there is a risk that the images included for a Deployment may be excessive. | Possible | Some impact | Medium | For each LFR Deployment the LFR Application and separate Authorisation by the Authorising Officer will ensure that the | Authorising Officer | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | categories of persons for inclusion on the Watchlist remain proportionate to the policing objective. The assessment prior to any Deployment will include the requirements and justification of the inclusion of images in the Watchlist to ensure that the strict necessity threshold is met and there is a reasonable expectation that those individuals will be in the vicinity of the Deployment of LFR. Watchlists will be limited in size and will include accurate, verifiable images lawfully held or obtained by the police for a law enforcement purpose at the time of use. | | |
| 13 | Excessive processing: As a result of the wide-ranging capability of LFR to process large amounts of personal data there is a risk that the processing of personal data may be excessive resulting in regulatory action. | Possible | Some impact | Medium | The LFR Application document and Authorisation will consider:<br>1. The specified purpose of the deployment and the legitimate aims it seeks to address.<br>2. The placement of LFR vans and / or camera, which need to be overt and unobstructed so that members of public are aware that LFR assets are deployed.<br>3. The way in which the Zones of Recognition will be identified. These signs will only be placed when LFR is deployed so as to | Authorising Officer and LFR Team | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | make the public aware specifically that a Deployment is occurring at that time.<br>4. How the Deployment location is intrinsically linked to the policing purpose of the Deployment and geographically limited to areas where it would be deployed.<br>5. The number of LFR cameras/ vans should be proportionate to the policing objectives. The application should include consideration of other locations that may be suitable and why the proposed location is more appropriate to achieve the policing objectives including limiting the number of cameras that are being used for LFR, the impact upon the rights and privacy of members of public who may be impacted by the Deployment and safeguards and mitigations to manage the interference that may occur in order to ensure that the impact is not disproportionate to any individual, group or community.<br><br>Duration – the Deployment of LFR cameras and vans must be time limited and linked to the policing purposes for which they are | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | deployed. The timings of Deployment should be foreseeable in the context of the policing operation (for example a shoplifting operation will be limited to times when local shops are actively open and trading rather than continuing into night -time economy).<br><br>While processing involves the capture of CCTV images and the automated extracted from those images of a biometric template for comparison against the watchlist, where no potential match is identified at the applicable configuration, the biometric template of the public is automatically and almost instantly deleted. Data retention policies and procedures apply to related personal data to ensure that processing is minimised to what is strictly necessary to enable the law enforcement purposes to be carried out and to support individuals' rights of recourse. The interference with the rights of members of the public is therefore limited. | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14 | Covert surveillance: There is a risk that LFR may be deployed during covert surveillance resulting in potential unlawful processing of personal data – potential court cases, loss of opportunity to prosecute, increased complaints, reputation damage and potential regulatory enforcement action. | Remote | Serious | Low | TVP only has intentions to use LFR as an overt capability. The vans used for LFR Deployments are marked with high visibility police markings and signage that outlines that they are owned and operated by TVP for the purposes of LFR. When LFR is deployed, Zones of Recognition will be identified with signage and public engagement via TVP website and social media indicating areas wherein members of public may be subject of LFR.<br>TVP does use covert surveillance capabilities outside of LFR, only where justified, necessary and proportionate and any covert surveillance will require authority under the Regulation of Investigatory Powers Act 2000. | Authorising Officer and LFR Team. | Low |
| 15 | Similar assessments: Due to the similarity in requirements for LFR there is a risk that each Deployment and Watchlist is not subject to a full assessment documenting the rationale for inclusion of images ‘the who’, the scope of the location, duration ‘the where’ and whether the strictly necessary threshold has | Remote | Some impact | Low | TVP LFR Policy requires a suite of documents to be completed prior to any Deployment of LFR or as soon as possible in urgent cases. These documents enable the Authorising Officer to consider and authorise or refuse each individual deployment. The Authorisation will document the justification, criteria and detail around necessity, | Authorising Officer | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | been met resulting in a risk of unlawful processing and breaches of the Data Protection Act 2018 which may lead to financial claims and penalties, court cases. | | | | effectiveness and purpose of Deployment to ensure it is targeted, proportionate; intelligence led and time limited | | |
| 16 | Incomplete deletion: As a result of potential incomplete deletion exercises there is a risk that Watchlists may be compiled using custody images which should have been deleted from police systems in line with established retention and deletion procedures or from images of uncertain provenance where accuracy may be an issue (e.g. sourced from social media) there is a risk that these may lead to an unjustified Engagement and potentially cause unwarranted and unjustified damage and distress to individuals. | Possible | Serious | High | Technical measures are in place to ensure that images identified and extracted for inclusion from the police custody image database are lawfully held as required by the TVP LFR SOP. No Engagement will be made without checks being made on Possible Matches without manual intervention to further reduce any damage and distress | Automated part of watchlist compilation | Low |
| 17 | Missing persons: As a result of different scenarios in which a person may be reported as missing there is a risk that the use of LFR to locate that person may not meet the strict necessity threshold and may be unlawful resulting in potential legal | Remote | Serious | Low | Where a Deployment is being used to locate a missing person, existing TVP missing persons risk assessments (as set out in national policing guidance) will be conducted to determine the degree to which the missing person is vulnerable (a high risk missing | LFR Team | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | challenge, complaints and financial penalties or regulatory enforcement action. | | | | person) and/or poses a risk of harm and whether there is sufficient intelligence to indicate that the individual may be in a particular area. | | |
| 18 | Appropriate policy document: Where TVP has not completed an Appropriate Policy Document there is a risk that it will be in breach of section 42 of the Data Protection Act 2018 resulting in potential regulatory enforcement action and/or financial penalties. | Possible | Some impact | Medium | TVP will have in place an LFR specific Appropriate Policy Documents for LFR processing under Part 2 and Part 3 of the Data Protection Act 2018. | Senior Information Governanc e Manager | Low |
| 19 | Watchlist composition: As a result of inconsistent guidance around the use of LFR there is a risk that officers may exercise too much discretion around inclusion in the Watchlists and the location of the Deployment resulting in excessive and unlawful processing of data which may lead to legal challenge, complaints and potential enforcement action. | Possible | Serious | High | TVP LFR Legal Mandate, Policy and SOP stipulates that documentation and authorisation by a specific officer of senior rank is required for a LFR Deployment and composition of a Watchlist ensuring consistency and oversight for each Deployment, based on the existing legal framework. | Authorising Officer | Low |
| 20 | Technical failure: As a result of technical failure there is a risk that the equipment will not function correctly resulting in False Alerts or failure to identify Possible Matches resulting in | Remote | Serious | Low | A LFR System Engineer, who has been trained in the use of the equipment, including amending the settings to enhance operating parameters and reduce generation of the False Alert Rate to below | LFR Operator & LFR Team | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | potential damage and distress or threat risk and harm to others. | | | | 0.1%, will be present at all Deployments. All relevant information is logged for audit purposes. The ongoing effectiveness of TVP's use of LFR is reviewed by way of the post - Deployment review process. This will help ensure that future Deployments reflect learning identified from each Deployment, and that the use of LFR remains an effective and proportionate policing tool.<br>The LFR Operator would review any possible matches providing them with an opportunity to detect and rule out any false positive matches. | | |
| 21 | Image retention: There is a risk that subject images will be retained and used for intelligence purposes leading to unlawful processing resulting in enforcement action. | Remote | Serious | Low | The LFR system is designed to automatically delete biometric templates of individuals passing through the zone of recognition that are not matched, almost instantaneously; preventing their retention and further use.<br>Any proposal to further use LFR CCTV collected at the zone of recognition is limited in the TVP LFR Policy to: use as evidence in a criminal investigation or to investigate a compliant about officer conduct. | Automated activity in LFR system.<br>LFT Team | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | In relation to the images and biometric templates of individuals on the Watchlist and individuals in respect of whom a potential match is flagged; these biometric templates are deleted no later than 24 hours following the end of the deployment and the images in a match report are retained only for LFR purposes for up to 31 days.<br><br>The images on the watchlist are deleted after each deployment and no later than 24 hours after the end of the deployment preventing their further use. | | |
| 22 | Image quality: Images used for the compilation of Watchlists are of insufficient quality or out-of-date. | Remote | Some impact | low | The TVP LFR Policy and SOP provides that in the first instance preference should be given to images which are originated by the police (custody images), which will be of sufficient quality.<br><br>Watchlists are required to be confirmed no longer than 24 hours in advance of a Deployment.<br><br>Further, all Alerts are considered by the LFR Operator and | LFR Operator, Engagement Officer.<br><br>Automated LFR system activity. | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | Engagement Officer prior to engagement.<br><br>The LFR system will not create and load a biometric template from any images of insufficient quality. | | |
| 23 | Data retention: Data, including CCTV images, are retained for longer than necessary. | Possible | Some impact | Low | TVP has established a data retention policy in connection with the deployment of the LFR which is reflected in the TVP Appropriate Policy Document.<br><br>The application is designed to automatically delete the image and biometric template. | LFR Team | Low |
| 24 | False alerts: The use of LFR results in false matches being flagged, potentially exposing individuals to the risk of engagement. | Remote | Some impact | Low | The TVP LFR Policy explicitly identify the configurations at which the system may be deployed to ensure that any risk of false matches or discrimination is minimised. This is then overlaid by the safeguards of requiring an LFR Operator to review and affirm a potential match, and then an independent decision being made by the LFR Engagement Officer regarding whether they will engage with the matched individual. Therefore, the fact that the LFR system has flagged a potential | LFR Operator, LFR Engagement Office | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | match does not automatically lead to engagement or further action. | | |
| 25 | Engagement: The LFR Operator and Engagement Officers fail to exercise their own judgment in deciding whether to engage with an individual matched by the LFR system. | Low | Serious | Low | TVP LFR Policy and SOP require that officers involved in an LFR deployment must receive LFR training prior to being deployed, and LFR operators receive specialist training including in relation to the operation of the system, environmental and other factors which may inhibit its effectiveness and their role in exercising independent judgment in relation to the flagging of potential matches. All officers involved in the operation will also receive a pre-deployment briefing from the LFR operational commander where these points will be re-affirmed immediately prior to commencing this.<br><br>Post-deployment reviews will be carried out, which will consider if LFR Operators are overly reliant on flagged potential matches. | LFR Team, LFR Operators, LFR Engagement Officers | Low |

**If you have accepted any of the above risks <u>without</u> taking any risk reducing action you must provide a rationale for doing so in the 'Agreed Actions' column.*

## 6. Authorisation of DPIA:

DPIA2 copies will be retained by the Information Governance Team in the Joint Information Management Unit (JIMU) and within the relevant Project Management records.

### a) Approval signatories

| Item | Name / role / date | Notes |
|---|---|---|
| Risk Reducing Measures approved by **Information Asset Owner & Senior Responsible Officer:** | Detective Chief Superintendent Craig Kirby – Head of Crime & Intelligence (LFR IAO and Senior Responsible Officer):<br><br>CKirby<br>15/12/2025 | Acceptance of residual risk level and integration of any BAU actions |
| **Data Protection Officer** approval of DPIA: | Director of Data and Information & Data Protection Officer – Jason Saxon:<br><br>Jason Saxon<br>15/12/2025 | Approval of residual risk and processing to proceed. |
| **DPO advice (by exception):** | | |

| **Distribution List** | **Distribution List** | |
|---|---|---|
| **Name** | **Force** | **LFR & DPIA Involvement** |
| Jason Saxon | TVP | Data Protection Officer & Director of Data and Information & DPIA Signatory |
| D/C/Supt. Craig Kirby & Tom Kempster | TVP | Information Asset Owner Strategic LFR Lead & DPIA action owner & DPIA Signatories |
| ACC Oliver Wright | TVP | Senior Responsible Officer & DPIA Signatory |
| Abbie Newnham | TVP | Project Manager |
| D/Supt. Ben Gasson | TVP | Authorising Officer |
| James Sullivan | TVP | LFR Silver Commander for 22/12/25 deployment & DPIA action owner |
| Sharon Warwick | TVP | Senior Information Governance Manager |

### b) Residual high risks (complete only if there are any 'high' residual risks):

| Item | Decision / Name / role / date | Notes |
|---|---|---|
| **SIRO decision on referring to ICO:** | N/A | If not referring to ICO SIRO to record rationale |
| **SIRO Rationale:** | | |
| **Date and name of person referring DPIA to ICO:** | N/A | As required by law if any high residual risks remain. |
| **Summary of ICO advice:** | | |

**c) Accountability – update of governance records and 'records of processing':**

| Accountability Task | IGO to date & sign when task complete | IGM to date & sign when checked complete |
|---|---|---|
| Information Asset Register updated | 05/12/2025 | Senior Information Governance Officer |
| Privacy Notice reviewed to see if new processing needs adding. | 12/12/2025 - LFR Specific Privacy Notice produced and published on TVP website (LFR Page) | Senior Information Governance Officer |
| Trigger points for action tracking agreed and in DPIA Register | No outstanding actions | N/A |
| ISA Catalogue / DPC Register updated if any new ISAs / DPCs. | Added 01/09/2025 | Checked 09/09/2024 & 03/12/2025 - Senior Information Governance Manager |

## 7. Review / Update of DPIA:

### a) Record Of Review

| Review Date | Reviewing IGO | Reason for Review |
|---|---|---|
| | | |
| **Record: Has the scope and nature of the processing changed? (Detail yes or no below)** | | |
| | | |
| | | |
| | | |
| **Record whether the DG is happy that the risks continue to be sufficiently mitigated? (If no detail below)** | | |
| *Please Note: If there are any new risks / actions or any changes to existing ones must be captured in risk table below:* | | |

### b) Changes to Data Protection Risks and Actions

| | **Describe the <u>problem</u> that is the risk, the <u>vulnerability</u> that creates the problem and the <u>potential impact</u> on individuals.** . | **Likelihood of harm** Remote, possible or probable. | **Severity of harm** Minimal, some impact or severe. | **Risk score** Low, medium or high. | **Agreed action** Detail to action that will reduce the risk | **Action Owner & due date** | **Residual Risk score** Low, high or medium. |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

**c) Review Sign Off**

| DPIA Review - Signatories | Name / role / date | Notes |
|---|---|---|
| **Information Asset Owner or Data Guardian.** | | IG will advise on correct signatories according to DPIA review guidance document |
| **JIMU (IGO, IGM or DPO)** | | IG will advise on correct signatories according to DPIA review guidance document |
| **DPO advice (by exception):** | | |

**d) IG Checklist**

| DPIA Review Checklist | Date | Signature |
|---|---|---|
| Next DPIA Review Date | | |
| DPIA Register Updated | | |
| IAR Register updated (if applicable) | | |