Thames Valley Police

Privacy Notice for Use of Live Facial Recognition

INTRODUCTION

This Live Facial Recognition (LFR) specific Privacy Notice has been created to make it easier for you to understand what personal data Thames Valley Police (TVP) may process about you, how and why it will be used in connection with the use of live facial recognition. It is a requirement of the Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR).

It is subordinate to, and should be read in conjunction with, the TVP's high-level Privacy Notice, which can be accessed from the home page of TVP's internet site: Privacy notice | Thames Valley Police. The high-level Privacy Notice provides you with complete details of the rights you have relating to the broader personal data we may hold about you now and any personal data we might collect about you in the future.

If you do not have digital access and require a physical copy of the high-level Privacy Notice please contact the address on page 7, section 6 to request a copy.

PROCESSING OF PERSONAL DATA IN RELATION TO LIVE FACIAL RECOGNITION

The TVP LFR deployments will be delivered using specialist equipment operated by the Thames Valley Police and Hampshire & Isle of Wight Constabulary collaborated Joint Operations Unit, LFR Team. During the preparation and delivery of a specific LFR deployment the LFR Team will be acting under the direction and control of the Chief Constable (as data controller) that is requesting the deployment in their force, according to the arrangements set out in their own LFR Policy and Standard Operating Procedure and other associated LFR impact assessments and documents. 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.

TVP's strategic intention for using its NEC's NeoFace live facial recognition technology is to: to prevent and detect crime, apprehend and prosecute offenders, support the administration of justice and help protect the vulnerable.

Facial Recognition is a technology capable of comparing a human face from a digital image against a database of faces. From a digital image, facial recognition technology analyses key facial features and generates a biometric template of these features. It then compares them against the biometric template of known faces in a database, generating possible matches where both images are highly likely to be the same person. The processing of the biometric template is classified as 'sensitive processing' when processed for law enforcement purposes under the DPA 2018, and is classified as 'special category data' when processed under the UK GDPR.

Live Facial Recognition (LFR) compares a live camera feed of faces collected from specific LFR CCTV cameras (set up at the location the LFR is deployed) against a predetermined database of images (called a watchlist) to find a possible match that generates an alert.

TVP will use LFR technology for the following policing objectives:

- 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.
- 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.
- 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.
- 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.

The watchlist is composed of images already held by the police, of persons who have been previously arrested on suspicion of committing an offence. On occasion, the image may have been sourced from outside of TVP such as for a high risk missing person believed to be at risk of, or pose a risk of, serious harm. The watchlist of images is created within the 24 hours before each LFR deployment and the persons included are specifically selected according to the policing objective that a particular LFR deployment is expected to address.

In the small geographical area where LFR is deployed, called the 'recognition zone', is where the LFR police vans hosting the live cameras will be set up to scan the faces of people passing through the recognition zone. The recognition zone will be clearly marked with signage ahead of the start of the zone so that persons can take an alternative route if they wish to do so. Leaflets and QR codes at the recognition zone will allow people to access more information about LFR if they choose to do so via the TVP website: Live Facial Recognition Technology | Thames Valley Police

TVP will also publish any planned use of LFR, on its website and social media channels, a minimum of 7 days ahead of any deployment.

TVP will carry out intelligence led analysis to select: persons on the watchlist, the location of the recognition zone and how the LFR technology will be set up at the deployment location. For each separate deployment of LFR we will carefully consider the privacy intrusion and impact on other rights of persons passing through the recognition zone to ensure it is at a proportionate level to the societal benefits of using LFR technology in a targeted way to prevent and detect crime, apprehend and prosecute offenders, support the administration of justice and protect the most vulnerable. TVP will only use LFR technology when other less privacy intrusive capabilities have not been successful or where we have strong reason to believe they would not be successful.

The LFR cameras at the recognition zone stream facial images to the LFR system. These images are compared against the images on the watchlist. When the LFR system finds a likely match an alert is generated.

An officer then compares the two images side by side to establish whether they believe them to be the same person, and if so they then decide whether to recommend that another officer speaks to the person, with that officer also exercising their independent judgement. We will explain why we have chosen to speak with someone and give them an information leaflet with contact details if they have further questions or concerns, which supplements existing mechanisms.

People who pass through the recognition zone and are scanned by the LFR cameras, are not identified unless they are also on the watchlist. No other personal identifiers are collected via the live LFR cameras in addition to the live feed image and biometric template.

The generated biometric template of persons passing through the recognition zone will be deleted in less than a second where there has been no flagged match to a person in the watchlist. Other images used in LFR will be retained for a minimum specified period afterwards and deleted when no longer needed. The specific retention periods are shown in section 9 of this privacy notice.

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.

More information about how TVP will use LFR can be found our dedicated LFR web page.

PRIVACY INFORMATION

1. TVP Data Controller:

The data controller is the person in an organisation who determines why (the purpose) personal data needs to be processed. The data controller for TVP is the Chief Constable. The data controller can be contacted at:

Chief Constable of TVP
c/o Data Protection Officer

Thames Valley Police
Public Access Office
Oxford Road
Kidlington
OX5 2NX

Email: publicaccess@thamesvalley.pnn.police.uk

Data protection legislation reference: DPA18: section 44(1)(a), UK GDPR: article 13(1)(a).

2. TVP Data Protection Officer:

The Data Protection Officer is a TVP employed data protection expert who informs, advises, and monitors TVPs data protection compliance. The Data Protection Officer can be contacted at:

Data Protection Officer
Thames Valley Police
Public Access Office
Oxford Road
Kidlington
OX5 2NX

Email: publicaccess@thamesvalley.pnn.police.uk

Data protection legislation reference: DPA18: section 44(1)(b), UK GDPR: article 13(1)(b).

3. Types of personal data processed by LFR:

The categories or types of personal data processed by LFR are:

- Watch list: digital custody or other images, limited identification details, mechanical facial template.
- Recognition zone / live camera feed: digital citizen images, mechanical facial template.
- Records / logs of LFR deployment: metrics of number of faces scanned, alerts, interventions and arrests (non-personal data). Details of police officers on LFR deployment.
- Arrest: for any alerts resulting in a person being located and arrested; details of their arrest (criminal data).

The categories or types of people whose personal data may be processed by LFR are:

- Watchlist:
    - persons wanted on court warrant, recalled to prison,
    - outstanding suspects of criminal offences,
    - persons 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,
    - high risk missing persons.
- Recognition Zone / live camera feed: citizens of any age who are in the deployment area and walk through the recognition zone.

- Deployment - Police Officers: TVP Engagement Officers and LFR System Operators.

4. The objectives for deploying LFR:

TVP has a common law duty to prevent and detect crime, set out as the 'policing purpose' in the Statutory Code of Practice on Police Information and Records Management:

- Protecting life and property.
- Preserving order.
- Preventing the commission of offences.
- Bringing offenders to justice.
- Any other police duty or responsibility arising from common or statute law.

More specifically TVP will use LFR to locate:

- Persons wanted on court warrant, recalled to prison.
- Outstanding suspects of criminal offences,
- Persons 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.
- High risk missing persons.

5. Your data rights under the DPA18 and UK GDPR:

Question	**Answer**	**DPA & UK GDPR Reference**
1. Who is the Controller (the person who determines the purpose and means by which your personal data is processed) and what are their contact details?	The Controller is: Chief Constable of TVP c/o Data Protection Officer Thames Valley Police Public Access Office Oxford Road Kidlington OX5 2NX Email: publicaccess@thamesvalley.pnn.police.uk	Section 44(1)(a) Article 13(1)(a)
2. What are the contact details of TVP's Data Protection Officer?	Data Protection Officer Thames Valley Police Public Access Office Oxford Road Kidlington OX5 2NXEmail: publicaccess@thamesvalley.pnn.police.uk	Section 44(1)(b) Article 13(1)(b)

3. What types of personal data will you be processing?	Categories of data: • Watch list: digital custody or other images, limited identification details, mechanical facial template • Recognition Zone / live camera feed: digital citizen images, mechanical facial template. • Records / logs of LFR deployment: metrics of number of faces scanned, alerts, interventions and arrests (non-personal data). Details of police officers on LFR deployment. • Arrest: for any alerts resulting in a person being located and arrested; details of their arrest (criminal data). Categories of data subject: • Watchlist - persons: wanted on court warrant, recalled to prison, outstanding suspects of criminal offences, in breach of bail conditions / court orders due to their presence in the LFR location, high risk missing persons. • Recognition Zone / live camera feed: citizens of any age who are in the deployment area and walk through the recognition zone. • Deployment - Police Officers: TVP Engagement Officers and LFR system operators.	
4. For what purpose(s) is my personal data intended to be processed by TVP?	TVP has a common law duty to prevent and detect crime, set out as the 'policing purpose' in the Statutory Code of Practice on Police Information and Records Management: • Protecting life and property. • Preserving order. • Preventing the commission of offences. • Bringing offenders to justice. • Any other police duty or responsibility arising from common or statute law. More specifically TVP will use LFR to locate: • Persons wanted on court warrant, recalled to prison. • Outstanding suspects of criminal offences, • Persons 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. • High risk missing persons.	

	• Analysis / evaluation into the efficacy and equitability of LFR systems.	
5. What are my rights under the DPA?	You have the following rights under the DPA 2018: • Right of access to your personal data • Right of rectification of your personal data • Right of erasure of your personal data or the restriction of its processing • Right to lodge a complaint with the Information Commissioner • Right not to be subject to automated decision making. Persons included on the watchlist because they are a high risk missing person at risk of, or poses a risk of, serious harm will enjoy equivalent rights as listed above, but under the UK GDPR plus the below additional right: • Right to object to the processing of your personal data. The operation of LFR technology does not involve any automated decision making. Where the LFR system alerts to a potential match, the two images are reviewed side by side by the LFR system operator. Where the LFR Operator believes there is a match they pass it to an Engagement Officer will make the decision on whether to engage with the individual.	Section 44(1)(d)(i) Section 45 Section 44(1)(d)(ii) Section 46 Section 44(1)(d)(iii) Section 47 Section 44(1)(e) - Section 51 Section 49-50 Article 12-19 and 22 Article 21
6. How can I exercise my data rights listed at 5 above?	Full details of those rights and how to exercise them can be found in TVP's high-level privacy notice, which can be found on the home page of the TVP website. It can also be obtained from: Joint Information Management Unit	

	TVP Oxford Road Kidlington OX5 2NX Email: publicaccess@thamesvalley.pnn.police.uk Website: Ask for, delete or change information | Thames Valley Police	
7. Is there any other information that is necessary to enable me to exercise any of rights listed at 5 above?	You will need to provide 2 forms of identification and if your request is about an image of you, one of those will need to be a form of photo ID. If you are enquiring about a CCTV image of you captured by the LFR cameras at the recognition zone, it might help us to locate you in the CCTV frames you were in, if you can provide the following: • The date and an approximate time you would have been walking through the LFR recognition zone. • Where the LFR recognition zone was located. • Any recollection of the visible outer clothing you were wearing at the time.	Section 44(2)(d) Section 44(3)(a) Article 12(6)
8. What is TVP's legal basis for processing my personal data?	**Personal data lawful bases under DPA 2018**: TVP's use of LFR to locate persons: wanted on court warrant, recalled to prison, outstanding suspects of criminal offences, in breach of bail conditions / court orders due to their presence in LFR location, high risk missing persons. The processing must also be 'based on law' and is underpinned by: • Section 64A of the Police and Criminal Evidence 1984 allows for custody images to be used for the prevention and detection of crime. • Common Law Policing Purpose of protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice, and any duty or responsibility of the police arising from common or statute law. **Sensitive processing lawful basis under DPA 2018:**	Section 44(2)(a) Section 35(2)

	• The mechanical template created from images from the watchlist and live LFR camera feed is biometric data which when processed for the law enforcement purposes is classed as sensitive processing. It requires the processing to be strictly necessary and an additional lawful basis to enable lawful processing. The processing will be necessary for one of the following, dependant on deployment reasons and watchlist inclusion:	Section 35 (5)
	○ Statutory purposes. ○ Administration of justice. ○ Protecting vital interests. ○ Safeguarding of children and individuals at risk. ○ Manifestly made public by the individual. ○ Necessary for or in connection with legal proceedings.	DPA 18 Schedule 8 (1,2, 3,4,5& 8)
	Personal data lawful bases under UK GDPR:	
	TVP's use of LFR to locate missing persons who are at risk of, or pose a risk of, serious harm, or to carry out research and analysis on the accuracy and efficacy of LFR, will be subject to the UK GDPR.	Article 6(1)(c), (d) & (e)
	• Processing is necessary for compliance with a legal obligation to which the controller is subject. • Processing is necessary to protect the vital interests of the data subject or another natural person. • Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	
	Special category data lawful basis under UK GDPR:	
	To locate missing persons at risk of harm: • Processing is necessary to protect the vital interests of the data subject or of another natural person where the data	Article 9(2)(c)

	subject is physically or legally incapable of giving consent • Processing relates to personal data which are manifestly made public by the data subject. • Processing is necessary for reasons of substantial public interest, on the basis of law and meets one of the following conditions: ○ the 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 ○ the processing is necessary for the equality of opportunity or treatment ○ processing is necessary for the purposes of safeguarding children and individuals at risk An Appropriate Policy Document outlining how TVP's use of LFR meets the principles of the DPA 18 and UK GDPR can be found on our dedicated LFR web page. **Criminal data lawful basis under UK GDPR:** 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 same conditions stated above in the section detailing special category data processed under UK GDPR.	Article 9(2)(e) Article 9(2)(g) Schedule 1 para. 6 Schedule 1 para. 8 Schedule 1 para. 18 Section 35(5)(c) DPA 18 Schedule 1, Part 4
9. How long will my personal data be retained by TVP?	**Watchlist:** • The images that populate the watchlist will usually be copies of images already stored in our source policing systems. The images in the source system will be retained in line with retention framework set out in the College of Policing Authorised Professional Practice on Information Management: Review, retention and disposal | College of Policing (APP). Only images lawfully retained will be drawn from the source system for the purposes of LFR. • The copies of images on the watchlist and the biometric templates will be removed from	Section 44(2)(b) Article 13(2)(a)

	the LFR system and any removable media used to transfer them within 24 hours of the conclusion of the deployment. • A list of metadata of persons who were on the watchlist, (but not the watchlist images/templates), deleted within 24 hours of the end of the deployment. **CCTV Footage / Live Camera Feed:** • CCTV footage recorded throughout deployment will be retained for 31 days and disposed of in line with national CCTV retention guidelines, unless retention is required to: o Investigate a complaint or data subject request to exercise their data rights. o Support a related investigation or prosecution. o Is identified within that time period as being needed for another criminal investigation (eg: a murder investigation reviews footage as suspect of witness believed to be in the area of the recognition zone at a relevant time). • Image and facial template used to compare to the watchlist: o No match / alert = automatic instant deletion. o True or false alert / match = deleted within 24 hours of the conclusion of each deployment. **LFR Deployment Logs – personal data:** • Deployment Record: o as soon as practical but within 31 days. o for retrospective review. • Match Report: o as soon as practical but within 31 days. o for retrospective review of any facial match alerts. **LFR Deployment Logs – no personal data:** • These documents are specific to each deployment and are retained for 6 years after each specific deployment.	

	LFR Policies & guidance: • These will not contain personal data and will be retained for at least 6 years after TVP has ceased using LFR technology.	
10. Who could TVP disclose my personal data to?	TVP will not routinely share your LFR personal data except where we are required to do so when working with other police forces, law enforcement bodies, and / or other agencies to assist TVP in discharging its common law policing powers. This action will not involve the sharing of biometric data but may involve sharing personal data.	Section 44(2)(c)