Classification	OFFICIAL
Handling Instructions	No restriction on distribution
Disclosable (FOI / Publication Scheme)	Yes

BRITISH TRANSPORT POLICE

Appropriate Policy Document –

Sensitive Processing Under Part 3 of the Data Protection Act 2018 (Live Facial Recognition Deployments)

Introduction

British Transport Police is a 'competent authority' for law enforcement processing, as defined at Section 30 and Schedule 7 of the Data Protection Act 2018 (DPA 2018)

Part 3 of the DPA 2018 outlines the requirement for an Appropriate Policy Document (APD) to be in place when a competent authority is processing sensitive personal data for law enforcement (LE) purposes.

Sensitive processing is defined in Part 3 section 35(8) and is equivalent to GDPR special category data. This includes: (a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; (b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual; (c) the processing of data concerning health; (d) the processing of data concerning an individual's sex life or sexual orientation.

Processing for LE purposes must comply with the data protection principles outlined in Part 3 of the DPA 2018. Specifically, the first data protection principle (section 35) states that processing for LE purposes must be lawful and fair.

Additionally, processing of sensitive personal data for LE purposes may only take place if the processing:

- is based on the consent of the data subject - section 35(4) and at the time when the processing is carried out, the Controller has an APD in place; or

- is strictly necessary for the LE purpose and meets at least one of the conditions in Schedule 8 and at the time when the processing is carried out, the Controller has an APD in place- section 35(5).

Sensitive processing under Part 3 DPA 2018 for LFR will not rely on consent. Although section 35(4) permits consent in theory, consent cannot be freely given in a policing context due to the clear imbalance of power between police and the public, and therefore cannot provide a valid lawful basis for LFR. All sensitive processing for LFR is carried out solely under section 35(5) DPA 2018. This requires that processing is:

• strictly necessary for a law-enforcement purpose under section 31;

• supported by at least one relevant Schedule 8 condition (Statutory etc purposes; Administration of justice; Vital interests; Safeguarding of children and individuals at risk);

• accompanied by a compliant Appropriate Policy Document under section 42.

No element of LFR activity relies on, or seeks to obtain, the consent of data subjects.

This document demonstrates that the processing of sensitive data is compliant with the requirements of Part 3 section 42 of the DPA 2018.

Description of Data Processed

Live Facial Recognition is a real-time deployment of Facial Recognition Technology, which compares a biometric template extracted from live camera feed(s) of a subject's face against an image on a pre-determined watchlist in order to identify and locate persons sought by the Police.

The image reference database will contain custody images previously arrested by the police. Exceptionally and with high level authorisation, an image may be used from a non-police source

Lawful Basis

Sensitive processing in the course of a Live Facial Recognition deployment may be carried out under a number of conditions listed at Schedule 8 of the DPA, including:

- Paragraph 1 – Statutory etc. Purposes
- Paragraph 2 – Administration of Justice
- Paragraph 3 – Protection of an Individual's Vital Interests
- Paragraph 4 – Safeguarding of Children and Individuals at Risk

Procedures for Ensuring Compliance with the Principles in accordance with Part 3, Chapter 2 of the DPA 2018

Principle (1): Lawfulness and Fairness

The lawfulness of the sensitive processing carried out by British Transport Police derives from our official functions as a Police Force.

Sensitive Processing will be carried out when necessary for the law enforcement purpose and in reliance on one of the Schedule 8 conditions detailed above.

British Transport Police provides fair processing information to data subjects by means of written notices published on our website. Extensive information about Live Facial Recognition is made available on the BTP website, including policy, legal mandate, data protection impact assessment and equality impact assessment. This will be enhanced by public facing announcements of deployments on media and social media channels and proactive publication of the outcomes and key performance metrics for each deployment. The deployments will be overt and highly visible, and information will be available to railway users passing through the areas from officers on the scene, written material, or via QR codes that will be displayed along with signage.

No-one will be forced to enter the zone of recognition at an LFR deployment. There will be alternative routes available for railway users to follow without entering the zone of recognition which will be clearly signposted and equally accessible so the individual does not incur any detriment or inconvenience from avoiding the zone of recognition.

Principle (2): Purpose Limitation

British Transport Police are authorised by law to carry out sensitive processing when necessary and proportionate for the law enforcement purposes. We will only use data collected for a law enforcement purposes. for purposes other than law enforcement where we are authorised by law to do so.

The Policy for deployment of Live Facial Recognition technology sets out the use cases where it may be used and ensures that every deployment must be specifically authorised for a specific purpose. Any image included on a watchlist must be endorsed by an intelligence case and comply with the use cases set out in the Policy.

Live facial recognition deployments are undertaken using a standalone system that is not linked to other Force systems or databases. Individuals will be aware of the nature and purpose of the deployment by announcements of future deployments and available information at the location of the deployment.

The segregation and retention policies for data created or collected in the course of a deployment ensure that sensitive data may not be further used for an incompatible purpose.

Principle (3): Data Minimisation

British Transport Police only conducts sensitive processing when necessary for the law enforcement purposes. Data is retained in line with documented retention schedules which ensures that personal data must be adequate, relevant, limited and not excessive in relation to the purpose for which it is processed. The processes are in place for records to be reviewed and assessed for continued retention.

A data protection impact assessment has been undertaken for the use of Live Facial Recognition technology which sets out a number of mitigations to any risk to the rights or freedoms of data subjects who may pass through a location where a deployment is being undertaken.

Principle (4): Accuracy

A new watchlist is generated for every LFR Deployment and each image included on a watchlist must be assured as being lawfully held, assessed as being of sufficient quality and backed by an intelligence case to justify inclusion.

The watchlist must be finalized and uploaded no more than 24 hours before a deployment. This ensures that the watchlist will be accurate and up to date and that officers acting on the basis of an alert will have the most up to date information available to them.

Principle (5): Storage Limitation

Where the LFR system does not generate and alert, that a person's biometric data is immediately deleted by the LFR software.

The LFR watchlist is deleted as soon as reasonably practicable, and in any case within 24 hours, following the conclusion of the deployment.

Where the LFR system generates an alert, all related biometric data is deleted as soon as practicable and in any case within 24 hours of the deployment, except to the extent that:

- Personal data is retained in accordance with the Data Protection Act 2018, Management of Police Information (MOPI) and the Criminal Procedures and Investigations Act 1996.
- Personal data is retained in accordance with BTP's complaints/conduct investigation policies.

All CCTV footage (not biometric data) generated by the LFR cameras is deleted within 31 days, except to the extent that the footage is retained:

- In accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996.
- In accordance with The Police (Conduct) Regulations 2020. https://www.legislation.gov.uk/uksi/2020/4
- In accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty – any requirement to retain the Closed Circuit Television (CCTV) footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

Principle (6): Integrity and Confidentiality

The LFR system includes a number of physical and technical security measures. These include:-

- images are transferred onto the LFR system via a USB device using an AES 256-bit hardware encrypted Integral USB 3.0 Crypto full disk hardware encryption engine;
- the LFR system is a closed circuit TV system that implements defences in depth principles to protect the application and related data;
- the LFR system is physically protected when in use and securely wiped following each Deployment;
- role based access controls with limited user permissions are implemented on the LFR system;
- the LFR application is connected to mobile devices using a private access point with three levels of protection;
- Specific IP addressing, password access to the access point, and password access to the mobile App.
- The mobile App has a RESTful API and will be covered by SSL;
- the Dashboard and RESTful API are secured with SSL and TLS by default; and all connections are directed through HTTPS;
- a full audit is maintained of all user initiated actions undertaken during the course of a Deployment;
- technical issues with the LFR system will be dealt with by LFR System Engineers deployed on the operation.
- Remote support from the algorithms developers (NEC) or LFR partners (Bedroq) support desk can be sought by LFR engineers if a fault or issue occurs with the LFR system.

The Accountability Principle

British Transport Police has in place technical and organizational safeguards to meet the requirement of accountability.

We have appointed a Data Protection Officer who reports directly to our Chief Officer Group. We have a dedicated Information Management department and a 'data protection by design and default' approach built into our processing, project management and procurement procedures. This ensures that we carry out Data Protection Impact Assessments and other risk and security assessments as applicable in relation to any potential high risk processing, have

written contracts in place with any processors used and implement appropriate security measures.

We maintain appropriate documentation of our processing activities, including:

- Record of processing activities maintained by each business area.
- Information detailed in appropriate privacy notices.
- A suite of policies relating to Data Protection and related areas.

In relation to Live Facial Recognition, a suite of policy and assurance documentation has been published on the BTP website.

Retention and Erasure Policies

British Transport Police has adopted the retention rules outlined in the Authorised Professional Practice on the Management of Police Information (MoPI) and has in place record retention schedules which show how long records are retained. We have records management policies which cover the principles of review, retention and disposal and also have a policy specifically for requests for record deletions.

Our Contact Details and Data Protection Officer

Our Information Management Unit manages our data protection compliance. Our Data Protection Officer is the Head of Information Management.

We take our data protection responsibilities seriously. We take great care to ensure we process your personal data properly to maintain your trust and confidence. You can contact our Data Protection team or our Data Protection Officer if you have any questions or concerns about how we process your personal data.

Post:

Data Protection & FOI Team,
British Transport Police,
Second Floor,

3 Callaghan Square,

Cardiff,

CF10 5BT

Email: dataprotection@btp.pnn.police.uk

Date of last update and changes

We last updated this Appropriate Policy Document on 31st January 2025. We keep this privacy policy under regular review and update it from time to time.