Data Protection Legislation

Appropriate Policy Document (APD)

Policy on Processing of Special Category Data under Part 2 Data Protection Act 2018 and Article 9 of the UK-General Data Protection Regulation

Essex Police Live Facial Recognition (LFR)

Processing biometric data, for the purpose of uniquely identifying an individual.

August 2024

Version 1.0

Version Control

Version	Date	Author	Purpose
V1.0	08/08/2024	Michelle WATSON	

ESSEX POLICE
Protecting and serving Essex

Introduction

This policy document has been produced in accordance with Essex Police obligations under the UK-General Data Protection Regulation (UK-GDPR). It should be read alongside the Essex Police Privacy Notice. Data protection policy specific to LFR is also to be found in the LFR Policy and Data Protection Impact Assessment (DPIA).

As part of Essex Police common law powers to protect and preserve life and property, we process special category data in accordance with the requirements of Article 9 of the UK-GDPR and supplemented by Part 2 and Schedule 1 of the Data Protection Act 2018 (DPA).

Our processing of special category and criminal offence data for law enforcement purposes is not covered in this document. Processing for law enforcement purposes is carried out by us in our capacity as a competent authority and falls under Part 3 of the DPA and is subject to a separate APD.

This Policy Document

The Schedule 1 DPA conditions for processing special category data require us to have an APD in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 UK-GDPR (relating to processing of personal data) and policies regarding the retention and erasure of such personal data. This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA (APD and Additional Safeguards)

Description of Data Processed

The special category data processed utilising LFR:

• Biometric data for the purpose of uniquely identifying a natural person.

LFR Is a real-time deployment of facial recognition technology (FRT), 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.

The Watchlist for LFR is primarily a subset of the Essex Police custody image dataset but may also include other lawfully held images.

All Watchlist images will have a biometric template created (special category data) at the point of enrolment to the FRT application.

All faces compared against the Watchlist have a biometric template created (special category data).

Biometric data used to uniquely identify an individual is considered to be special category data. For this processing we will be collecting the personal data of members of the public which will include an image that may be utilised by extracting a biometric template from it for the purposes of uniquely identifying them. Where this data does not generate an Alert against that held on the Watchlist it will not be further processed and biometric data of the natural person permanently deleted once this comparison has been completed. No other personal identifiers are collected in addition to the biometric image.

We maintain a record of our processing activities in accordance with Article 30 of the UK-GDPR.

UK-GDPR conditions for processing special category data

Essex Police processes special categories of personal data under the following GDPR Articles:

Lawful conditions for processing special categories of personal data under GDPR:

Article 9(2)(a) – explicit consent

In the limited circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is a freely given, fully informed affirmative action which is recorded and managed to ensure the facilitation of individual rights, including withdrawal of consent. Processing under this article will be limited to the below example.

E.g. processing participating staff images for the purpose of validating LFR.

Article 9(2)(g) - Substantial Public Interest

E.g. Identification of missing persons or safeguarding children or vulnerable individuals.

Section 10 DPA supplements Article 9 GDPR, requiring the following conditions of Schedule 1 to be satisfied where Essex Police relies on Article 9(2)(g).

Schedule 1 DPA Condition for processing Special Category Data

We process special category data for the following purposes identified in paragraphs 6 and 18 of Part 2 of Schedule 1 (substantial public interest conditions):

• Paragraph 6 – Statutory etc and government purposes - exercise of function conferred upon a person by enactment or rule of law. This condition is met if the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law AND for reasons of substantial public interest.

The police have a common law duty not only to prevent and detect crime but to protect the public and preserve life and property: this is the relevant 'rule of law' pursuant to which the processing is necessary for the police to exercise their functions. The processing is also necessary for reasons of substantial public interest, that is, the safety and protection of the public. In determining necessity, Essex Police will always consider whether less intrusive measures can be used without compromising the objective and the interests of the individual balanced against the interests of the community.

• Paragraph 18 - Safeguarding of children or individuals at risk

This condition is met if the processing is necessary for the purposes of protecting an individual under 18 (or over 18 and at risk i.e. vulnerable for reasons defined in the paragraph 18) from neglect or physical or emotional harm or protecting the physical, mental or emotional well-being of an individual, where the consent cannot reasonably be given or obtained in the relevant circumstances, and the processing is necessary for reasons of substantial public interest.

Procedures for ensuring compliance with the principles in Article 5 UK-GDPR

Accountability Principle (Article 5(2) UK-GDPR)

Essex Police have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:
• The appointment of a data protection officer who is responsible for data protection in relation to LFR and who reports directly to the Chief Officer team for Essex Police.
• Taking a 'data protection by design and default' approach to our activities.
• Maintaining documentation of our processing activities.
• Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
• Implementing appropriate security measures in relation to the personal data we process.

• Carrying out DPIA's for our high-risk processing.

We regularly review our accountability measures and update or amend them when required.

Principle (a): lawfulness, fairness, and transparency

Processing personal data must be lawful, fair, and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, and this policy document. The DPIA for LFR gives specific detail regarding the way in which data is processed and how the measures we have in place ensure that the processing is lawful, fair and transparent. Relevant documentation and additional information about how LFR is used is available to the public at Live facial recognition | Essex Police

The processing of data by LFR for the purposes of substantial public interest is necessary on the basis of Essex Police common law functions which might fall outside strict law enforcement purposes (for which data would be processed under Part 3 DPA); it is proportionate to the aims pursued (see above conditions for processing where we have explained the legislative conditions on which Essex Police relies and examples of purposes that meet each of those conditions). Essex Police practices respect the right to data protection and employs suitable and specific measures to safeguard the fundamental rights and interests of the data subject in so far as is necessary and lawful in a democratic society. Essex Police will always consider whether the use of LFR is strictly necessary (i.e. taking into account consideration of other measures not involving the processing of special category data and whether they could achieve the same outcome) and will ensure that at least one relevant UK-GDPR condition or processing of specific category data and attendant DPA requirements are satisfied.

Principle (b): purpose limitation

We process personal data where it is necessary for the purposes of protecting the public, fulfilling our common law functions to preserve and protect life and property, and to safeguard children and vulnerable persons, all in the substantial public interest as explained above.

This data will not be further processed for purposes which are incompatible with the purpose for which it was collected.

We will only share this personal data with another organisation where there is a legal power to do so and in accordance with data protection requirements.

This means that in particular we consider what we seek to achieve, whether there are alternative measures which would not involve processing special category data but which would achieve substantially the same outcomes, and the same or lesser impact on individuals and the community.

If we are sharing data collected for one of our lawful purposes with another controller, we will document that they are authorised by law to process the data for a lawful purpose under data protection legislation and that the processing is necessary and proportionate to that purpose.

We will not process personal data for purposes incompatible with the original purpose for which it was collected.

We will not process data collected for a law enforcement purpose (for which, see the APD for Part 3 DPA) for a purpose that is not a law enforcement purpose unless the processing is authorised by law and meets the requirements of the UK-GDPR and DPA.

Principle (c): data minimisation

We process personal data necessary for the specified purposes and ensure it is adequate, relevant, and not excessive in relation to the purpose(s) for which it is processed. The information we process is only that which is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it. An example would be if another individual's image was captured that was not subject to an enquiry.

In addition, we require the data to be of an acceptable quality for comparison e.g., an image of a face with a minimum of fifty pixels between the eyes of the subject. For LFR, this is sufficient facial biometric data to compare against a Watchlist.

Ultimately an LFR Operator will determine whether a match is made between the probe and candidate image after an Alert. This is an additional safeguard against identification of similar but incorrect individuals.

Principle (d): accuracy

We will retain the probe image of the individual and biometric template for no longer than is necessary for non-law enforcement purposes for which it is processed. The source system (Athena) image will be maintained in accordance with the Management of Police Information (MOPI). The probe image and related biometric template will be automatically and immediately deleted (where no alert is generated). For images where an alert is generated the probe image and biometric template will be deleted as soon as practicable and within 24 hours. The comparison process takes a matter of seconds. After an Alert is generated consideration will be undertaken by an LFR Operator. Where we become aware that personal data contained within a Watchlist is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision and take appropriate steps to inform the data subject. Where we erase or rectify personal data we will inform any recipients with whom we have shared that data.

Principle (e): storage limitation

All special category data processed by us using LFR for non-law enforcement purposes will be deleted immediately or in any case within 24 hours of the deployment. The probe image and related biometric template will be automatically and immediately deleted (where no alert is generated). For images where an alert is generated the probe image and biometric template will be deleted as soon as practicable and within 24 hours. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

In limited circumstances images and biometric templates will be used for research purposes and evaluation of the effectiveness and performance of LFR. Where possible personal data will be anonymised or pseudonymised. Personal data being processed for research purposes will be done so in accordance with a data sharing agreement requiring sufficient guarantees around the security of the information in transit and at rest, including physical, personnel and technical security measures. Such measures will be subject to scrutiny by Force Information Security Officers and the Data Protection Officer.

Principle (f): integrity and confidentiality (security)

Personal data processed by LFR is processed within our accredited secure computer network which is located locally within Essex Police force area in accordance with national and local security policies. Hard copy information is processed in line with our information management policies. Data Protection Polices are applied from inception of initiatives to ensure legislative compliance with our data protection obligations and to determine appropriate levels of technical and organisational safeguards and controls when processing personal data and sensitive data. All of our security measures are designed to protect against unauthorised or unlawful processing, accidental loss, destruction or damage.

Our electronic systems and physical storage have appropriate access controls applied including for example, multi-factor authentication to access mobile devices (in the form of multiple sign in/access codes/facial recognition etc), password protection, encryption and locking mechanisms. Information Asset Owners are responsible for ensuring that all information management processes are applied to information and there is a continuous cycle of review and information risk identification and management. LFR has also been subject to a robust DPIA.

All staff receive basic data protection training must undertake annual mandatory training for managing information. Specific training is provided to officers working with LFR which is supplemented with bespoke Standard Operating Procedures.

The systems we use to process personal data allow us respond to individual rights requests and to erase or update personal data at any point in time where appropriate and where personally identifiable information regarding data subjects is held. All events which take place on operation systems are recorded on an audit log which enables identification of the action executed, when it was carried out and by whom.

Retention and Erasure

Particular to LFR Application

• where the LFR application does not generate an Alert, then a person's Biometric Template and Probe Image is immediately automatically deleted.
• where the LFR system generates an Alert all personal data (to include Biometric Template and Probe Image) is deleted as soon as practicable and in any case within 24 hours following the conclusion of the Deployment.
• Watchlists are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the Deployment.

• LFR Operator and Engagement logs are retained in line with MOPI retention periods

All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:
• in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and /or
• in accordance with Essex Police's complaints / conduct investigation policies.

Source System – Athena Record Management System

Please refer to Home Office Review of the Use and Retention of Custody Images published February 2017 (recommendation 4)

Non-conviction – upon request
Group 1 or 2 (Public Protection Matters & sexual, violent or other serious offences respectively) – 10 years upon request then review
Group 3 (all other offences) – 6 years upon request then review
Group 4 (missing persons) – 6 years then review

All other personal data will be stored in accordance with MOPI standards.
Group 1 - subject is 100 years the review
Group 2 – 10 year clear period then review
Group 3 – 6 year clear period Group 4 (missing persons) – 6 years then review

Appropriate Policy Document review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed annually or revised more frequently if necessary.

Policy document Sign-Off

Person completing the APD	Name (in capitals)	**D/SUPT STEPHEN JENNINGS**
	Date:	**08/08/2024**
Data Protection Officer	Name:	**Michelle WATSON**
	Date:	**08/08/2024**
Approval Signature (Approval will be required by either the	Signed:	

Senior Responsible Officer (SRO)/ the Information Asset Owner (IAO) or Head of Unit (HoU))		
	Name (in capitals)	**ACC ANDREW PRITCHARD**
	Date:	**15/8/24**