Data Protection Legislation

Appropriate Policy Document (APD)

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

South Wales Police (SWP)/ Gwent Police (GWP) Operator Initiated Facial Recognition (OIFR)

Processing biometric data, for the purpose of uniquely identifying a natural person.

September 2021

Version 2.0

Version Control

Version	Date	Author	Purpose
V1.0	01/07/19	S.Lloyd	Original Draft
V1.1	12/08/19	S.Lloyd	Minor Amendments
V1.2	14/08/19	S.Lloyd	ICO Format
V1.3	05/02/20	S.Lloyd	Version Control
V1.4	10/02/20	D. Howe	Reviewed

V1.5	17/02/20	S.Lloyd	Reviewed
V1.6	01/04/20	S.Lloyd	Reviewed
V1.7	08/07/20	S.Lloyd	Legal Amendments
V1.8	24/08/20	S.Lloyd	DPO Review
V1.9	08/07/21	S.Lloyd	SRO Review
V2.0	17/09/21	S.Lloyd	National Terminology

Terms & Definitions: Capitalised terms used within this APD shall have the meaning given to them in section 3 of the OIFR Policy Document unless otherwise defined.

Introduction

This policy document has been produced in accordance with SWP/GWP obligations under the General Data Protection Regulation (GDPR). It should be read alongside the SWP/GWP of Processing Activities (maintained in accordance with Article 30 GDPR and the SWP/GWP Personal Information Charter. Data protection policy specific to OIFR is also to be found in the Standard Operating Procedure and Data Protection Impact Assessment and the Part 3 Data Protection Act 2018 APD.

As part of SWP/GWP' 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 GDPR (which is incorporated into UK law under and supplemented by Part 2 and Schedule 1 of the 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 2018 and is subject to a separate APD.

This Policy Document

Some of 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 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 2018 (Appropriate Policy Document and Additional Safeguards).

Description of Data Processed

The special category data processed utilising Operator Initiated Facial Recognition (OIFR)

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

Operator Initiated Facial Recognition

The use of facial recognition where:
(i) media is directly captured of a Subject present; or
(ii) media is otherwise acquired in lieu of capturing it,

with the intent of subjecting it to analysis by the FRT System. The results of such analysis could shape events to which the footage relates in real time.

The use of operator initiated facial recognition which takes an image of a particular person and uses it to either (i) help policing establish who a person in the image is or (ii) establish where a person has previously appeared in other media held by the police.

In SWP/GWP this consists of a mobile phone (OIFR Device) deployment of FRT technology, which compares a photograph of a person's face taken on a mobile phone which is processed to create Biometric Template which is then compared with the Biometric Template from images contained in the Image Reference Database(s) in order to assist an officer to identify a Subject.

Biometric data used to uniquely identify an individual is considered to be sensitive personal data. For the purpose of this processing we will be collecting this personal data of members of the public which will include a Probe Image that may be utilised by extracting a Biometric Template from it for the purposes of uniquely identifying them. Where this data does not match that held on the predetermined on the Image Reference Database(s) it will not be further processed and permanently deleted. No other personal identifiers are collected in addition to the Biometric Template.

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

GDPR conditions for processing special category data

SWP/GWP 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.

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

Article 9(2)(c) – vital interests

Processing is necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent.

E.g. processing images at Road Traffic Collisions where the person may be unconscious with a view to saving their life by identifying relevant information recorded about them if they are on the Image Reference Database.

Article 9(2)(g) - Substantial Public Interest
E.g. Identification of missing persons or safeguarding children or vulnerable individuals.

Article 9(2)(j) – Historical research or statistical purposes
E.g. Undertaking an academic evaluation into the equitability of OIFR.

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

Schedule 1 Condition for processing

Special Category Data

We process special category (SC) data for the purposes in Part 1, paragraph 4 of Schedule 1 DPA: -

- Paragraph 4 – Research, etc.

This condition is met if the processing is necessary for archiving purposes, scientific or historical research purposes or scientific purposes, is carried out in accordance with Article 89(1) of the GDPR (as supplemented by section 19) and is in the public interest.

An independent academic evaluation of OIFR is to be conducted. The sharing of data will be subject to a Service Level Agreement. Any sharing of data will be time limited via a web-based sharing platform rather than data transfer. The platform will be accessed by academic partners via a secure log on for a time limited period. The scientific research purpose is relied upon here. Where possible anonymised or pseudonymised data is used. Where members of police staff consent to the use of their images for testing or evaluation of performance of the system this is collected in accordance with recognised research ethics standards.

We also process SC data for the following purposes identified in paragraphs 6 and 18 of Part 2 of Schedule 1 (substantial public interest conditions) for which we are required to have in place an APD:

- 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, SWP/GWP will always consider whether less intrusive measures can be used with compromising the objective and the interests of the individual balanced against the interests of the community.

Wherever possible SWP/GWP will seek to identify an individual via traditional means. If this is not possible for example when the individual is suspected of providing a false name then OIFR may be utilised.

- 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 GDPR

Accountability Principle (Article 5(2) GDPR)

SWP/GWP 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 OIFR and who reports directly to the Chief Officer team for South Wales.
- 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 data protection impact assessments 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 OIFR 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 FRT is used is available to the public on the Home | South Wales Police (south-wales.police.uk).

The processing of data by OIFR for the purposes of substantial public interest is necessary on the basis of SWP/GWP 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 SWP/GWP relies and examples of purposes that meet each of those conditions). SWP/GWP 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. SWP/GWP will always consider

whether the use of OIFR 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 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 vital interests of the data subject, 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 only be further processed where it is not incompatible with the purpose for which it was collected (including research to ensure accuracy of the developing technology).

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 SC 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 GDPR and DPA 2018.

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 individuals 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 OIFR, this is sufficient facial biometric data to compare against a database. All Probe Images will be immediately deleted from the mobile device and FRT System.

For OIFR, this is sufficient facial biometric data to compare against a database. All images captured using the technology (Probe Images) will be immediately deleted from the mobile device and FRT System.

Ultimately a human operator will determine whether there is a match is made between the Probe and Candidate Image where the automated comparison indicates that they may be the same person. This is an additional safeguard against identification of similar but incorrect individuals.

Principle (d): accuracy

We will retain the Probe Image of the Subject and Biometric Template for no longer than is necessary for the non-law enforcement purposes for which it is processed. The Probe Image will be automatically deleted immediately from the OIFR Device and FRT System. The comparison process takes a matter of seconds, where a match is indicated further consideration will be undertaken by a human Operator. Whether it is determined that the match is similar but incorrect or a match is made by the Operator the image will be automatically and immediately deleted from the OIFR Device and FRT System. Where we become aware that personal data contained within a Image Reference Database 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. This is an automated process and occurs every ten minutes. This will involve comparing images in the Image Reference Database and images from the source systems, both sets of images will have a hash value applied and compared for accuracy to ensure they are the same. If there is an imbalance an alert will be sent to the database team for review. 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. An additional safeguard in the process is that a police officer will attempt to manually establish the identity of the individual prior to using OIFR.

Principle (e): storage limitation

All special category data processed by us using OIFR for non-law enforcement purposes will be deleted immediately. The Probe Image of an individual including the Biometric Template is automatically immediately deleted. Whether it is determined that the match is similar but incorrect or a match is made by the officer the image will be automatically and immediately deleted from the OIFR Device and FRT System. 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 OIFR. 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 OIFR is processed within our accredited secure computer network which is located locally within SWP/GWP 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. OIFR has also been subject to a robust Data Protection Impact Assessment.

All staff receive basic data protection training must undertake annual mandatory training for managing information. Specific training is provided to officers working with OIFR 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. 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 OIFR and FRT System

- Image of the Subject as captured by OIFR (Probe image) - immediately deleted in the OIFR Device and FRT System.
- Biometric Template of Probe Image - immediately deleted in the FRT System
- Candidate images and Biometric Template (held on FRT System) – mirror MOPI retention periods for NICHE RMS

Electronic Pocket Notebook

- Electronic Pocket Notebook – MOPI retention of personal information (detailed within ePNB DPIA), not including the Probe Image.

Source System – Custody Images and Missing Person Images

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.

Further information relating to SWP/GWP use of OIFR can also be found in relevant supporting documents, to include: -

- OIFR Standard Operating Procedures – How to guide for officers
- OIFR Policy
- OIFR Equality Impact Assessment
- iPatrol Standard Operating Procedures – How to guide for officers to include ePNB
- OIFR Data Protection Impact Assessment
- iPatrol Data Protection Impact Assessment

Other relevant policies/guidance documents available to police personnel are:

Information Security Information
Data Protection Policy
Data Protection Impact Assessment Guidance
Information Asset Management Guidance
Information Asset Owner Handbook

Information Risk Management Guidance
Data Minimisation, Anonymisation and Pseudonymisation Guidance
Consent Guidance
Force Retention Schedule

Policy document Sign-Off

Person completing the APD	Name (in capitals)	**Scott Lloyd** **Chief Inspector**
	Date:	**08/07/2021**
Data Protection Officer	Name:	**Louise Voisey**
	Date:	**24/08/2020**
Approval Signature (Approval will be required by either the Senior Responsible Officer (SRO)/ the Information Asset Owner (IAO) or Head of Unit (HoU))	Signed:	
	Name (in capitals)	**Mark Travis** **Assistant Chief Constable**
	Date:	**08/07/2021**