HEDDLU DE CYMRU
SOUTH WALES POLICE

Appropriate Policy Document: Retrospective Facial Recognition

Part 3 Data Protection Act 2018

Law Enforcement Processing

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category and criminal offence data under certain specified conditions.

This document is a policy for sensitive processing of data by the force as part of Retrospective Facial Recognition (RFR). Where there are potentially high risks as a result of specific processing activities, a tailored policy document will be produced in respect of that activity, however this will be on an exceptional basis.

Force	SWP
RoPA Ref:	IG/42
DPIA Ref:	AR0120
APD No.	APD003a.ii

1. Description of data processed

Give a brief description of each category of special category data/criminal offence data processed and indicate how long it is retained for.

Special Category Data *Special category data includes personal data* ***revealing or concerning*** *the above types of data. Therefore, if you have inferred or guessed details about someone which fall into one of the*	Indicator "x"	Description of Data	Retention

above categories, this data may count as special category data. It depends on how certain that inference is, and whether you are deliberately drawing that inference.			
Data revealing race or ethnic origin			
Data revealing political opinions			
Data revealing religious or philosophical beliefs			
Data revealing trade union membership			
Genetic data			
Biometric data (where used for identification purposes)	x	RFR is a post event use of facial recognition technology (FRT), which compares still images of faces of unknown subjects against an Image Reference Database in order to identify them. The Image Reference Database for RFR is the South Wales Police / Gwent Police custody image dataset. The images in the Image Reference Database are referred to as Candidate Images. All custody images will have a Biometric Template created (sensitive personal data) at the point of enrolment to the FRT system. An RFR Probe Image is any facial image which is searched against the Image Reference Database and can be retrieved from a variety of sources. The common sources of RFR Probe Images may include CCTV systems, digital cameras, mobile phones and social media, although any source of image will be considered. The faces of individuals in the Probe Image will have a Biometric template created from the Probe Image and this will be compared against the Image Reference Database.	No biometric data is retained. The untemplated images are retained in line with MoPI retention which will depend on the offence.

		Whilst utilising RFR a Probe Image is searched against every Candidate Image in the selected Image Reference Database(s). At the conclusion of the comparison, regardless of whether a match has been made, the Biometric Template of the Probe Image is automatically and immediately deleted. South Wales Police / Gwent Police is not relying on consent for processing.	
Data concerning a person's sex life			
Data concerning a person's sexual orientation			

Criminal Offence Data	Indicator "x"	Description of Data
Criminal Activity	x	The Image Reference Database will contain images of individuals previous arrested by SWP and taken into custody
Criminal Allegations (including unproven allegations)	x	As above – the subject may be on bail
Criminal Investigations	x	As above
Criminal Proceedings	x	As above
Criminal Offences	x	As above
Criminal Penalties/Sanctions/Fines	x	As above
Information about the absence of convictions		
Conditions or restrictions placed on an individual as part of the criminal justice process	x	As above
Civil Measures which may lead to a criminal penalty if not adhered to.		

2. Schedule 8 DPA 2018 Condition for Processing

Please insert link to Privacy Policy, record of processing or any other relevant documentation if appropriate:
SWP Privacy Notice

Schedule 8 Conditions[1]	Indicator "x"
Statutory etc and government purposes	x
Administration of justice and parliamentary purposes	x
Protecting individuals' vital interests	x
Safeguarding of children and of individuals at risk	x
Personal data in the public domain	
Legal claims	
Judicial acts	
Archiving	

3. Ensuring Compliance with the Principles

There is no requirement to reproduce information which is recorded elsewhere – questions may be answered with a link or reference to other documentation, to your policies and procedures, Data Protection Impact Assessments (DPIAs) or to your privacy notices.

Accountability Principle

Question	Y/N	Details
Do we maintain appropriate documentation of our processing activities?	Y	DPIA; APD; Audit trails; Occurrence log updates; policy documents
Do we have appropriate data protection policies	Y	Overarching DP Policy
Do we carry out data protection impact assessments (DPIA) for uses of personal	Y	DPIA is in place AR0120

[1] Data Protection Act 2018 (legislation.gov.uk)

data that are likely to result in high risk to individuals' interests?		

Principle (a) Lawfulness, fairness and transparency

Question	Y/N	Details
Have we identified an appropriate lawful basis for processing and a further Schedule 8 condition for sensitive processing under Part 3	Y	S35(5) Data Protection Act 2018 the processing is necessary for the law enforcement purpose Schedule 8 (1) Statutory etc purposes Schedule 8 (3) Protecting individuals' vital interests Schedule 8 (4) Safeguarding of children and individuals at risk
Do we make appropriate privacy information available with respect to the special category/criminal offence data?	Y	Yes – Privacy policy is available online and has links from the FRT pages specifically. The DPIA captures information and guidance specific to the use of RFR data and also how individuals can access their rights in order to understand how their data is held and processed and also how to request removal on their data. Information relating to data held on police systems and access to rights is also available in Custody suites for persons in detention to understand options to request information on their data and to request deletion of data where applicable.
Are we open and honest when we collect the special category/criminal offence data and do we ensure we do not deceive or mislead people about its use	Y	Yes – see above. Operators are also subject to the Code of Ethics

Principle (b): purpose limitation

Question	Y/N	Details
Have we clearly identified our purpose(s) for processing the special category/criminal offence data?	Y	See AR0120
Have we included appropriate details of these purposes in our privacy information for individuals?	Y	Yes – as above, privacy policy is available online and FRT page links to privacy policy.

		There is information available in Custody Suites in regard to requesting data and also data rights.
If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), do we check that this is compatible with our original purpose or get specific consent for the new purpose?	Y	Information is not used for a different purpose.

Principle (d): accuracy

Question	Y/N	Details
Do we have appropriate processes in place to check the accuracy of the special category/criminal offence data we collect, and do we record the source of that data?	Y	Yes – ongoing assessment of the FRT takes place to ensure that the Public Sector Equality Duty is met. The capture and processing of the data is auditable in police systems.
Do we have a process in place to identify when we need to keep the special category/criminal offence data updated to properly fulfil our purpose, and do we update it as necessary?	Y	Yes – this is documented in DPIA AR0120 – the biometric templates of Probe Images are not retained. Retention of Candidate Images in the Image Reference Database is governed by MOPI and individuals, or persons acting on their behalf, are able to make requests for data to be deleted if compatible with right to erasure.
Do we have a policy or set of procedures which outline how we keep records of mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification?	Y	Yes the overarching privacy policy deals with individual rights and there is also a joint information management policy. The Digital Service Division manages data quality and the Niche RMS allows officers to include updates and correction.

Principle (e): storage limitation		
Question	**Y/N**	**Details**
Do we carefully consider how long we keep the special category/criminal offence data and can we justify this amount of time?	Y	Probe Image The Probe Image will likely form part of the investigation and therefore will be retained in line with MOPI for the appropriate length of time. Group 1 Serious offences (e.g. murder, rape, terrorism) Indefinite retention unless review determines otherwise every 10 years Group 2 Significant offences (e.g. burglary, assault) Minimum retention 10 years review every 5 years Group 3 Minor offences (e.g. petty theft, public order) Minimum retention 6 years review every 3 years Biometric Templates – Probe Images The Biometric Templates of Probe Images are immediately and automatically deleted at the conclusion of the RFR comparison. Candidate Images Candidate Images are retained in line with MOPI for the appropriate length of time. Biometric Templates – Candidate Images The Biometric Templates of Candidate Images are held in line with MOPI for the appropriate length of time. Where the Candidate Image is deleted in the Record Management System, the FRT system will automatically detect that the Candidate Image has been deleted and will delete the Biometric Template held in the FRT system. Source System – Niche Record Management System – MOPI retention period depending on suspected offence All personal data will be stored in accordance with MOPI standards – • Tier 1 for 31 days • Tier 2 for 6 years plus 1 • Tier 3 retained for one hundred years.
Do we regularly review our information and erase or anonymise this special	Y	As above

category/criminal offence data when we no longer need it?		
Have we clearly identified any special category/criminal offence data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes?	N	No.

Principle (f): integrity and confidentiality (security)

Question	Y/N	Details
Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data?	Y	A DPIA/Info Sec assessment has been carried out
Do we have an information security policy (or equivalent) regarding this special category/criminal offence data and do we take steps to make sure the policy is implemented? Is it regularly reviewed?	Y	There is a separate information security policy which is reviewed annually. Force Information Security Officers monitor compliance with this policy
Have we put other technical measures or controls in place because of the circumstances and the type of sensitive data we are processing?		Personal data processed by RFR is processed within SWP accredited secure computer network which is located within South Wales 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 security measures are designed to protect against unauthorised or unlawful processing, accidental loss, destruction or damage. 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. RFR has also been subject to a robust DPIA. All SWP/ GWP Officers and staff receive basic data protection training must undertake annual mandatory training for managing information. Specific training is provided to officers working with RFR which is supplemented with bespoke Standard Operating Procedures. Access to RFR is limited to those who have undertaken specific training and have specific role-based access permissions. Permission to access the RFR system can be removed remotely at any time if there are any concerns of misuse. The systems used to process personal data allow SWP/ GWP respond to individual rights requests and to erase or update personal data at any point in time where appropriate and where personally identifiable information 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. No biometric templates or captured images are retained in the FRT system There is no automated decision making.

Review of APD

Review Date	Reviewer		Actions	Date of next review
09/12/2020	CI Scott Lloyd	V0.1	Original Draft	
31/12/2020	CI Scott Lloyd	V0.2	DSD SMT Review	
12/01/2021	CI Scott Lloyd	V0.3	DPO Review	
16/04/2021	CI Scott Lloyd	V0.4	FRT Board Review	
29/09/2022	CI Scott Lloyd	V1	Review	
29/09/2023	Insp Ben Gwyer	V1	No Changes	
29/09/2024	Insp Ben Gwyer	V2	No Changes	
08/08/2025	Insp Ben Gwyer		Information amended for new document format. Actions taken to	08/08/2026

			address recommendations raised during ICO Audit process 2025	