HEDDLU DE CYMRU
SOUTH WALES POLICE

HEDDLU GWENT POLICE

Appropriate Policy Document: Operator Initiated 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 Operator Initiated Facial Recognition ("OIFR"). 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/GWP
RoPA Ref:	
DPIA Ref:	245
APD No.	004

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	OIFR is a mobile phone deployment of Facial Recognition Technology which compares a biometric template extracted from a still image of an individual immediately captured on a smart phone against a predetermined watchlist in order to assist an officer identify the subject	
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)		
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 laced 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 GWP Privacy Notice

Schedule 8 Conditions[1]	Indicator "x"
Statutory etc and government purposes	x
Administration of justice and parliamentary purposes	
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; APP; Audit trails; ePNB updates

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

Do we have appropriate data protection policies	Y	Overarching DP Policy
Do we carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests?	Y	

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 - information is published on the SWP/GWP websites and operators inform subjects at the time that OIFR is deployed.
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 DPIA245 OIFR
Have we included appropriate details of these purposes in our privacy information for individuals?	Y	Yes individuals are informed of the specific purpose at the time of deployment.
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 245 – the subject image and biometric templates are not retained.
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	Where no matches are identified no biometric data is retained; other information retained for audit purposes are kept under current management of police information retention periods
Do we regularly review our information and erase or anonymise this special category/criminal offence data when we no longer need it?	Y	As above
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
Have we put other technical measures or controls in place because of the circumstances and the type of sensitive data we are processing?		The OIFR Device (force issued smart phone) is built with force accredited security to protect data, principally using two factor authentication to the device and a Virtual Private Network (VPN). There is

		an auditing capability to prevent unauthorised access or misuse.

Review of APD

Review Date	Reviewer	Actions	Date of next review
30/07/2024	L Voisey, DPO	Reformatted	30/07/2025