SMARTER RECOGNITION SAFER COMMUNITY | CYDNABYDDIAETH DOETHACH CYMUNED DDIOGELACH

Data Protection Legislation

Policy on Sensitive Processing under Part 2 Data Protection Act 2018 and GDPR

South Wales Police (SWP) Automated Facial Recognition (AFR)

Processing Biometric Data to uniquely identify a person

May 2019

Version 3.0

1. Introduction

This policy document has been produced in accordance with South Wales Police (SWP) obligations under General Data Protection Legislation (GDPR). It should be read alongside the South Wales Police (SWP) Record of Processing Activities (maintained in accordance with Article 30 GDPR), and the South Wales Police Personal Information Charter.

Article 9(1) of the GDPR prohibits the processing of special categories of personal data unless a condition in Article 9(2) is met. (Schedule 1 of the DPA 2018). For South Wales Police, the processing of special categories of personal data (sensitive processing) is only permitted where it is necessary for scientific research (part 2) and is in the public interests. . Additionally during non-live testing and validation consent (part 3) may also be sought. There is a further requirement that this condition will only be met if the sensitive processing is carried out in accordance with this policy. South Wales Police staff must therefore have regard to this policy when carrying out sensitive processing on behalf of the Force, when it is acting in its capacity as Controller of the personal data.

South Wales Police is most likely to carry out sensitive processing for a law enforcement purpose in reliance on the conditions set out in Schedule 8 to include:-

paragraph 4 - safeguarding of children and of individuals at risk
paragraph 9(b) – scientific or research purposes

2. Purpose

The purpose of this policy is to explain:

1. South Wales Police procedures which are in place to secure compliance with the GDPR data protection principles when relying on public interest conditions in Part 2 and Part 4 of Schedule 1 DPA 2018; and

2. Retention and erasure policies concerning the processing of special categories of data on grounds of public interest.

3. Compliance with Data Protection Principles

a) ‘lawfulness and fairness’

The lawfulness of South Wales Police processing is derived from its official functions as a UK police service.

b) ‘purpose limitation’

South Wales Police only processes sensitive personal data when permitted to do so for explicit and legitimate purposes. Such personal data is collected for explicit and legitimate purposes such as biometric data during the deployment of Automated Facial South Wales Police function is required to have a specific lawful basis and it must be compatible with data protection obligations; the processing must therefore be proportionate and necessary.

c) ‘data minimisation’

During AFR Locate deployments South Wales Police collects the information necessary to determine whether the individual is on a watchlist. If an intervention is made the process will not prompt data subjects to answer questions and provide information that is not required.

Where processing is for research and analysis purposes, wherever possible this is done using anonymised or de-identified data sets.

d) ‘accuracy’

Providing complete and accurate information is required when constructing a watchlist. During AFR Locate deployments watchlists will be constructed on the day of deployment and where the deployments extend beyond 24 hours these will be amended daily. Where permitted by law, and when it is reasonable and proportionate to do so, South Wales Police may check this information with other organisations – for example other police and or law enforcement services.

If a change is reported by a data subject to one service or part of South Wales Police, whenever possible this is also used to update the AFR application, both to improve accuracy and avoid the data subject having to report the same information multiple times.

e) ‘storage limitation’

South Wales Police has a comprehensive set of retention policies in place which are published online, further information specific to AFR can be found on SWP AFR webpage.

f) **‘integrity and confidentiality’**

South Wales Police has a range of security standards and policies based on industry best practice and policing requirements to protect information from relevant threats. We apply these standards whether South Wales Police data is being processed by our own staff, or by a processor on our behalf.

All staff handling South Wales Police information are security cleared and required to complete annual training on the importance of security, and how to handle information appropriately.
In addition to having security guidance and policies embedded throughout SWP business, SWP also has specialist security, cyber and resilience staff to help ensure that information is protected from risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

4. How often will this policy document be reviewed?

South Wales Police will formally review this document not less than six months after its introduction (not later than the end of April 2019) and yearly thereafter.

Requirement to keep records

Where the sensitive processing is carried out by South Wales Police (in its capacity as the processor), South Wales Police staff must on behalf of the controller, include the following information in the Record of Processing:

a. Whether the sensitive processing is carried out in reliance on the consent of the data subject, or if not, which condition in Schedule 8 is relied on;
b. How the processing satisfies section 35 (lawfulness of processing); and
c. Whether the personal data is retained and erased in accordance with the policies described above in section 3 of this policy, and, if it is not, the reasons for not following those policies.

Further information relating to South Wales Police use of Automated Facial Recognition (AFR) can also be found in relevant Data Protection Impact Assessment (DPIA) and Standard Operating Procedures (SOPS.)

5. Policy document Sign-Off

Person completing the DPIA	Name (in capitals)	**SCOTT LLOYD** **Inspector**
	Date:	**22/05/2019**
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)	**RICHARD LEWIS** **Deputy Chief Constable**
	Date:	**22/05/2019**