Heddlu Police
DYFED-POWYS

Appropriate Policy Document - as required under UK Data Protection Legislation

Policy number:	026/2021		
Version control:	**Version: 1.0** **Date:** July 2021 **Author:** [redacted] **Rationale:** First version		
Date implemented:	July 2021		
Review date:	July 2023		
Owner/contact:	Data Protection Advisor		
Approval:	Information Manager / Data Protection Officer Date of approval: 22/07/2021		
Suitability for publication:	Yes	22/07/2021	[redacted]

Please note:
This document sets out principles to help guide decision making and in some parts may be quite prescriptive. However, it is vital that officers and staff have the freedom to innovate, exercise discretion and take risk based decisions centred on the needs of the victim and the merits of each case.

There may be occasions when an employee is considered to have acted outside of the content of this document but if they have done so with honesty, integrity and professionalism, to make the best decision for the community we serve, they will be trusted and supported. On the occasions when this is the case, the rationale for it must be properly recorded.

Introduction

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions, and when processing sensitive personal data for law enforcement (LE) purposes.

The UK General Data Protection Regulation (UK GDPR) defines SC data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation,

with an equivalent definition of sensitive processing available under Part 3 of the DPA 2018.

The term CO data covers a wide range of information, including but not limited to:

- criminal activity
- allegations, including unproven allegations
- investigations
- proceedings
- information relating to the absence of convictions
- personal data of victims and witnesses of crime
- personal data about penalties
- conditions or restrictions placed on an individual as part of the criminal justice process
- civil measures which may lead to a criminal penalty if not adhered to.

In order to lawfully process SC and CO data, a UK GDPR Article 6 lawful basis must be identified, and a separate Article 9 condition for processing must also be identified for SC data.

Section 10 of the DPA 2018 requires that where the processing of SC data is reliant on one of the following lawful bases, as described in Article 9 of the UK GDPR, the processing must also satisfy a condition in Schedule 1 of the DPA 2018:

- Article 9 (b) Employment, social security and social protection
- Article 9 (g) Substantial public interest
- Article 9 (h) Health and social care
- Article 9 (i) Public health
- Article 9 (j) Archiving, research and statistics.

In many cases, you also need an APD in place in order to meet a UK Schedule 1 condition for processing in the DPA 2018.

Section 35 (4) and (5) of the DPA 2018 require that where the processing of personal data for any of the LE purposes is sensitive processing, based either on the consent of the individual or a condition within Schedule 8, the Controller shall have an APD in place.

This APD is intended to complement Dyfed-Powys Police's general record of processing under Article 30 of the UK GDPR and provides SC and CO data with further protection and accountability. It demonstrates that the processing of SC and CO data based on specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. It also demonstrates that the processing of sensitive data for LE purposes is compliant with the requirements of Part 3 section 42 of the DPA 2018.

Dyfed-Powys Police will keep this APD under review and will retain it until six months after the date the relevant processing stops. This document should be read in conjunction with the Force Data Protection Policy and Guidance Document.

***Applies (but not limited) to**: All categories of Dyfed-Powys Police employees, whether full-time, part-time, permanent, fixed term, temporary (including agency staff, associates and contractors) or seconded staff. Any employee accessing and using Force assets and property must have due regard to the contents of this policy.*

Associated Documentation

- The Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- Crime and Disorder Act 1998
- Criminal Justice and Immigration Act 2008
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- Data Protection Policy
- Data Protection Guidance Document
- Data Protection Breach Policy
- Information Security Policy
- Information Sharing Policy
- Records Management Policy
- Data Protection Compliance Audit Policy
- College of Policing Authorised Professional Practice (APP) Information Management Guidance
- The National Police Chiefs Council (NPCC) Data Protection Manual of Guidance
- The Information Commissioner's Office's Code of Practice and Guidance

Description of data processed

Details of the types of personal data we process are available in our privacy notice. Our privacy notice can be located on our website: https://www.dyfed-powys.police.uk/hyg/fpndyfed-powys/privacy-notice/.

Schedule 1 condition for processing

Section 10 of the DPA 2018 requires that where the processing of SC data is reliant on one of the following lawful bases, as described in Article 9 of the UK GDPR, the processing must also satisfy a condition in Schedule 1 of the DPA 2018:

- Article 9 (b) Employment, social security and social protection
- Article 9 (g) Substantial public interest
- Article 9 (h) Health and social care
- Article 9 (i) Public health
- Article 9 (j) Archiving, research and statistics.

If the Force relies on conditions (b), (h), (i) or (j), we will also ensure that we meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.

If the Force relies on the substantial public interest condition in Article 9(2)(g), we will also ensure we meet one of the 23 specific public interest conditions set out in paragraphs 6 to 28 of Schedule 1 of the DPA 2018:

6. Statutory and government purposes
7. Administration of justice and parliamentary purposes
8. Equality of opportunity or treatment
9. Racial and ethnic diversity at senior levels
10. Preventing or detecting unlawful acts
11. Protecting the public
12. Regulatory requirements
13. Journalism, academia, art and literature
14. Preventing fraud
15. Suspicion of terrorist financing or money laundering
16. Support for individuals with a particular disability or medical condition
17. Counselling
18. Safeguarding of children and individuals at risk
19. Safeguarding of economic well-being of certain individuals
20. Insurance
21. Occupational pensions
22. Political parties

23. Elected representatives responding to requests
24. Disclosure to elected representatives
25. Informing elected representatives about prisoners
26. Publication of legal judgments
27. Anti-doping in sport
28. Standards of behaviour in sport

Consent or Schedule 8 condition for processing

When the Force undertakes 'sensitive processing':
the processing will be **strictly necessary** for the law enforcement purpose, and either be based on consent or satisfy one of the following conditions in Schedule 8 of the DPA 2018:
- Statutory etc purposes
- Administration of justice
- Protecting individual's vital interests
- Safeguarding of children and of individuals at risk
- Personal data already in the public domain
- Legal claims
- Judicial acts
- Preventing fraud
-Archiving etc

Procedures for ensuring compliance with the principles

Accountability principle
The Force understands the requirement to have appropriate policies in place. We have in place the Data Protection policy, Data Protection Breach policy and the associated guidance document. We also have in place the DPIA policy, template document, guidance document and overall process. This ensures that DPIAs are carried out for uses of personal data that are likely to result in high risk to individuals' interests. The Force also conducts a Data Protection Compliance Audit program which ensures data is being processed in line with UK data protection legislation and the principles outlined within.
Principle (1): lawfulness and fairness
Law Enforcement Processing

The Force understands that the processing of personal data for any of the LE purposes must be lawful and fair.

The lawfulness of sensitive processing carried out by the Force is derived from its official functions as a public body and obligations or rights imposed or conferred by law as an employer.

The processing will be **strictly necessary** for the law enforcement purpose, and either be based on consent or satisfy one of the conditions in Schedule 8 of the DPA 2018, as detailed above.

When relying on consent, we will ensure that the consent is valid and fully compliant with the definition provided in UK data protection legislation.

General Processing

The Force understands that SC and CO data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Where sensitive processing is carried out by the Force for operational policing purposes that are NOT prescribed for under Part 3 of the DPA, the processing will rely on one of the following lawful bases from Article 9 of the UK GDPR and will meet a relevant condition from Schedule 1 of the DPA 2018:

- Article 9 (a) Consent
- Article 9 (c) Protecting vital interests
- Article 9 (e) Manifestly made public by the data subject
- Article 9 (f) Establishment, exercise or defence of legal claims
- Article 9 (g) Substantial public interest

Schedule 1, Part 2 (6): Statutory and government purposes
Schedule 1, Part 2 (7): Administration of justice and parliamentary purposes
Schedule 1, Part 2 (8): Equality of Opportunity or treatment
Schedule 1, Part 2 (9): Racial and Ethnic diversity at senior levels of organisation
Schedule 1, Part 2 (10): Preventing or detecting unlawful acts
Schedule 1, Part 2 (11): Protecting the public against dishonesty
Schedule 1, Part 2 (12): Regulatory requirements relating to unlawful acts and dishonesty
Schedule 1, Part 2 (14): Preventing fraud
Schedule 1, Part 2 (18): Safeguarding of children and of individuals at risk
Schedule 1, Part 2 (19): Safeguarding of economic well-being of certain individuals

- Article 9 (j) Archiving, research and statistics

Schedule 1, Part 1 (4): Research

Where the processing of SC and CO data is carried out by the Force for non-operational policing purposes but predominantly as an employer, we will rely upon the following lawful bases from Article 9 of the UK GDPR and from Schedule 1 of the DPA 2018:

- Article 9 (a) Consent
- Article 9 (b) Employment, social security and social protection

Schedule 1, Part 1 (1): employment, social security and social protection

- Article 9 (h) Health and social care

Schedule 1, Part 1 (2): Health or social care purposes

- Article 9 (f) Establishment, exercise or defence of legal claims
- Article 9 (j) Archiving, research and statistics

Schedule 1, Part 1 (4): Research

Further information is available by accessing our privacy notice. Our privacy notice can be located on our website: https://www.dyfed-powys.police.uk/hyg/fpndyfed-powys/privacy-notice/.

We ensure we are open and honest when we collect SC and CO data, and we do not deceive or mislead people about its use.

Principle (2): purpose limitation

Law Enforcement Processing

The Force understands that LE purposes are defined under UK data protection legislation as the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The Force's LE purposes, for which personal data is collected on any occasion, are specified, explicit and legitimate.

The Force does not process personal data in a manner that is incompatible with the purpose for which it was collected.

Personal data collected by the Force, for a LE purpose, can be processed for any other law enforcement purpose - provided that it is authorised by law, the processing is necessary and proportionate to that other purpose and meets the requirements of the UK GDPR and DPA 2018.

General Processing

The Force understands that personal data must be collected for specified, explicit and legitimate purposes and will not further process that data in a manner that is incompatible with those purposes.

The Force will only reuse SC and CO data collected under UK GDPR where that further use is compatible with the original purpose it was collected for.

Principle (3): data minimisation

Law Enforcement & General Processing

The Force will ensure that SC and CO data, and personal data processed for any of the LE purposes, will be adequate, relevant and not excessive in relation to the purpose for which it is processed.

The Force will only collect personal data required for our specified purpose and ensure that it is proportionate.

Force policies, guidance and training also require staff to process only the minimum data required to achieve the specified purpose.

Through the Force Data Protection Compliance Audit program, we also review SC data and ensure retention and deletion policies are adhered to.

Principle (4): accuracy

Law Enforcement & General Processing

The Force understands that personal data processed for any purpose (including LE purposes) must be accurate and, where necessary, kept up to date. We will ensure that every reasonable step is taken to ensure that personal data that is inaccurate, having regard for the purposes (including LE) for which it is processed, is erased or rectified without delay.

When the Force processes personal data for any of the LE purposes, personal data based on facts will be, so far as possible, distinguishable from personal data based on personal assessments. The Force will also ensure that, where relevant and as far as possible, a clear distinction can be made between different categories of data subject such as suspects, convicted offenders, victims and witnesses.

The development and procurement of Information Management systems in the Force will require that 'data protection by design and default' is embedded in such processes.

The Force will also take reasonable steps to ensure that any personal data which is inaccurate, incomplete or out of date is not disclosed. If it is discovered, after disclosure, that the data was inaccurate, then the Force will inform the recipient as soon as possible.

If an individual contacts the Force to question the accuracy of their data it will respond to such requests in accordance with Article 16 of the UK GDPR/Section 46 DPA 2018. Where the Force decides not to erase or rectify the data it will document this decision.

Requests for the disclosure of any personal information will only be considered once the Force is fully satisfied that the enquirer or recipient is identified and authorised to receive the information.

Sources of personal data are listed in our privacy notice which can be located on our website:
https://www.dyfed-powys.police.uk/hyg/fpndyfed-powys/privacy-notice/.

Principle (5): storage limitation

Law Enforcement & General Processing

The Force are committed to improving records management to ensure that information is managed throughout its life cycle in a systematic, cost-effective and efficient manner. In particular, it provides a means of applying controls to information to maintain its evidential weight and ensure its authenticity, availability and integrity. Only retaining personal, SC and CO data processed for a general purpose and law enforcement purpose.

The Force will carefully consider the retention periods for sensitive data and the purpose for which it is processed. A periodic review of retention periods will be undertaken by the Force to justify the need for retention of such data in line with the National Police Chief's Council in their National Guidance on the Minimum Standards for the Retention and Disposal of Police Records (Section 23 Standing Orders).

Principle (6): integrity and confidentiality / security

Section 2 of the UK GDPR and Sections 66-68 of the DPA 2018 contain the requirements for the security of personal data to include the implementation of appropriate technical and organisational measures to include a level of security appropriate to the risks arising from the processing of personal data.

Force appropriate technical and organisational security measures will include:

- Using and developing technological solutions to ensure compliance with the data protection legislation
- Using and developing physical measures to protect force assets
- Ensuring the reliability of any persons who have access to police information
- Reporting and investigating security breaches

These obligations include the need to consider the nature of the data to be protected and the harm that might arise from such unauthorised or unlawful processing, accidental loss, destruction or damage. The Government Security Classifications provide for such considerations and is adopted by the Force as part of its compliance with the NPCC Community Security Policy.

Retention and erasure policies

Retention and erasure

Personal data is not retained by the Force for longer than it is needed. Retention and disposal of documents are in line with guidance as set out by the National Police Chief's Council in their National Guidance on the Minimum Standards for the Retention and Disposal of Police Records (Section 23 Standing Orders). In addition, retention requirements are outlined under the College of Policing Authorised Professional Practice (APP) – Information Management - Retention Review and Disposal - Section 3.4.

In the case of any queries regarding this policy and its content - individuals should contact:

- Dyfed-Powys Police Data Protection Advisor
- Email: dataprotection@dyfed-powys.pnn.police.uk
- Post: Data Protection Advisor, Dyfed-Powys Police, PO BOX 99, Llangunnor, Carmarthenshire, SA31 2PF