Police Service of Northern Ireland

Sensitive Processing for General Administrative Purposes, under Part 2 DPA (2018)

This Guidance document clearly defines the responsibilities placed on the Police Service of Northern Ireland to ensure compliance with the Data Protection Act 2018 and the General Data Protection Regulation with regard to processing of sensitive data. Adherence to this Guidance document will assist in meeting the objectives of the overall Information Management Service Policy and Data Protection Service Instruction.

Police Service of Northern Ireland

INDEX

Police Service of Northern Ireland

1. Aims

This policy aligns with PSNIs existing SI0518 Data Protection and is produced in accordance with our obligations to protect special category and criminal convictions data that it processes in accordance with Article 9 and 10 UK GDPR, and has been produced in accordance with PSNI obligations under UK data protection legislation (Schedule 1 DPA 2018).

This policy applies to sensitive processing for general administrative purposes undertaken by the PSNI in accordance with Part 2 of the DPA 2018.

PSNI processing of special category data for law enforcement purposes is covered in a separate service instruction PSNI APD for sensitive processing, UK GDPR/Part 3. Sensitive Processing under Part 3.docx

The purpose of this policy is to explain:

- PSNI procedures which are in place to secure compliance with the data protection principles set out in Part 2 of the DPA 2018 when sensitive processing is carried out by PSNI (in its capacity as controller) on the basis of 'strict necessity' in reliance on one of the conditions set out in Schedule 1, or (on the basis of 'consent'; and
- PSNI policies about the retention and erasure of such personal data, including an indication of how long such data is to be kept.

Police Service of Northern Ireland

2. Introduction

This document is the appropriate policy document for the PSNI which sets out the safeguards PSNI has in place to protect special category and criminal convictions data that it processes in accordance with Article 9 and 10 UK GDPR, and has been produced in accordance with PSNI obligations under UK data protection legislation (Schedule 1 DPA 2018). It should be read alongside the PSNI's Data Protection Policy, and maintained in accordance with Article 30 UK GDPR. The PSNI's Information Asset Register also contains more detailed information about its data processing.

Commented [MN1]: Link no longer working

3. Scope and Purpose

This policy applies to the processing of special category data – which is defined in Article 9(1) – processed in accordance with the UK GDPR/Part 2 of the DPA 2018. PSNI processing of special category data for law enforcement purposes is not covered in this document. Processing for law enforcement purposes is carried out by PSNI in its capacity as a competent authority and falls under Part 3 of the DPA 2018. Sensitive Processing under Part 3.docx

Commented [MN2]: Link no longer working
Do you want this alternative link Part 3 of the DPA 2018

The purpose of this policy is to explain:

1. PSNI procedures that are in place to secure compliance with the UK GDPR data protection principles when relying on 'substantial public interest' conditions in Part 2 of Schedule 1 DPA 2018, or for the purposes of 'employment, social security or social protection' in accordance with Part 1 of Schedule 1 DPA 2018 when processing special category data;

2. PSNI's retention and disposal schedule concerning the processing of special categories of data on grounds of substantial public interest or for the purposes of employment, including an indication of how long such data is to be kept.

Police Service of Northern Ireland

4. Governance and Responsibility

Each Chief Officer is a "Data Controller" and has a legal obligation to ensure that all processing of personal data, by or on behalf of their police service is in accordance with changes to the Data Protection legislation. Every police officer and police staff member, as well as those contractors working for the police, is therefore required to comply with the Data Protection legislation. When the PSNI are involved in partnership working, where both partners determine the purpose for, and the manner in which the data is processed, both partners will be responsible as Data Controllers and are referred to as 'joint data controllers'.

The PSNI Data Protection Officer will author this policy and has responsibility for review of this Service Instruction.

5. Lawful Basis and Conditions

Special categories of personal data

Article 9(1) of the UK GDPR creates a general prohibition on the processing of special categories of personal data.

This prohibition is disapplied if a condition in Article 9(2) is met in relation to the proposed processing. Article 9(4) allows the conditions in Article 9(2) to be subject to further requirements, in particular it is worth noting that in relation to Article 9(2)(b), 'necessary for the purposes of performing or exercising obligations or rights in connection with employment, social security or social protection', and Article 9(2)(g), 'necessary for reasons of substantial public interest' – these will only be met if the controller also has an appropriate policy document in place (paragraphs 1 and 5 of Schedule 1 DPA).

PSNI staff must therefore have regard to this service instruction when carrying out processing of special category data on behalf of the Department, when it is acting in its capacity as controller.

The PSNI has considered whether in the course of its official functions there are additional types of data that might be treated as special category data although not prescribed under Article 9(1) UK GDPR or Part 2 of the Data Protection Act 2018. One such occurrence is that of nationality. PSNI will always treat data revealing community background, racial and ethnic background as sensitive data. Where other data (such as nationality data in some specific cases) is processed in such a way as to reveal characteristics amounting to special category data (e.g. of community background, race and/or ethnicity) the other data will, as appropriate, be processed subject to the enhanced safeguards for sensitive data.

Additionally PSNI may in practice voluntarily decide on a case-by-case basis to apply the enhanced safeguards to other data that it processes – this will include any cases where it is more practical for PSNI to treat all data as special category data (even when it is not legally necessary or required to be processed as such).

Criminal convictions data

Article 10 of the UK GDPR provides that the processing of personal data about criminal offences and convictions can only be carried out either where it is done under the 'control of official authority' or where the processing is authorised under Union or Member State law providing appropriate safeguards. Section 10(4-5) of the DPA 2018 sets out the requirements for the processing of such data where it is done other than under the control of official authority (i.e. it is only permitted if it meets an additional condition set out in Part 1, 2 or 3 of Schedule 1 DPA 2018).

PSNI's processing of criminal convictions data as a controller is done under the control of official authority in accordance with Article 10.

Police Service of Northern Ireland

Conditions for processing Special Category data

The lawfulness of the PSNI's processing is in most cases derived from its official functions as a law enforcement agency and 'competent authority', as per Part 3 of the Data Protection Act 2018 and relevant conditions within schedule 8.

However, under Part 2 of the Data Protection Act 2018 and relevant conditions within schedule 1, PSNI also processes sensitive information (other than criminal convictions see above) for 'general administrative' purposes e.g. HR, OHWB, Recruitment etc. PSNI must ensure that all such processing is necessary and proportionate to the identified purpose.Sensitive Processing under Part 3.docx

When PSNI processes special category data for general administrative purposes it does so in accordance with the requirements of Article 9 and 10 of the UK GDPR and Schedule 1 of the DPA 2018.

The majority of the PSNI's processing of special category data is for the following permitted purposes in Article 9:

- 9(2)(b) 'employment';
- 9(2)(g) 'substantial public interest'

PSNI is therefore required to have this Appropriate Policy Document in place, and to meet the additional conditions prescribed in schedule 1 DPA.

PSNI may also occasionally process some special category data in accordance with other Article 9 conditions, such as:

- 9(2)(a) 'consent' – as a ;aw enforcement authority PSNI may not always rely on consent as the basis for processing. When it does, PSNI ensures that explicit and freely given consent for each special category data item is sought, that the data subject is informed they have the right to withdraw their consent at any time, and that processes are in place to easily facilitate the withdrawal of consent;

- 9(2)(c) 'vital interests' – PSNI may rely on this condition under certain circumstances, such as where the processing is necessary to protect adults or children who are at risk.
- 9(2)(e) data 'made public by the data subject' – PSNI may rely on this if, for example, it checks and further processes data in the public domain to confirm the accuracy of the information it holds;
- 9(2)(j) 'archiving purposes' – PSNI relies upon this condition, for example, to transfer data to OPRONI, The National Archives and the Office of National Statistics for archival research purposes;
- 9(2)(f) 'for the establishment, exercise or defence of legal claims' – PSNI may rely on this if, for example, it provides personal data to assist a third party (such as a vulnerable person or claimant against PSNI) in relation to their legal claim, or is required to disclose material to a claimant, and where such processing is not strictly in support of the PSNI's own public tasks;
- 9(2)(h) for the purposes of health – PSNI may rely on this, for example, when processing Occupational Health referrals.

These other Article 9 conditions do not require an APD to be in place.

6. Compliance with Data Protection Principles

A) Accountability Principle

The PSNI has put in place appropriate technical and organisational measures to meet the requirements of accountability [as required by Article 5(2)]. These include:

- the appointment of a Data Protection Officer (DPO) who has a key assurance, compliance and advisory role on data protection matters within the PSNI, whose responsibilities include (among other things):
  - providing leadership in raising the profile of data protection compliance across PSNI;
  - monitoring compliance with data protection legislation, including the assignment of responsibilities, and overseeing training of officers/staff involved in processing operations;
  - the design and implementation of risk-based assurance reviews/audits to test compliance with privacy and UK data protection legislation, and recommend ways of reducing any identified risks;
  - investigating complaints from data subjects and other stakeholders about the organisations processing of personal data;
  - acting as the organisations main point of contact with the Information Commissioner's Office (ICO) on issues related to the organisations processing of personal data.
- a direct reporting line from the DPO to our highest management levels, including to the SIRO and the Audit and Risk Assurance Committee (ARAC) on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control in relation to its data protection obligations;
- the development and regular review of corporate data protection policies and guidance for officers/staff setting how the PSNI meets its data protection obligations – such as when and how a Data Protection Impact Assessment (DPIA) should be completed; and how to ensure new projects, applications or systems meet the legislative, technical and organisational requirements set out within UK data protection legislation;

- the development of more detailed local guidance relevant to the processing taking place within each business area, such as HR, OHW etc;
- the PSNI Information Governance Delivery Group – which reports directly to PSNI's SIRO and Executive Committee on the management of data related risks – providing top-level oversight of data protection strategy, policy, and governance across the PSNI, including reviewing the highest risk data protection impact assessments (DPIAs) referred to it by the DPO or business owner;
- the appointment and training of Information Asset Owners (IAOs) to be responsible for the management of assigned information assets, including the identification and mitigation of risks arising from the processing of personal data, and ensuring the appropriate documentation is maintained for each of PSNIs processing activities;
- the establishment, management and on-going data protection training across the organisation.
- PSNIs Information Security Unit being responsible for advising the business on the organisational measures and technical controls required to protect the security and integrity of personal data processed by PSNI;
- PSNI information and Communications Service being responsible for advising system developers and managers to ensure that risks to PSNI data and the systems on which it is processed, stored and transmitted are identified and mitigated;
- implementing appropriate security measures in relation to the personal data we process by using the above governance, policy, guidance, and processes (such as the DPIA) to ensure officers/staff access to personal data and/or to systems containing such are limited and monitored;
- regularly reviewing PSNIs accountability measures, and update or amend them when required, and to ensure we take a 'data protection by design and default' approach to our activities, including the design of PSNI systems.

Further information can also be found in PSNIs Data Protection SI9518 which sets out the ways in which PSNI complies with data protection legislation (including integrating data protection by design and default).

B) Principle 1 – 'Lawfulness, Fairness and Transparency'

Lawfulness

As noted above, the lawful basis for the PSNI's processing is in most cases derived from its official functions as a ;aw enforcement agency, and its corporate functions as an employer, and by ensuring all processing is fair, necessary and proportionate to the identified purpose (see 'data minimisation' below) and applicable legal basis.

When processing special category data for the **employment purposes** PSNI ensures the processing is **necessary** and **proportionate** to perform its duties and meet its obligations to the data subject(s) (Part 1 para 1 of Schedule 1 to the DPA 18). This includes processing:

- for compliance with a **legal obligation** in connection with employment and personnel matters (e.g. reporting Trade Union Representative data);
- personal data concerning health in connection with PSNI's rights and duties under employment law;
- data relating to criminal convictions in connection with recruitment, discipline or dismissal.

This list is not exhaustive - further details are recorded in PSNI's Information Asset Register (IAR).

The specific conditions under which data may be processed for reasons of **substantial public interest** are set out in paragraphs 6 to 28 of Schedule 1 of the DPA. As a government department, most of PSNI's processing of special category data for a substantial public interest is in support of its public tasks or functions and in accordance with the purposes set out in para 6(2), Part 2, Schedule 1:

- exercise of a function conferred on a person by an enactment or rule of law; and/or
- exercise of a function of the Crown, a Minister of the Crown or a government department.

PSNI meets the further requirements of Part 2 Schedule 1 by ensuring it only processes such data where it is in the substantial public interest and the processing is necessary and proportionate to perform the specific lawful functions of the PSNI. We do this in various ways, including by:

- providing all officers/staff with training on how to comply with the privacy and data protection legislation
- providing standard contractual clauses for contractors working for
- tailored advice is also provided by the DPO across PSNI, and via the networks described in the above section on Accountability;
- using the DPIA process to ensure our collection and subsequent processing of data is appropriate;
- ensuring our IAOs are trained to fulfil their responsibilities; and
- taking the further steps set out in the 'data minimisation' section below.

PSNI may, on occasion, rely on other conditions in Schedule 1, such as:

- para 8, 'Equality of opportunity or treatment' to ensure compliance with our obligations under legislation such as the Equality Act 2010 and Sex Discrimination Act 1970; or,
- para 10, 'preventing or detecting unlawful acts', if providing information to other law enforcement bodies;
- para 18, 'Safeguarding of children and of individuals at risk', for example, if any of our safeguarding teams identify an at risk individual for referral to social services, a GP, or other relevant professional;
- para 24, 'Providing information to elected representatives' such as Members of Parliament in response to a data subjects requests for assistance.

Fairness and Transparency

Detailed information about how the PSNI uses personal data, including special category data, is published in the PSNI's privacy information notices which provide high-level information about how the PSNI uses personal data, PSNIs obligations as a data controller and data subjects rights.

PSNI is also bound by the public sector equality duty and HM Government's Data Ethics Framework. Both are followed to ensure appropriate and responsible data use. PSNI conducts Equality Impact Assessments (EIAs) where appropriate to assess the fairness and likely impact of policy decisions on particular groups and to ensure it develops policies and delivers services which are fair and just and uses the Ethics Framework to ensure ethical considerations are addressed within PSNI projects.

a) Principle 2 - 'purpose limitation'

PSNI only processes personal data when permitted to do so by law. Personal data is collected for specific, explicit and legitimate purposes and will not be further processed for reasons that are incompatible with the purposes for which the data was originally collected for the PSNI, unless that processing is permitted by law. Where the PSNI obtains data on a basis that imposes specific purpose (or other) limitations, then such data will not be processed in any way that is incompatible with those further specific limitations.

Privacy information notices are used to inform individuals of the legitimate purposes for which data will be processed, and PSNI uses the governance, policy, and processes outlined above to ensure it meets these requirements.

b) Principle 3 - 'data minimisation'

PSNI will in each case collect only the personal data that is needed for the particular purpose/purposes of its processing, ensuring it is necessary, proportionate, adequate and relevant.

Additionally, PSNI internal guidance, training and policies require officers/staff to use only the minimum amount of data required to enable specific tasks to be completed.

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

c) Principle 4 - 'accuracy'

Data subjects are required to notify the PSNI of relevant changes in their personal details, such as changes of address or marital status.

Details of how to do this will be provided at the point of data collection and/or via PSNI website, and its privacy notices. PSNI systems are designed to allow for changes to personal data to be made, or for data to be erased where appropriate to do so.

If a change is reported by a data subject to one part of the PSNI, whenever possible this is also used to update other services, both to improve accuracy and avoid the data subject having to report the same information multiple times.

Where permitted by law, and when it is reasonable and proportionate to do so, PSNI processes may include cross-checking information provided by a data subject with other organisations – for example local authorities or sponsors, to ensure accuracy.

If PSNI decides not to either erase or rectify the data, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision and, unless an exemption applies, inform the data subject of this outcome.

d) Principle 5 - 'storage limitation'

PSNI has a retention and disposal schedule in place and separate retention periods for its operational records/casefiles based on relevant legislation and the period for which information is needed for a justified business process. Also some types of information have specific policies – for example, where information relates to court proceedings or contractual arrangements.

Commented [MN3]: Hyperlink not working

All special category data processed by the PSNI for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in these policies. PSNI retention schedules are reviewed regularly and updated when necessary.

Sensitive data processed on the basis of consent is also retained for the periods set out in these policies unless consent is revoked before then: details of how to revoke consent are provided when the data is collected, and details of how to contact PSNI's DPO are published on our website.

e) Principle 6 - 'integrity and confidentiality'

PSNI systems are designed to ensure to the greatest extent possible personal data cannot be corrupted when it enters or is processed within them; this includes ensuring adequate security for example to guard against hackers who might try to corrupt the data, and a method for monitoring the ongoing integrity of inputted data, for example, by the production of regular data quality reports.

The PSNI has a range of security standards and policies based on industry best practice and government requirements to protect information from relevant threats. We apply these standards whether PSNI data is being processed by our own staff, or by a processor on our behalf. The security policy framework for government is published on gov.uk.

All officers/staff handling PSNI information or using an official system must have the appropriate security clearance and are 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 PSNI branches and districts, PSNI 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.

7. Monitoring and Review

PSNI will formally review this document not less than six months after its introduction (not later than the end of May 2022) and yearly thereafter.

This document will be made available to the Information Commissioner on request, in accordance with s42(3)(c) of the DPA.