Police Service of Northern Ireland

Sensitive Processing for Law Enforcement Purposes, under Part 3 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

1. Aims 3
2. Introduction 4
3. Governance and Responsibility 4
4. Lawful Basis and Conditions 5
5. Compliance with Data Protection Principles 8
6. Monitoring and Review 15

Police Service of Northern Ireland

1. Aims

This policy aligns with PSNIs existing SI0518 Data Protection reflects the Home Office Appropriate Policy Document (APD) and is produced in accordance with our obligations under sections 35(4) and 35(5) of Part 3 of the Data Protection Act 2018 ("DPA 2018").

This policy applies to sensitive processing – as defined in section 35(8) DPA – undertaken by the PSNI in accordance with Part 3 of the DPA 2018. PSNI processing of special category data for general purposes is covered in a separate document APD for sensitive processing, UK GDPR/Part 2.

Commented [MS1]: Link not working

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.

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 3 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 8, or (in rare cases) 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 is the appropriate policy document (APD) for the PSNI produced in accordance with its obligations under sections 35(4) and 35(5) of Part 3 of the Data Protection Act 2018 ("DPA 2018").

This policy meets the requirements in section 42 DPA 2018 to set out the safeguards PSNI has in place for sensitive processing carried out for a law enforcement purpose when acting in its capacity as a competent authority. It should be read alongside the PSNI's Data Protection Policy, and APD for sensitive processing under UK GDPR/Part 2. The PSNI's Adult Privacy Notice and Information Asset Register (IAR) also provides more detailed information about its processing.

Commented [MS2]: Link not working

3. Governance and Responsibility

Legal Obligations

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.

Police Service of Northern Ireland

4. Lawful Basis and Conditions

Lawful Basis for Sensitive Processing

Section 35(3) of the Data Protection Act 2018 (the first data protection principle: law enforcement processing) provides sensitive processing (as defined in section 35(8) DPA) for any of the law enforcement purposes is permitted only in the two cases set out in sections 35(4) and (5):

- 35(4): where the data subject has given consent to the processing for the law enforcement purpose; or,
- 35(5): the processing is strictly necessary for the law enforcement purpose and it meets at least one of the conditions in Schedule 8.

An additional requirement for both conditions is that the controller must, at the time the processing is carried out, have an appropriate policy in place.

PSNI officers and staff must therefore have regard to this policy when carrying out sensitive processing on behalf of the PSNI, when it is acting in its capacity as the competent authority and controller of the personal data. When the PSNI is acting in the capacity of a processor it will do so in accordance with the instructions and policies set by the controller in each case.

PSNI has considered whether in the course of its official functions there are additional types of data that should be treated as sensitive processing although not prescribed as such under the Law Enforcement Directive and Part 3 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 of the data subject as sensitive processing. Where other data (such as nationality data in some specific cases) is processed in such a way as to reveal characteristics amounting to sensitive 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 processing.

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 the department to treat all data as sensitive processing (even when it is not legally necessary or required to be processed as such).

Police Service of Northern Ireland

Conditions for Sensitive Processing

Organisations that have a law enforcement function and are designated as competent authorities can process personal data for law enforcement purposes – defined in section 31 DPA, which includes processing for the purpose of the prevention, detection, investigation or prosecution of criminal offences – and when they do, such processing must be in accordance with Part 3 DPA 2018. As a Law Enforcement Agency, the PSNI is a competent authority in accordance with schedule 7, para 1, DPA 2018 in respect of the law enforcement activities it carries out as part of its official functions.

PSNI is most likely to carry out 'sensitive processing' for a law enforcement purpose on the basis of 'strict necessity' under s.35(5). It is also able to rely on consent under s.35(4), but consent is not always a primary necessity and particularly in situations where the lawfulness of the consent could be challenged if the police are in a more powerful position than the data subject who had given their consent or if consent is highly likely to be withheld or withdrawn.

PSNI is therefore required to have this Appropriate Policy Document in place for both scenarios, and when relying on the s.35(5) condition to permit such processing to also meet at least one of the additional conditions prescribed in schedule 8 DPA.

The schedule 8 conditions for sensitive processing that the PSNI is most likely to rely on are:

- para 1, 'statutory etc purposes', where the sensitive processing is necessary to fulfil one of its official law enforcement functions and/or is in accordance with its responsibilities under legislation, as well as other relevant law (including under common law), and where the processing is necessary for reasons of substantial public interest for example:
  - Data Protection Act 2018, part 3
  - Police (NI) Act 2000
  - Powers or duties conferred under amendments to the Police and Criminal Evidence Act 1984;
- para 2, administration of justice', for example, for processing in relation to the handling of mutual legal assistance (MLA) claims;

- para 4, ‘safeguarding of children and of individuals’, for example, where the sensitive processing is necessary to protect an individual, such as a child or a person at risk -- for example domestic violence;
- para 5, ‘personal data already in the public domain’, for example if considering information available via the internet when deciding whether to proceed with an investigation;
- para 6, ‘legal claims’, also for processing data in relation to MLA claims.

PSNI may on occasion also rely on other conditions in Schedule 8, such as:

- para 3, ‘protecting individual’s vital interests’;
- para 7, ‘judicial act’
- para 8, preventing fraud;
- para 9, ‘Archiving etc.’.

Police Service of Northern Ireland

5. Compliance with Data Protection Principles

Section 34 of the DPA sets out the data protection principles which apply to the processing of personal data by a competent authority for a law enforcement purpose. The procedures PSNI has in place to ensure compliance with these when carrying out sensitive processing is set out below.

a) Principle of 'Accountability'

PSNI has put in place appropriate technical and organisational measures to meet the requirements of accountability (as required by s.34(3)). 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 organisation;
- a direct reporting line from the DPO to our highest management levels;
- the development and regular review of corporate data protection policies and guidance for officers/staff setting out how PSNI meets its data protection obligations – such as how to ensure new projects, applications or systems meet the technical 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,;
- PSNIs Information Governance Delivery Group – which reports directly to the PSNI's Senior Information Risk Owner and Senior Management on the management of data related risks – providing top-level oversight of data protection strategy, policy, and governance across the organisation;
- the appointment and training of Information Asset Owners (IAOs) (at SCS level where appropriate) 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 that the appropriate documentation is maintained for each of our processing activities;

- the establishment, management and on-going Data Protection Training across the organisation, providing officers/staff with advice on data protection matters and steps to ensure compliance within their local business area;
- PSNI Information Security Unit being responsible for advising the business on the organisational measures and controls required to protect the security and integrity of personal data processed by PSNI;
- PSNI Information and Communication Services 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 arrangements, 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 our 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 our Data Protection Policy which sets out the ways in which PSNI complies with data protection legislation (including integrating data protection by design and default), and in the APD for sensitive processing, UK GDPR/Part 2

Commented [MS3]: Link not working

b) Principle 1 - 'lawful and fair'

Lawful

The lawfulness of PSNI's processing for law enforcement purposes is in most cases derived from its official functions and statutory/common law powers, and by additionally ensuring all processing is necessary and proportionate to the identified law enforcement purpose (see 'data minimisation' below).

PSNI gathers and holds personal information which it uses for policing purposes. The policing purposes are set out in Part 6 of the Police (Northern Ireland) Act 2000. It states that it shall be

the general duty of police officers to protect life and property, preserve order and to prevent the commission of offences and, where an offence has been committed, to take measures to bring the offender to justice. They provide the legal basis for collecting, recording, evaluating, sharing and retaining police information.

The PSNI processes personal data for three broad purposes:

1. Policing;
2. Staff administration;
3. The provision of services to support the Policing Purpose.

The PSNI is also obliged to process information when required to do so by other legal obligations including enactments, court orders, or common law reasons and also for research and statistical purposes, including the production of official statistics. On the unique occasion where the PSNI relies solely on consent to process personal data, individuals should be aware that they have the right to withdraw this consent at any time. Where the PSNI have a legal basis to process information, consent will not be sought and will not be the basis relied upon to process that information.

As a competent authority within the meaning outlined in section 30 of the Data Protection Act 2918, PSNI's law enforcement functions are set out in section 31 of the Data Protection Act 2018 and include 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.

As a 'competent authority' PSNI must also comply with the Data Protection Act 2018 which contains, at Part 3, those provisions that relate to the processing of personal data for law-enforcement reasons. The Chief Constable of the PSNI is registered with the Information Commissioner as a 'Data Controller' for the purposes of this legislation. As such, he is obliged to ensure that the PSNI handles all personal data in accordance with the legislation.

Strictly necessary

When PSNI carries out sensitive processing it will mainly be in reliance on the 'strictly necessary' criteria (s.35(5)), and must meet at least one of the permitted conditions set out in Schedule 8 DPA – the ones the PSNI is most likely to rely on are listed in section 2 above.

Before carrying out sensitive processing PSNI officers/staff must undertake an assessment to determine whether the proposed processing is strictly necessary for and proportionate to the specified law enforcement purpose being pursued and schedule 8 condition, and whether it will serve a substantial public interest. If the aim could be achieved by other means -- such as by not processing the data, or limiting the processing to data that is not sensitive, or by using an anonymised version – the sensitive processing will not take place. The outcome of the assessment must be documented in line with local policies and guidance and retained for a period of at least six months after the processing has ceased.

We ensure staff who might carry out sensitive processing are trained to understand their obligations when processing personal data, and provided with local guidance specific to the area of law enforcement work they are engaged in on how to assess and record their decision-making on a case-by-case basis about whether the processing is strictly necessary etc. Further details of how we ensure this are set out in the PSNI's **APD for UK GDPR /Part 2 DPA**

Consent

The PSNI is also able to rely on consent as permitted by section 35(4) as the basis for its sensitive processing. While we are not aware of this being relied upon in the context of law enforcement processing, were it necessary to do so we would ensure data subjects are provided with a Privacy Information Notice and that explicit consent for each data item is sought, data subjects are informed they have the right to withdraw their consent at any time, are provided with details of how they can do this, and that the PSNI has processes in place to easily facilitate any withdrawal of consent.

Fairness

High-level information about how the PSNI uses personal data, including sensitive processing, is published in the **PSNI's Adult Privacy Notice.**

As a competent authority and data controller the 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. The 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 – 'specified, explicit and legitimate'

PSNI only carries out sensitive processing when permitted to do so by law. Such personal data is collected for specific, explicit and legitimate purposes -- such as medical data for the issuing of firearms licensing -- and will not be further processed for reasons that are incompatible with the purposes for which the data was collected (unless allowed for under s.36(2)).

PSNI uses the governance, policy and processes outlined above (and expanded on in the APD for the processing of Sensitive Data under UK GDPR/Part 2) to ensure it meets these requirements.

b) Principle 3 - 'adequate, relevant and not excessive'

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

Each form or process will not prompt data subjects to answer questions and provide information that is not required, nor (as far as possible) will they require data subjects to provide the same information, such as date of birth or address, repeatedly to the department: application forms will

instruct data subjects to skip questions that either do not apply, or which they have already answered, and digital processes will be designed in the same way.

Additionally, PSNI internal guidance, training and policies require 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 - 'accurate and up to date'

When the PSNI becomes aware that personal data is inaccurate or out-of-date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, the reason for that decision will be documented.

Data subjects and partner organisations including processors and joint controllers are required to notify PSNI of relevant changes, such as changes of address. Where permitted by law, and when it is reasonable and proportionate to do so, PSNI may check this information with other organisations before amending details on our records.

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

Categorisation of data

PSNI will, as far as possible, distinguish between personal data based on facts and personal data based on personal assessments or opinions by marking the file/information to reflect the distinction.

Where relevant, and as far as possible, we will also distinguish between personal data relating to different categories of data subject in order to fulfil our obligations under section 38(3) DPA, such as:

- People suspected of committing an offence or being about to commit and offence
- People convicted of a criminal offence
- Known or suspected victims of a criminal offence
- Witnesses or other people with information about offences.

This will be done by marking the file/information in accordance with guidance specific to the system/type of file on which the data is being recorded, and by ensuring new systems are designed with this functionality.

PSNI only does the above where the personal data is relevant to the law enforcement purpose being pursued.

Verification of data before transmission

PSNI will take reasonable steps to ensure that personal data which is inaccurate, incomplete or out-of-date is not transmitted or made available for any of the law enforcement purposes. Where possible and practicable, we do this by verifying any data before sending it externally or otherwise making it available, and by providing the recipient with the necessary information we hold to assess the accuracy, completeness and reliability of the data, including how up-to-date it is.

PSNI will document all decisions to make personal data available for any of the law enforcement purposes and, if we discover after transmission that the data was incorrect or should not have been transmitted, we will inform the recipient as soon as possible.

The HO uses the governance, policy and processes outlined above (and expanded on in the APD for the processing of Sensitive Data under UK GDPR/Part 2) to ensure it meets these requirements.

d) Principle 5 - 'kept no longer than is necessary'

PSNI has a records retention and disposal schedule in place, which is published online. Most record types have separate tailored retention policies, as the period for which information is necessary for the purpose for which it is processed will differ e.g. MOPI categories.

Police Service of Northern Ireland

Retention that is lawfully based on consent must also facilitate the withdrawal of such consent.

PSNI has a process to facilitate data subjects rights to request erasure, amendment, restricted processing etc. Requests can be made using the DAT3 form emailed to zenhancedrequests@psni.police.uk

e) Principle 6 - 'processed in a secure manner'

Relevant 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 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.

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 staff handling PSNI information or using an official system must have the appropriate security clearance and are required to complete mandatory training on the importance of security, and how to handle information appropriately.

In addition to having security guidance and policies embedded throughout the organisation, 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.

6. Monitoring and Review

Police Service of Northern Ireland

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 on request to the Information Commissioner pursuant to s42(3)(c) of the DPA.