



Adult Privacy Notices

Individuals have the right to be informed about how their personal data is handled by the Police Service of Northern Ireland ('PSNI'). This document explains how the PSNI processes¹ personal data². It details the steps we take to ensure that it is protected, and also describes the rights individuals have with regard to personal data handled by PSNI.

From the 25th May 2018 the processing of personal data is governed in the United Kingdom by the Data Protection Act 2018 and the General Data Protection Regulations (GDPR). The GDPR will cover all processing of personal information by PSNI for all non- law-enforcement purposes. 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.

This privacy notice serves as an overarching document for PSNI. Additional privacy notices exist which are specific to certain processes and procedures within PSNI. Explicit lawful processing conditions will be set out in these tailored documents, for example, a witness statement.

1. Why do we process personal data and under what basis?

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.

¹ 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

² 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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.

2. How do we process personal data?

The PSNI must ensure compliance with data protection principles; therefore, staff are directed by relevant policies and procedures in relation to data protection. In order to meet these standards the PSNI will ensure data is processed in a specified, legitimate, adequate, accurate, timely manner with stringent security controls. The PSNI maintains a record of processing activities throughout the organisation in order to retain these standards. We will only process personal data by lawful means and in line with processing conditions, for personal and Special Category Data³ as dictated in legislation.

3. What types of personal data do we handle?

PSNI holds information relating to a range of individuals including victims, witnesses, complainants, suspects and offenders, in connection with this policing purposes as well as details of others who work for or with PSNI. The PSNI may process both personal information and special category information relating to or consisting of the following:

Personal details such as name, date of birth, address and biographical details	Physical identifiers including DNA, fingerprints and other genetic samples
Family, lifestyle and social circumstances	Criminal proceedings, outcomes and sentences
Religious or other beliefs of a similar nature	Physical or mental health or condition
Education and training details	Employment details
Financial details	Goods or services provided
Racial or ethnic origin	Political opinions
Trade union membership	Offences (including alleged offences)

³ Reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership. Is genetic data or biometric data used to uniquely identify a person. Is data concerning health or concerning a person's sex life or sexual orientation.

Sound and visual images	Licenses or permits held
Criminal Intelligence	Sexual life/Sexual orientation
References to manual records or files	Complaint, incident and accident details

This information will be held both electronically and in hard copy. Electronic records include information stored on a computer and CCTV, while hard copy records include paper records, i.e. in a file.

4. Whose personal data do we handle and where do we obtain it from?

The PSNI may process personal data relating to a wide variety of individuals (data subject); this data can come from a wide variety of sources, these are noted below:

Data Subject	
Witnesses and victims	Correspondents, enquirers and complainants
Offenders and suspected offenders	Personnel including permanent police officers and police staff, volunteers, agents, temporary and casual workers
Relatives, guardians and associates of the individual concerned	
Other individuals necessarily identified in the course of police enquiries and activity	Former and potential members of staff, pensioners and beneficiaries
Advisers, consultants and other professional experts	Suppliers
Data Source	
Individuals themselves including witnesses, victims, offenders, suspected offenders and persons making an enquiry or complaint	PSNI may also obtain personal data from other sources such as its own CCTV systems, or correspondence
Relatives, guardians or other persons associated with the individual	Producers of statistics and research including surveys ⁴
Employees of PSNI	Private sector organisations working with the police in anti-crime strategies
Ombudsmen and regulatory authorities	Voluntary sector organisations
Prisons	Auditors
HM Revenue and Customs and other law enforcement agencies	Current, past or prospective employers of the individual
Courts, legal representatives, prosecuting authorities and defence solicitors	Healthcare, social and welfare advisers or practitioners
Her Majesty's Inspectorate of Constabulary	Education, training establishments and examining bodies
Central and Local government - governmental agencies and departments	Business associates and other professional advisors
The media	Suppliers, providers of goods or services
Emergency services	Persons making an enquiry or complaint
Licensing authorities	Financial organisations and advisors
Security companies	Survey and research organisations

⁴ PSNI, like many police forces, may use a private company/ies to undertake some surveys on our behalf with strict controls to protect the personal data of those involved.

Partner agencies involved in crime and disorder strategies	Trade, employer associations and professional bodies
Voluntary and charitable organisations	Publicly accessible sources e.g. internet search

5. How long does the PSNI retain personal data?

The PSNI retains information, including personal information, as long as the Service considers necessary for the purpose or purposes for which it was collected. The time periods are as detailed in the Service Review, Retention and Disposal Schedule, available online.

6. How do we ensure the security of personal information?

PSNI takes the security of all personal information under our control very seriously; we have a number of policies in place which provide detailed procedures on specific information security controls, countermeasures and practices which must be adhered to. We will comply with the relevant parts of the legislation relating to security. We will ensure that appropriate policy, training, technical and procedural measures are in place, including audit and inspection, to protect our manual and electronic information systems from data loss and misuse, and only permit access to them when there is a legitimate reason to do so, and then under strict guidelines as to what use may be made of any personal data contained within them. These procedures are continuously managed and enhanced to ensure up-to-date security.

7. Who do we disclose personal data to?

In order to carry out the purposes described under paragraph 1 above the PSNI may disclose personal data to a wide variety of recipients. This will include, but not be limited to disclosures to those listed as “data sources” in section 4 including, law enforcement agencies, partners in criminal justice, and to bodies or individuals working on our behalf such as contractors or survey organisations for example within the Criminal Justice System as part of the pre-charge and post charge processes, i.e. prosecuting someone through the Court. We may also disclose to other bodies or individuals where necessary to prevent harm to individuals. Disclosures of personal data will be made on a case-by-case basis, using the personal data appropriate to a specific purpose and circumstance, and with necessary controls in place.

Some of the bodies or individuals to which we may disclose personal data are situated outside of the European Union - some of which do not have laws that protect data protection rights as extensively as in the European Union. If we do transfer personal data to such

territories, we will take proper steps to ensure adequate safeguards are in place as required by the Data Protection legislation and policing guidelines.

PSNI will also disclose personal data to other bodies or individuals when required to do so by, or under, any act of legislation, by any rule of law, and by court order such as to other professional or regulatory bodies PSNI may also disclose personal data on a discretionary basis where it is necessary for the purpose of, and in connection with, any legal proceedings or for obtaining legal advice. Any disclosure of personal information is carefully considered in accordance with legislation, policy, and/or information sharing agreements governing that sharing.

8. What are the rights of the individuals whose personal data is handled by the PSNI?

Individuals have various rights enshrined in the Data Protection legislation, these are detailed below. Further detail on these rights can be accessed within Articles 15 – 23 of the GDPR and Part 3 of the Data Protection Bill. The PSNI are permitted to ask data subjects to provide proof of their identity before giving effect to their rights. This ensures the security of your personal information. Requested information or responses to individuals requesting their rights are enacted should be provided, subject to exemptions⁵, to the individual without undue delay and in any event within one month of receipt of the request and free of charge. Where a controller receives large numbers of requests from individuals, or they are especially complex, the time limit may be extended by a maximum of two further months. Requests deemed excessive or manifestly unfounded will not be processed. Individuals will be made aware of this extension and the reasons for delay explained. The PSNI will process any requests from individuals in relation to these rights; however, where PSNI have a legitimate business purpose for processing this data, or an exemption applies, PSNI does not have to give effect to the right. We will communicate this to you and highlight our reliance on the Data Protection legislation for this. By requesting your rights are enacted, the PSNI will be required to further process your personal information in order to keep a record of what amendments, if any, have been made and the justification for any decisions made. Where PSNI need to enact the rights of rectification, erasure and restriction, we will do so as far as is reasonably practicable.

The Right to Access

⁵ There may be occasion where individuals will not be entitled to their personal data, for example, to protect the rights of others. More information on exemptions can be found on the ICOs website - www.ico.gov.uk

Subject Access is the most commonly exercised right. Individuals can request a copy of their personal data and other information about how PSNI processes your information. Where PSNI withholds some/all of the requested information we will provide details, where possible, around the decision in line with Data Protection legislation.

The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If PSNI has disclosed the personal data in question to third parties; we must inform them of the rectification where possible. We will also inform the individuals about the third parties to whom the data has been disclosed, where appropriate. Where the PSNI is not taking action in response to a request for rectification, we will provide details around the decision.

The right to erasure

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances including, if consent is withdrawn, the data was processed unlawfully, compliance with legal obligation, and where processing is no longer necessary for the purpose it was originally collected.

There are some specific circumstances where the right to erasure does not apply and PSNI can refuse to deal with a request including, if it is necessary to meet a legal obligation or defend a legal claim.

The right to restrict processing

In certain conditions individuals have a right to request PSNI 'block' or suppress/restrict processing of personal data such as where individuals dispute the accuracy of their information or the processing is no longer needed.

Once processing is restricted, the PSNI is permitted to store the personal data, but not process it further except on limited grounds such as with individual's consent or in relation to legal claims. If the PSNI has disclosed the personal data in question to third parties, we must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The PSNI must inform individuals before any restriction is lifted.

As above, the PSNI may be required to restrict processing when an individual has contested the accuracy of data or has objected to the processing and these issues are being investigated. Or when the data subject has opposed erasure or requires the data to be retained in order to progress a legal claim.

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services, this includes individuals being provided with their data in a commonly used electronic format in order that it can then be easily transferred or 'ported' to another data controller as and when required (either by the individual themselves, or PSNI). This right only applies to personal data which an individual has provided to PSNI which is processed by automated means; by virtue of the individual's consent or for the performance of a contract. The right to data portability does not extend to processing of personal information for law-enforcement processing.

The right to object

Individuals have the right to object to processing unless the PSNI can demonstrate explicitly how it is linked to the purposes described under paragraph 1 or the processing is for the establishment, exercise or defence of legal claims. Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling), and processing for purposes of scientific/historical research and statistics. The right to object does not extend to processing of personal information for law-enforcement processing.

Rights in relation to automated decision making and profiling

Although the PSNI is unlikely to carry out any automated decision-taking or automated profiling that does not involve some human element, an individual has the right to require that PSNI ensures that no decision that would significantly affect them is taken by PSNI or on its behalf purely using automated decision making software.

Further details on all of the rights within Data Protection legislation can be found on the Information Commissioner's Office website at www.ico.org.uk.

9. Monitoring

PSNI may monitor or record and retain telephone calls, texts, emails and other electronic communications to and from the Service in order to deter, prevent and detect inappropriate or criminal activity, to ensure security, and to assist the purposes described under section 1

above. PSNI does not place a pre-recorded 'fair processing notice' on telephone lines that may receive emergency calls (including misdirected ones) because of the associated risk of harm that may be caused through the delay in response to the call.

The PSNI will utilise CCTV within their establishments for the security and protection of the Police Estate.

10. Contact Us

If you would like to exercise any of the rights discussed in this document, you can do so by contacting the following department.

Corporate Information

Police Service of Northern Ireland
Police Headquarters
65 Knock Road
Belfast
BT6 5LE
Telephone: 02890700164
Email: DataProtection@psni.pnn.police.uk

The PSNI has a designated Data Protection Officer (DPO). The DPO is an independent advisor to the PSNI and is responsible for ensuring that PSNI are processing personal data in line with the legislation. Any individual with concerns over the way PSNI handles their personal data may contact our Data Protection Officer at the address above or by email via DataProtectionOfficer@psni.pnn.police.uk

If you remain unhappy about how your request has been handled you have the right to apply directly to the information Commissioner. The Information Commissioner is the independent regulator responsible for enforcing the legislation and can provide useful information about the legislation's requirements. Our local Information Commissioner's address is:

Information Commissioner's Office

3rd Floor
14 Cromac Place
Belfast, BT7 2JB
Tel: 028 90278757
Email: ni@ico.org.uk