

**POLICE OMBUDSMAN FOR NORTHERN IRELAND**

**Data Protection Policy**

POLICY OWNER: Data Protection Officer

POLICY APPROVED BY: Police Ombudsman

IMPLEMENTATION DATE: 1 January 2024

VERSION: 2.0

NEXT REVIEW: 1 January 2027

**Contents**

1. Scope
2. Definitions
3. The Police Ombudsman’s Office
4. The Police (Northern Ireland) Act 1998
5. Processing personal information
6. A Principled Approach to Data Protection
7. Data Sharing
8. Data Protection Impact Assessments
9. Review

APPENDIX A: Section 63 of the Police (Northern Ireland) Act 1998

APPENDIX B: Relevant Legislation and Regulations

APPENDIX C: Role of the Data Protection Officer

APPENDIX D: Handling of Shared Information

# Scope

## This Data Protection Policy applies to the processing of personal data, including special category data necessary for the purposes of the functions of the Police Ombudsman for Northern Ireland (the Ombudsman).

## This policy should be read in conjunction with the Office’s Data Protection Appropriate Policy Document for Law Enforcement Processing, its Privacy Notices and with its Retention and Disposal Schedule.

## The Ombudsman as controller processes this information primarily for the purpose of meeting the legal requirement to ensure an efficient and effective system that has the confidence of the police and the public. She does so to meet other legal requirements in matters including employment, equality, health and safety and human rights.

## The aim of this policy is to explain how the Office’s processing of personal information meets the requirements of the Police (Northern Ireland) Act 1998 (the 1998 Act) and Data Protection legislation and related Codes of Practice. (see Appendix B).

## This policy has been approved by the Police Ombudsman. The Police Ombudsman and her staff must comply with this policy and all related data protection policies and procedures (including Information Commissioner Codes of Practice).

# Definitions

## This policy uses a number of terms also defined in the Data Protection Act 2018 (the DPA 2018). For the purposes of clarity, it sets out an understanding of those terms:

## In using the term “processing”, means “an operation or set of operations which is performed on information, or on sets of information such as –

1. collection, recording, organisation, structuring or storage,
2. adaptation or alteration,
3. retrieval, consultation or use,
4. disclosure by transmission, dissemination or otherwise making available,
5. alignment or combination, or
6. restriction, erasure or destruction of that information.

## In using the term “data subject” means any identified or identifiable living individual to whom personal data relates.

## In using the term “personal data” we mean any information relating to an identified or identifiable living individual.

## Reference to “special categories of personal data” means any data, which would reveal information about a person’s racial or ethnic origin, their political opinions, their religious or philosophical beliefs, their health; an individual’s sex life or sexual orientation or whether they are a member of a trade union. It may also include the processing of genetic data, or of biometric data, for the purposes of uniquely identifying an individual;

## When we use the term ‘controller’, we mean the authority, which determines the purpose and means of processing personal information. The Police Ombudsman is the controller for these purposes.

## By using the term ‘processor’ we are referring to the person who acts on the ‘controllers’ behalf.

# The Police Ombudsman’s Office

## The Office of the Police Ombudsman for Northern Ireland was established by Part VII of the Police (Northern Ireland) Act 1998. The Ombudsman must exercise her powers so as to secure an efficient, effective and independent police complaints system, and to do so in the way she thinks best calculated to secure the confidence of the public and of the police in that system (section 51(4) of the 1998 Act).

## The Police Ombudsman investigates complaints about the officers of the following bodies exercising police powers when operating in Northern Ireland:-

* The Police Service of Northern Ireland including designated civilians
* The Belfast Harbour Police
* The Belfast International Airport Police
* The Ministry of Defence Police
* The National Crime Agency

## In addition, she has jurisdiction to investigate serious[[1]](#footnote-1) complaints about:

* Mutual Aid police officers from Great Britain
* Home Office employees (Immigration officers, designated customs officials and custom revenue officials)
* Independent Commission for Reconciliation and Information Recovery (ICRIR) officers[[2]](#footnote-2)

## When the Ombudsman and her staff receive, assess, investigate and report on a complaint or referral about the conduct of a police officer she does so for the performance of a task carried out in the public interest or in the exercise of the Ombudsman’s authority, including that which is necessary for administration of justice. This includes processing for law enforcement purposes[[3]](#footnote-3). This processing is for the purpose 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 Police (Northern Ireland) Act 1998

## Part VII of the 1998 Act provides for the independent investigation of complaints about the conduct of police officers by the Ombudsman. The 1998 Act provides for the lawful processing of personal information. It includes:

* Section 61AA allows the Police Ombudsman to provide such statistical information and any other general information as is required to enable the Policing Board to carry out its functions.
* Section 62 allows the Police Ombudsman to publish a statement as to her actions, her decisions, determinations, and the reasons for these.
* Section 63 places restrictions on the disclosure of information (including personal data) obtained by the Ombudsman and her staff. (see Appendix A)

## For further information on the functions of the Ombudsman, please visit the website at [www.policeombudsman.org](http://www.policeombudsman.org).

# Processing personal information

## The Ombudsman processes personal information for the purposes of providing an independent police complaints system for Northern Ireland. This will include processing data for law enforcement purposes. For more information of how the Office compiles with the DPA 2018, see our Appropriate Policy Document for Law Enforcement Processing.

## There may be circumstances when it will be necessary to process personal data for both law enforcement and non-law enforcement purposes. For example, there may be an investigation into several allegations of conduct only some of which are potentially criminal. Personal data, which the Ombudsman obtained for a law enforcement purpose, may also be used in disciplinary investigations, proceedings and unsatisfactory performance proceedings. The Information Commissioner’s Office has provided guidance on law enforcement processing[[4]](#footnote-4).

# A Principled Approach to Data Protection

The DPA 2018 sets out the principles by which organisations must process and protect the information they hold. The Ombudsman processes personal information, which meets the following principles:

## Accountability:

The Ombudsman has put in place measures to meet the requirements of accountability, which are regularly reviewed. These include:

* The appointment of a Data Protection Officer who reports directly to the CEO and Police Ombudsman.
* Integration of the concept of ‘data protection by design and default’ into all processes and activities.
* The maintenance of records of its processing activities.
* The adoption and implementation of data protection policies and data sharing agreements.
* Regular monitoring and maintenance of these policies.
* Security measures for the protection of personal data processed and
* Data protection impact assessments for high risk processing.

## Lawful and fair

Processing of personal information must be lawful and fair.

The Ombudsman’s Office acts lawfully and in compliance with the 1998 Act and related legislation and regulations. Our processing of personal information, including special category information, is necessary for the exercise of a function conferred on the Ombudsman for the purposes of the legislation listed in Appendix B. We use Privacy Notices to inform data subjects of the purpose for which their personal data is processed. These can be found at www.policeombudsman.org

## Specified, explicit, legitimate, and processed for the purpose it was collected.

The Ombudsman’s Office collects personal data and undertakes sensitive processing solely for the purpose of its statutory functions of law enforcement and does not use that data for any incompatible purpose. We are explicit about the manner in which personal information is processed and about any intended disclosure(s).

We may disclose personal data obtained for any other purpose provided this is authorised by law and the processing is necessary and proportionate to that other purpose. If the data is shared with another controller, we will document that they are authorized by law to process data for those purposes.

We maintain an Information Asset Register, which details the purpose and legal basis for processing this personal data.

## Adequate, relevant and not excessive

The Ombudsman’s Office does not systematically collect or harvest personal data. We ensure that such processing is adequate, relevant and not excessive in relation to the purpose in which it was processed. Where special category data is provided to us or obtained by us but is not relevant for the Office stated purposes, it will be erased.

## Accurate and where necessary kept up-to-date

The Ombudsman’s Office operates procedures to ensure the quality of the data it holds. Staff are made aware of their obligations to update complainant personal details if notified of any change, Where the Office becomes aware that personal data is inaccurate, having regard to the purpose for which it is being processed, it will take every reasonable step to ensure that this is erased or rectified without delay. The reasons for any decision not to rectify or seek rectification will be documented.

Personal information held in HR, finance and corporate services files is checked for factual accuracy before onward disclosure to a third-party. The recipient will be provided the necessary information to verify and assess the accuracy of the data. If after onward transmission, the Office is aware that personal data was incorrect and should not have been transmitted, the recipient will be informed as soon as possible. Any decisions to disclose personal data available will be documented.

## Retained for no longer than necessary

The Office has a Disposal and Retention schedule, which lists the different categories of information it holds and how long each category of data should be retained. The schedule is based on advice from the Public Records Office NI and regularly reviewed by the Office and approved by the NI Assembly.

All material not marked for retention is destroyed in a secure environment. The remaining material is held securely by the Police Ombudsman’s Office until such a stage, as it shall be transferred to the Public Records Office.

## Kept securely

The information we hold is only available to those staff who need access to it for the purposes of their role within the Ombudsman’s Office.

Electronic information is processed within the Office’s secure networks. Hard copy information is processed within secure premises.

The Office deploys a wide range of technical and procedural controls outlined at Appendix C in order to protect the personal data we hold. These controls are under the oversight of our Information Assurance Security Group. Its principal aim is to oversee all functional data protection and ensure all areas within the Office comply with relevant information security standards. Residual information risk is accepted on behalf of the Office by the Senior Information Risk Owner (the Chief Executive).

# Data Sharing

## The Ombudsman recognises that the sharing of personal data can be beneficial and in the public interest in certain circumstances. The Ombudsman’s Office processes personal data of police officers and member of the public who complain to the Office for law enforcement purposes and also the personal data of staff and those who are job applicants.

## When considering disclosing personal data to another controller (data sharing), the Ombudsman and all staff must comply with section 63 of the 1998 Act and data protection law as well as the ICO Code of Practice on Data Sharing[[5]](#footnote-5). Data Sharing requires an assessment of the risks of the data sharing using a Data Protection Impact Assessment (DPIA). It is good practice to have a data sharing agreement, which follows the following key principles in data protection legislation:

* **Accountability** - The accountability principle means that both the Ombudsman and staff are responsible for compliance with data protection law and relevant Codes of Practice must be able to demonstrate compliance and provide justification for their decisions in this regard.
* **Fairness** - all personal data must be shared fairly and transparently and the Office Privacy Notice LINK outlines the purposes for the disclosure and who we share data with.
* **Lawfulness** – The Ombudsman and staff must identify at least one lawful basis for sharing data before any sharing is commenced.
* **Security** - All personal data must be disclosed securely, with appropriate organisational and technical measures in place.
* **Data Subject Access Rights** - Any data sharing arrangement/agreement entered into by the Ombudsman must be supported by procedures that allow data subjects to exercise their individual rights.

7.3 Personal data can be shared in an emergency, where this is necessary and proportionate. Examples of an emergency situation bare the risk of serious harm to life, or an immediate need to protect national security.

7.4 All Data Sharing Agreements must meet the standards set out in the ICO Code of Practice and be reviewed by the Legal Directorate. The Ombudsman anticipates that all data sharing agreements will be held centrally on TRIM and published on the PONI website.

7.5 The handling of shared information must follow the procedures outlined in Appendix D.

# Data Protection Impact Assessments (DPIA)

8.1 Data protection impact assessments or DPIAs (previously known as privacy impact assessments or PIAs) are a tool that can help you identify the most effective way to comply with your data protection obligations and meet individuals’ expectations of privacy. An effective DPIA will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to your reputation, which might otherwise occur.

8.2 The Ombudsman must carry out a DPIA before you process personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals.

8.3 Processing that is likely to result in a high risk includes (but is not limited to):

* systematic and extensive processing activities, including profiling and where decisions that have legal effects, or similarly significant effects, on individuals;
* large scale processing of special categories of data or personal data relation to criminal convictions or offences;
* using new technologies (for example surveillance systems).

The Ombudsman must take into account the nature, scope, context and purposes of the processing when deciding whether or not it is likely to result in a high risk to individuals’ rights and freedoms.

A DPIA must contain:

* at least a general description of your processing operations and the purposes;
* an assessment of the risks to the rights and freedoms of individuals;
* the measures envisaged to address those risks;
  + the safeguards, security measures and mechanisms in place to ensure you protect the personal data; and
  + a demonstration of how you are complying with Part 3 of the Act, taking into account the rights and legitimate interests of the data subjects and any other people concerned.

8.4 Report to the ICO

When the Ombudsman has carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, she will need to consult the ICO. You cannot go ahead with the processing until you have done so.

The focus is on the ‘residual risk’ after any mitigating measures have been taken. If the DPIA identified a high risk, but the Ombudsman has taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

The Information Commissioner’s Guidance states that the ICO will respond within **six weeks**. This timescale may increase by a further month, depending on the complexity of the processing you intend to carry out.

# Review

## The Ombudsman’s Office reviews and revises all data protection policies and controls as appropriate to ensure the highest standards of data security as part of ongoing information assurance checks. This policy will be reviewed annually every three years.

# APPENDIX A: Section 63 of the Police (Northern Ireland) Act 1998

Restriction on disclosure of information.

63. –

(1) No information received by a person to whom this subsection applies in connection with any of the functions of the Ombudsman under this Part shall be disclosed by any person who is or has been a person to whom this subsection applies except-

(a) to a person to whom this subsection applies;

(b) to the Department of Justice or the Secretary of State;

(c) to other persons in or in connection with the exercise of any function of the Ombudsman;

(ca) for the purposes of an inspection of the Ombudsman carried out by the Chief Inspector of Criminal Justice in Northern Ireland under Part 3 of the Justice (Northern Ireland) Act 2002; [added SR (NI) 2002/414 from 20 Dec 2002]

(d) for the purposes of any criminal, civil or disciplinary proceedings; or

(e) in the form of a summary or other general statement made by the Ombudsman which-

(i) does not identify the person from whom the information was received; and

(ii) does not, except to such extent as the Ombudsman thinks necessary in the public interest, identify any person to whom the information relates.

(2) Subsection (1) applies to-

(a) the Ombudsman; and

(b) an officer of the Ombudsman.

(2A) [added from 4 Nov 2001, am. 2003 c.6 from 8 April 2003] Subsection (1) does not prevent the Ombudsman, to such extent as he thinks it necessary to do so in the public interest, from disclosing in a report of an investigation under section 60A-

(a) the identity of an individual, or

(b) information from which the identity of an individual may be established.

(3) Any person who discloses information in contravention of this section shall be guilty of an offence and liable on summary conviction to a fine not exceeding level 5 on the standard scale.

(4) Nothing in subsection (1)(b) permits the disclosure to the Department of Justice of information—

(a) which has been supplied to the Ombudsman under section 66(1) of the Police (Northern Ireland) Act 2000(a) for the purposes of or in connection with an investigation under section 60A of this Act, and

(b) in relation to which the Ombudsman has been informed under section 66(3)(b) of the Police (Northern Ireland) Act 2000 that the information is, in the opinion of the Chief Constable or the Board, information which ought not to be disclosed on the ground mentioned in section 76A(1)(a) of that Act.

|  |
| --- |
| APPENDIX B: Relevant Legislation and Regulations The legislation which governs the work of the Police Ombudsman's Office is Part VII of the Police (Northern Ireland) Act 1998.  The following is a list of some of the legislation and regulations which also regulates the work of the Office:  Legislation   * Anti-terrorism, Crime and Security Act 2001 * Criminal Appeal Act 1995 * Criminal Justice and Police Act 2001 * Criminal Law Act (NI) 1967 * Criminal Procedure and Investigations Act 1996 * Data Protection Act 2018 * Freedom of Information Act 2000 * Human Rights Act 1998 * Investigatory Powers Act 2016 * Justice (Northern Ireland) Act 2000 * Justice (Northern Ireland) Act 2002 * Justice (Northern Ireland) Act 2004 * Northern Ireland Act 1998 * Police (Northern Ireland) Act 1998 * Police (Northern Ireland) Act 2000 * Police (Northern Ireland) Act 2003 * Proceeds of Crime Act 2002 * Regulation of Investigatory Powers Act 2000 * The Police and Criminal Evidence (application to the Police Ombudsman) Order (NI) 2009 * The Serious Organised Crime and Policing Act 2005 * The Northern Ireland Troubles (Legacy and Reconciliation Act) 2023 |
| Orders in Council   * The Commissioner for Children and Young People (Northern Ireland) Order 2003 * The Police (Northern Ireland) Act 1998 (Modification) Order 2003 * Criminal Justice (Northern Ireland) Order 2004 * Criminal Justice (Northern Ireland) Order 2005 * The Policing (Miscellaneous Provisions) (Northern Ireland) Order 2007 |

Statutory Rules

* Statutory Rule 1989 No. 1341: The Police and Criminal Evidence Order (Northern Ireland) 1989
* Statutory Rule 2000 No. 314: The Police and Criminal Evidence (Application to Police Ombudsman) Order (Northern Ireland) 2000
* Statutory Rule 2000 No. 315: The Royal Ulster Constabulary (Conduct) Regulations 2000
* Statutory Rule 2000 No. 316: The Royal Ulster Constabulary (Unsatisfactory Performance) Regulations 2000
* Statutory Rule 2000 No. 317: The Royal Ulster Constabulary (Appeals) Regulations 2000
* Statutory Rule 2000 No. 318: The Royal Ulster Constabulary (Complaints etc.) Regulations 2000
* Statutory Rule 2000 No. 319: The Royal Ulster Constabulary (Complaints) (Informal Resolution) Regulations 2000
* Statutory Rule 2000 No. 320: The Royal Ulster Constabulary (Conduct) (Senior Officer) Regulations 2000
* Statutory Rule 2000 No. 399: The Police (Northern Ireland) Act 1998 (Commencement) Order (Northern Ireland) 2000
* Statutory Rule 2000 No 412: The Police (Northern Ireland) Act 2000 (Commencement) Order 2000
* Statutory Rule 2001 No.132: The Police (Northern Ireland) Act 2000 (Commencement No. 2) Order 2001
* Statutory Rule 2001 No. 184: Royal Ulster Constabulary (Complaints etc) Regulations 2001
* Statutory Rule 2001 No. 396: The Police (Northern Ireland) Act 2000 (Commencement No.3 and Transitional Provisions) Order 2001
* Statutory Rule 2001 No. 369: Police Trainee Regulations (NI) 2001
* Statutory Rule 2003 No.184: Police Service of Northern Ireland (Amendment) Regulations 2003
* Statutory Rule 2003 No. 68: Police Service of Northern Ireland (Conduct) Regulations 2003
* Statutory Rule 2003 No.142: Police (Northern Ireland) Act 1998 (Commencement No.5) Order (Northern Ireland) 2003
* Statutory Rule 2003 No. 399: Police Service of Northern Ireland (Appeals) (Amendment) Regulations 2003
* Statutory Rule 2004 No.122: The Police Service of Northern Ireland (Secondment) (Garda Síochána) Regulations 2004
* Statutory Rule No. 376: The Police (Northern Ireland) Act (Modification) Order 2003
* Statutory Rule 2004 No. 315: Police Service of Northern Ireland (Conduct etc.) (Amendment) Regulations 2004
* Statutory Rule 2004 No. 379: Police (Appointments) Regulations (Northern Ireland) 2004
* Statutory Rule 2005 No. 341: The Police Service of Northern Ireland (Complaints etc.) (Amendment) Regulations 2005
* Statutory Rule 2006 No. 69: The Police (Recruitment) (Amendment) Regulations (Northern Ireland) 2006
* Statutory Rule 2007 No.177: The Police (Northern Ireland) Act 2003 (Commencement No.2) Order 2007
* Statutory Rule 2007 No.58: Police and Criminal Evidence (Northern Ireland) Order 1989 (Code of Practice) (No.3) Order 2007
* The Police and Criminal Evidence (Amendment) (Northern Ireland) Order 2007
* Statutory Rule 2007 No.130: Police Service of Northern Ireland (Unsatisfactory Performance and Attendance) Regulations 2007
* Police Powers for Designated Staff (Complaints and Misconduct) Regulations (NI) 2008

Statutory Instruments

* The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003
* The Regulation of Investigatory Powers (Communications Data) Order 2003
* The Criminal Justice (No 2) (Northern Ireland) Order 2004
* Policing (Miscellaneous) Provisions (Northern Ireland) Order 2007
* Northern Ireland Act 1998 (Devolution of Policing and Justice) Order 2010

# APPENDIX C: Role of the Data Protection Officer

**Data Protection Officer’s (DPO) Responsibilities**

1. The controller must entrust the data protection officer with at least the following tasks:

1. Informing and advising the controller, any processor engaged by the controller, and any employee of the controller who carries out processing of personal data, of that person’s obligations under this Part,
2. Providing advice on the carrying out of a data protection impact assessment under section 64 and monitoring compliance with that section,
3. Co-operating with the Commissioner,
4. Acting as the contact point for the Commissioner on issues relating to processing, including in relation to the consultation mentioned in section 65, and consulting with the Commissioner, where appropriate, in relation to any other matter,
5. Monitoring compliance with policies of the controller in relation to the protection of personal data, and
6. Monitoring compliance by the controller with this Part.

2. In relation to the policies mentioned in subsection (1)(e), the data protection officer’s tasks include:

1. Assigning responsibilities under those policies,
2. Raising awareness of those policies,
3. Training staff involved in processing operations, and
4. Conducting audits required under those policies.

3. In performing the tasks set out in subsections (1) and (2), the data protection officer must have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

# APPENDIX D: Handling of Shared Information

## **Handling of Shared Information**

# Access to information shall be limited to those with a ‘Need to Know’. Shared information shall be handled and stored with care, and used under conditions that make accidental or opportunity compromise unlikely and which deter deliberate compromise.

## The Office must be satisfied that the organisations with which it shares data have implemented appropriate information policies derived form a risk assessment methodology in line with the ISO27000 Standards.

## Individuals that require access to shared information must have the appropriate level of security clearance to access the information.

## **Aggregation of Shared Information**

## Care must be taken to avoid the potential for the aggregation of low-level information together to create a higher level.

## There are two ways in which low-level information can aggregate to a higher level.

## **Accumulation**, where increasingly large amounts of information stored together increases the overall Impact Level of compromise of Confidentiality, Integrity and/or Availability.

## **Association,** where the association of different types of information, which in themselves have no or a low-level impact when compromised, when combined together have a higher Impact Level of compromise.

## **Security Incident Involving Shared Information**

## Any actual or potential loss of data including personal data must be reported to the Data Protection Officer who will consider the need to report this to the Department of Justice sponsoring body and to the Information Commissioner.

## Any security weaknesses that could adversely affect the information asset must also be reported using the Office’s security incident procedures.

## **Retention and Disposal of Shared Information**

## Information obtained from a third-party will be held as appropriate to its level of protective marking until such times as it is no longer required.

## When no longer required the shared information paperwork shall be disposed in accordance with the Police Ombudsman Retention and Disposal Schedule.

1. Serious complaints are defined at Schedule 1 of the agreements made pursuant to sections 60, 60ZA, 60ZB AND 60ZD of the 1998 Act. [↑](#footnote-ref-1)
2. From 1 May 2024 [↑](#footnote-ref-2)
3. Section 31 of the DPA 2018 [↑](#footnote-ref-3)
4. [ICO Law Enforcement Processing Guidance](https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/law-enforcement-processing/) [↑](#footnote-ref-4)
5. [ICO Code of Practice on Data Sharing](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/) [↑](#footnote-ref-5)