Fiosrú | Oifig an Ombudsman Póilíneachta | Office of the Police Ombudsman

Data Protection Policy

Author: DPO

Issue/Publication Date: 02/04/2025

Contents

1. Introduction

Fiosrú, Office of the Police Ombudsman is an independent statutory body whose function is to deal with matters involving possible misconduct of members of An Garda Síochána. Fiosrú is responsible for receiving and dealing with complaints made by members of the public concerning the conduct of garda members, as well as referrals made by the Garda Commissioner, the Minister for Justice or the Policing and Community Safety Authority.

Fiosrú may also investigate any matter, even where no complaint has been made, where it appears that a garda member may have committed an offence or behaved in a way that would justify disciplinary proceedings.

In performing our statutory functions under the Policing Security and Community Safety Act, 2024 (PSCS Act, 2024), Fiosrú collects, processes and stores significant amounts of personal data within the meaning of General Data Protection Regulation EU 2016/679 (GDPR), Law Enforcement Directive EU 2016/680 (LED) and the Data Protection Acts, 1988 to 2018 (Applicable Data Protection Legislation).

In accordance with the Applicable Data Protection Legislation, Fiosrú is a Data Controller and, therefore, has responsibility for ensuring the privacy of the data subjects and safeguarding the personal data processed.

Data Protection Legislation provides legal protections for individuals concerning the processing of their personal data by:

- giving rights to individuals in order to secure privacy and fairness in relation to their personal data;
- imposing obligations on those controlling and processing their personal data to have in place appropriate organisational and technical measures so that they can meet those obligations, and
- giving rights to individuals in relation to accessing, amending and or erasing their own personal data.

The process by which Fiosrú upholds these rights is dealt with in this policy and separately in our Process for Dealing with Data Subject Requests.

1.1 Law Enforcement Directive

The Law Enforcement Directive EU 2016/80 (LED) was put into effect in Irish law under Part 5 of the Data Protection Act, 2018. The LED deals with the processing of personal data by data controllers for the purposes of law enforcement. Fiosrú, when conducting criminal investigations, is processing personal data for law enforcement purposes.

1.2 Competent Authority

Fiosrú is a "competent authority" under Part 5 of the Data Protection Act, 2018.

A competent authority means:

(a) A public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security, or

(b) Any other body or entity authorised by law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security;

1.3 Scope

This document sets out the Data Protection Policy of Fiosrú. Therefore, it governs the obtaining, storage, processing and release of personal data by Fiosrú. The scope of this policy is to set out our approach in relation to:

- our legal obligations regarding confidentiality and data protection;
- how we discharge these responsibilities in practice.

1.4 Supporting Documents

Consideration should also be given to the documents below:

- Fiosrú's Cookies Policy (which is available at www.fiosru.ie/privacy is designed to inform members of the public who use our website about what happens to any personal data that they provide via Fiosrú's website;
- Fiosrú's Data Protection Privacy Statement;
- Fiosrú's Data Breach Management Plan;
- Fiosrú's Process for Dealing with Data Subject Requests. Requests from individuals should be forwarded to Fiosrú's Data Protection Unit.

2. Data Protection Definitions

In order to understand Fiosrú's obligations under the Applicable Data Protection Legislation, it is necessary to set out the meanings of some of the core terms.

2.1 Data Protection

Data protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data. The Applicable Data Protection Legislation imposes certain obligations on Data Controllers and Data Processors in respect of the personal data which it processes and also gives rights on individuals to protect their privacy.

2.2 Personal Data

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[1].

2.3 Data

Data means information in a form that can be processed. It includes automated data and manual data. Automated data refers to information held on or intended to be held on a computer. Manual data means information that is kept as part of, or intended to be kept as part of, a relevant filing system. Data forms part of such a system in circumstances where that system is structured, either by reference to the individual or by reference to criteria relating to the individual, in such a way that specific information relating to the individual is readily accessible. [2]

2.4 Data Subject

Data subject means an individual who is the subject of personal data.

2.5 Data Controller

A Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data[3]. Therefore, Fiosrú is a Data Controller under the Applicable Data Protection Legislation because we control the contents and use of personal data (either alone or with

[1] Article 4 (1) General Data Protection Regulations EU 2016/679
[2] Data Protection Acts 1988 and 2003 A Guide for Data Controllers (Data Protection Commissioner)
[3] Article 4 (7) General Data Protection Regulations EU 2016/679

others) in our possession, irrespective of where or from whom the personal data was obtained.

2.6 Data Processor

A Data Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller, however the processing activity does not include an employee of the Data Controller who processes such data in the course of their employment[4]. For example, the National Shared Services Office is a Data Processor of Fiosrú because it processes the personal data of Fiosrú staff.

2.7 Processing

Processing means performing an operation or set of operations on personal data, whether or not by automatic means, including:

- obtaining, recording or keeping the information;
- collecting, organising, storing, altering or adapting the information;
- retrieving, consulting or using the information;
- disclosing the information by transmitting, disseminating or otherwise making it available, or
- aligning, combining, blocking, erasing or destroying the information.[5]

2.8 Special Category Data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation are defined in Article 9 of the GDPR as "Special category data". Special category personal data is afforded additional protection under data protection law.

[4] Article 4 (8) General Data Protection Regulations EU 2016/679
[5] Article 4 (2) General Data Protection Regulations EU 2016/679

3. Types of Personal Data Processed by Fiosrú

In line with our functions under section 173 (2) of the PSCS Act 2024 (see Appendix A of this Policy), Fiosrú processes many types of personal data. The descriptions of the different types of data we deal with during the course of our business are set out below. These are presented in terms of the different groups of people that come into contact with us. Some of this data is categorised as special category data and is outlined in section 3.6 below.

3.1 Complainants/Witnesses

Name, address, email address, gender, date of birth, occupation, phone numbers, vehicle registrations, call recordings, images, financial information, identification documents, criminal convictions, medical information, racial or ethnic origin, data concerning health, sex life or sexual orientation (special category data).

3.2 Gardaí

All of the above at section 3.1 and garda rank, district number, registration number, epaulette number, station details, physical attributes, educational and training qualifications.

3.3 Members of the Public (e.g. legal advisers, complainants' next of kin, visitors to the Fiosrú premises)

All of the above at section 3.1 may be provided directly by a complainant (whether on the complaint form or otherwise) or may be otherwise received or collected by Fiosrú in the course of investigating complaints, referrals or through other investigative routes as provided for under the PSCS Act 2024.

3.4 Staff

The above types of data are also processed by Fiosrú in relation to our staff and former staff. In addition, Fiosrú may also process information relating to educational and training qualifications, exam results, disability status and trade union membership. This information is normally provided directly by the employees in question and is retained securely by Fiosrú's Human Resources Unit and the Learning and Development Unit solely for the purposes of personnel administration.

Processing of this information may be conducted solely by Fiosrú or in conjunction with or solely by the National Shared Services Office and other relevant Government organisations and databases (including HRMS) on Fiosrú's behalf.

3.5 Contractors and Suppliers

All of the above data at sections 3.1 and 3.4 which Fiosrú processes in the course of the corporate management of our operations e.g. security of our premises, building maintenance services, professional services etc.

3.6 Special Category Personal Data

Some personal data processed by Fiosrú comes within the definition of special category personal data in the Applicable Data Protection Legislation. For example, Fiosrú routinely processes data relating to the injuries sustained by a complainant alleging assault. This data will usually be disclosed to us by the complainant and be in the form of a report from their doctor or medical professional or where the complainant has consented for us to obtain the records directly from their GP practice or hospital.

In line with Fiosrú's obligations under the Applicable Data Protection Legislation, Fiosrú processes this special category personal data only for the performance of the statutory functions conferred under the PSCS Act, 2024 (including the administration, staffing and resourcing of the organisation).

3.7 CCTV

Fiosrú operates a CCTV system in the environs of its offices. The objectives of the CCTV, which form the lawful basis for the processing of personal data, are to:

- ensure the security of the Fiosrú premises, and
- ensure the health and safety of Fiosrú staff and visitors to the premises.

In line with guidance issued by the Data Protection Commissioner, the use of CCTV cameras is prominently sign-posted. CCTV recordings are periodically deleted every 30 days unless an alleged incident has occurred which justifies retention for a longer period. Copies of CCTV footage will be shared with An Garda Síochána where necessary to investigate actual or reported incidents.

4. Principles of Data Protection

The General Data Protection Regulations (GDPR) requires compliance with six principles, these are set out in Article 5 and require that personal data is:

Article 5 (1) GDPR:

1. **Processed in a way that is lawful, fair and transparent;**
   (Lawfulness, Fairness and Transparency Principle)
2. **Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;**
   (Purpose Limitation Principle)
3. **Adequate, relevant and is limited to what is necessary;**
   (Data Minimisation Principle)
4. **Accurate and kept up to date;**
   (Accuracy Principle)
5. **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, and**
   (Storage Limitation Principle)
6. **Processed in a manner that ensures appropriate security of the data.**
   (Integrity and Confidentiality Principle)

"**Accountability**" Article 5 (2) of the GDPR also obliges Fiosrú to *"be responsible for, and be able to demonstrate compliance with the principles"*.

Principles of Data Protection – Law Enforcement Directive

Where personal data is processed for the purposes of 'law enforcement' similar principles to the GDPR apply. These principles of data protection under the Law Enforcement Directive are set out in Section 71 of the Data Protection Act, 2018.

Application of the Data Protection Principles in Fiosrú

4.1 Lawfulness, Fairness and Transparency

Fiosrú is obliged to process data on lawful grounds. The Data Protection Legislation sets out the grounds on which personal data processing is lawful. These grounds include where processing is necessary for compliance with a legal obligation or the performance of a task carried out in the public interest.

Personal data processed by Fiosrú is carried out for the performance of Fiosrú's functions under section 173 of the PSCS Act, 2024 (Appendix A).

In addition, personal data is processed by Fiosrú for compliance with certain legal obligations to which Fiosrú is subject (e.g. Ethics in Public Office Act, 2005, Children First Act, 2015).

Fiosrú will be fully transparent regarding how we collect and use personal data, in particular ensuring that the data is not used in a way that the individual would not expect. When we collect data or at our earliest available opportunity, we will provide information regarding how we use personal data to the individual in plain and clear language. We will also provide that information on our website to ensure it is easily accessible.

4.1.1 Direct marketing and surveys

Fiosrú does not engage in any direct marketing activity but we do conduct anonymous surveys from time to time. For certain surveys, e.g. customer satisfaction or attitudes surveys, the information received and processed is anonymous and cannot be traced back or used to identify an individual in any way. Such data will not be 'Personal Data' as defined in the Data Protection Legislation.

4.2 Purpose Limitation

Fiosrú processes personal data only for the purposes for which it is collected. Usually these purposes are to fulfil our functions under the PSCS Act, 2024 including the administration, staffing and resourcing of the organisation. Where personal data is processed for the purpose of archiving in the public interest, scientific or historical research purposes or statistical purposes[6]. Fiosrú will ensure that the appropriate technical and organisational safeguards are in place and adhere to the principle of data minimisation.

The table below describes some of the relevant sections of the PSCS Act, 2024 under which Fiosrú processes personal data as part of its core function as a police oversight body:

Sections of the PSCS Act, 2024

Section	Description of Fiosrú Activity
Section 191	Confidentiality of information obtained by Fiosrú and the authorised sharing of information obtained.
Section 198	Deciding if a complaint will be admitted.
Section 208	Investigation of complaints (both criminal and non-criminal) by Fiosrú.
Section 216	Keeping people informed about the progress and results of Fiosrú investigations.

Fiosrú has other statutory obligations under legislation such as the Protected Disclosures Act 2014 (as amended), the Ethics in Public Office Act 1995 or the Standards in Public Office Act, 2001.

[6] Article 89 (1) GDPR

Fiosrú will not disclose personal data to third parties unless the data subject has consented to this disclosure or unless the disclosure to the third party is necessary for the performance of Fiosrú's functions or is otherwise authorised or mandated by law.

4.2.1 Examples

Examples of legitimate disclosures necessary to fulfil Fiosrú's functions would include the provision of personal data from Fiosrú to the Office of the Director of Public Prosecutions or the Garda Commissioner and/or staff of the Garda Commissioner.

Personal data in relation to Fiosrú staff members may be shared with other Government organisations including, but not limited to, the National Shared Services Office and the Public Appointments Services.

4.2.2 Voluntary Discovery

Fiosrú will disclose personal data to third parties if we are required to disclose it in order to comply with any applicable law, a summons, a search warrant, a court or regulatory order or other statutory requirement. Third party disclosure may arise in the context of criminal trials being conducted by or on behalf of the Director of Public Prosecutions, or on foot of a garda investigation.

4.3 Data Minimisation

Fiosrú will only process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

In order to investigate any complaint properly, Fiosrú must seek to obtain all of the facts to enable it to make an assessment regarding what information is relevant and what is not relevant. Fiosrú only retains personal data which is necessary or relevant to the performance of its duties under the PSCS Act, 2024 including the administration, staffing and resourcing of the organisation. It does not seek, nor does it wish to receive, excessive levels of data which are not relevant to these duties.

4.4 Data Accuracy

Fiosrú will ensure that the personal data we process is accurate and, where necessary, kept up to date. Each business unit within Fiosrú has a responsibility for ensuring the personal data which they process is adequately maintained, and any inaccuracies are corrected in a timely manner. Accordingly, Fiosrú will consider any data rectification requests received under the Data Protection legislation.

4.5 Storage Limitation

The storage limitation principle provides that personal data shall not be kept longer than is necessary for the purpose of processing. Fiosrú, in compliance with the National Archives Act, 1986, will determine the period of time that personal data will be retained for and the purpose of its retention. The retention periods for the different types of personal data are set out in Fiosrú's Data Retention Policy.

4.6 Integrity and Confidentiality

Fiosrú ensures that the appropriate technical, organisational and physical security is in place to safeguard the personal data which is processed and held by us at all times. Due to the sensitivity of the information available to staff, security measures and policies are in place to ensure that the confidentiality of Fiosrú files is maintained. Staff are required to adhere to Fiosrú's security policies and procedures whether working within Fiosrú's offices, blended working or remotely.

5. Data Subject Rights

Fiosrú will uphold the rights of data subjects as set out in the GDPR. Those rights are as follows:

- right to be informed/right of access to their personal data;
- right of rectification;
- right to erasure of their data;
- right to restrict processing;
- right to data portability;
- right to object to their data being processed; and
- right in relation to automated decision making and profiling.

Where personal data are processed for law enforcement purposes under the LED, data subjects have similar rights, found in sections 89-95 of the Data Protection Act, 2018, which are subject to a range of restrictions. These rights include the right to information, right of access, and rights to rectification, erasure and restriction.

5.1 Right to be informed and right of access

Subject to certain limitations at law, data subjects are entitled to find out what personal data Fiosrú holds on them and the purpose of processing their personal data. In addition, data subjects have the right to access their personal data through a Subject Access Request (Article 15, GDPR).

Fiosrú have procedures in place to ensure that all Subject Access Requests are responded to in accordance with the Applicable Data Protection Legislation.

A data subject access request may be subject to restrictions in accordance with the Data Protection Act, 2018 and the GDPR. Examples of restrictions applied by Fiosrú are:

- For the prevention, detection, investigation and prosecution of criminal offences,
- Legal proceedings and legal privilege.

Information on how to make a Subject Access Request can be found www.fiosru.ie or alternatively you can contact the Data Protection Unit at data.protection@fiosru.ie

5.2 Right of rectification

Data subjects have the right to have inaccurate personal data held by Fiosrú rectified (Article 16, GDPR). Data subjects may inform Fiosrú of any changes in their personal data, and in accordance with Fiosrú's obligations under the Applicable Data Protection Legislation we will, where appropriate, rectify, update or delete the personal data accordingly. This entitlement extends to information that is factually incorrect.

5.3 Right of erasure

Data subjects have the right to have their personal data erased (right to be forgotten) in certain circumstances (Article 17, GDPR). These circumstances include:

- the personal data are no longer necessary in relation to the purpose for which they were collected or otherwise processed;
- the only legal basis for processing the personal data is the data subjects' consent, and the data subjects' consent has been withdrawn;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased in order to comply with a legal obligation.

The right to erasure is not an absolute right and does not apply to the processing of personal data that is necessary:

- to comply with a legal obligation or the performance of a task carried out in the public interest (functions of Fiosrú);
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- for the establishment, exercise or defence of legal claims.

To make a request to have their personal data rectified, updated, amended or erased from Fiosrú databases and/or files, data subjects should write to the Data Protection Unit at Fiosrú.

Any such data rectification/erasure request may be subject to verification requirements[7].

5.4 Right to restriction of processing

A data subject shall have the right to obtain a restriction in relation to the processing of their personal data where one of the following applies:

- the data subject contests the accuracy of their personal data. The restriction will apply to enable Fiosrú to verify the accuracy of the personal data;
- the processing is unlawful and the data subject objects to their personal data being erased and requests the restriction of its use instead;

[7] The rectification/erasure of data is not an absolute right and will be determined on a case by case basis.

- Fiosrú no longer needs the personal data for the purpose of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims; or
- The data subject has objected to the processing of their personal data by Fiosrú. The restriction will apply pending the verification whether the legitimate grounds of Fiosrú override those of the data subject.

Fiosrú will restrict the processing of data to what is 'strictly necessary' in order to review the accuracy of the personal data and the legitimate grounds for processing the personal data is carried out.

5.5 Right to data portability

Fiosrú collects and processes a significant amount of personal data in order to fulfil our statutory functions under the PSCS Act, 2024. The lawful basis for the collection of personal data by Fiosrú is in accordance with Article 6.1 (c) or 6.1 (e) of the GDPR:

Article 6.1

(c) processing is necessary for compliance with a legal obligation; or

(e) processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller.

In cases where Fiosrú has collected personal data from the data subject, where the processing of personal data is carried out by automated means and where the data subject has consented to the processing or where the processing is conducted on the basis of a contract[8], Article 20 of the GDPR affords the data subject the right to data portability.

The data subject can request that Fiosrú transfer their personal data in electronic format to another Data Controller.

This right does not apply to the processing of personal data that is necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller.

5.6 Right to object

Data subjects have the right to object to certain types of processing of their personal data, where processing is carried out in connection with tasks: in the public interest, under official authority, or in the legitimate interests of others (Article 21, GDPR). Fiosrú will consider such requests on a case by case basis.

5.7 Right not to be subject to automated decision making

Article 22 of the GDPR gives data subject's the right not to be subject to decision making based on automatic processing, including profiling, which have a legal or similarly significant effect on them.

[8] Article 6.1 (a) & (b) GDPR

5.8 Right to complain

Data subjects who are concerned that their rights under the Applicable Data Protection Legislation are not upheld by Fiosrú can contact Fiosrú's Data Protection Officer (DPO). The DPO will work with the data subject to bring the complaint to a satisfactory conclusion.

The DPO can be contacted at: Data.Protection@fiosru.ie

The data subject will be informed of their right to bring their complaint to the Data Protection Commission and provided with their contact details.

6. Responsibilities of Fiosrú

Under the Applicable Data Protection Legislation Fiosrú is responsible for the following:

6.1 Ensuring appropriate technical and organisational measures

Fiosrú has implemented appropriate technical and organisational measures to ensure that the personal data we process is safeguarded and not at risk from unauthorised access. Measures in place are monitored on an ongoing basis.

Fiosrú has established appropriate security provisions to ensure that:

- access to Fiosrú's computers and information is restricted to Fiosrú authorised staff;
- Fiosrú's systems are password protected;
- Fiosrú has comprehensive back up procedures in operation;
- all waste papers, printouts, etc. are disposed of securely;
- personal data is transmitted via secure encrypted email;
- access to the server room is restricted to Fiosrú's ICT and Corporate Services authorised personnel by magnetic lock and swipe and pin cards.

6.2 Maintaining a record of data processing (ROPA)

Data protection legislation requires Fiosrú to maintain a record of processing activities (RoPA) for which it is responsible. A RoPA is a documented record of Fiosrú's personal data processing activities and details how we process personal data.

6.3 Data Protection Agreements

In order for Fiosrú to fulfil its functions under the PSCS Act, 2024, it is necessary that we share personal data with other government departments and state agencies, example: An Garda Síochána. Fiosrú will ensure that the appropriate data sharing agreements will specify, the lawful basis and purpose for sharing the personal data, the manner in which data subject rights will be upheld, the requirements for adequate security, the requirement for termination of the agreement and the steps necessary for the return/deletion of the data shared.

6.4 Data Protection by design and default

In accordance with the Applicable Data Protection Legislation, Fiosrú implements technical and organisational measures to fulfil the data protection principles as set out in section 3 of this policy, and to ensure that, by default, only personal data necessary for each purpose of processing is processed.

6.5 Data Protection Impact Assessments (DPIA)

When Fiosrú considers that a proposed processing activity, in particular processing that involves a new technology, poses a high risk to the rights and freedoms of its data subjects, it shall carry out a data protection impact assessment. As part of this process Fiosrú's DPO will be consulted and a copy of the DPIA will be retained by the DPO.

6.6 Transfers of personal data outside of the European Economic Area

Fiosrú will not normally transfer personal data of its data subjects outside the European Economic Area. However, if it does so, it will ensure that an adequate level of protection is in place and that the transfer is permitted by one of the means set out in the Applicable Data Protection Legislation.

6.7 Personal data breaches

Article 4 (12) of the GDPR defines a personal data breach as:

'*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted stored or otherwise processed*'.

Fiosrú has procedures in place for dealing with possible personal data breaches. Staff in Fiosrú will notify the DPO where they identify or suspect a breach of personal data. The DPO will assess the breach and where the breach is likely to result in a risk to the rights and freedoms of the data subject(s) involved. The DPO will notify the Data Protection Commissioner (DPC) in accordance with the Applicable Data Protection Legislation and the effected data subject(s), where this is deemed necessary.

6.8 Data Protection Officer (DPO)

Fiosrú has a designated Data Protection Officer in accordance with Article 37.1 (a) of the GDPR and section 88 of the Data Protection Act, 2018. The role of the DPO within Fiosrú includes:

- To monitor and ensure compliance with the processing activities conducted by Fiosrú on personal data;
- Provide updates to the Senior Management Team about data protection responsibilities, risks and issues;
- Informing and advising staff in Fiosrú who process personal data of their obligations under the Applicable Data Protection Legislation, through awareness raising and training;

- To monitor and ensure that all data protection policies are reviewed and updated regularly;
- Providing advice where requested on data protection impact assessments and monitoring its performance; and
- Cooperating with, and acting as a point of contact with the Data Protection Commission.

7. Data Protection Contact

Data Protection Officer

Fiosrú, Office of the Police Ombudsman
Data Protection Unit
150 Upper Abbey Street
Dublin 1
D01 FT73

Email: data.protection@fiosru.ie

8. Communication, Monitoring and Review

This policy will be subject to regular monitoring and review by the Data Protection Officer in conjunction with the Senior Management Team to reflect any organisational or legislative changes. Any changes will be reflected in Document Control section at the end of this document.

This policy will be published on Fiosrú's website and the contents of this policy will be communicated to staff through awareness and data protection training.

Appendix A - Legislation

A.1 Data Protection

Data protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data. The Applicable Data Protection Legislation imposes certain obligations on Data Controllers and Data Processors in respect of the personal data which it processes and also gives rights on individuals to protect their privacy.

In addition, the PSCS Act, 2024 and the Official Secrets Act, 1963 lay down further binding legislative obligations regarding what Fiosrú does with the information it processes.

There are different legal obligations Fiosrú must adhere to when dealing with personal data or information. These obligations are outlined in further detail below.

A.2 The Policing Security and Community Safety Act, 2024

A.2.1 Objectives of the Police Ombudsman

Section 173(1) of the Policing Security and Community Safety Act, 2024 (PSCS Act, 2024) sets out the objectives of Fiosrú, the Police Ombudsman as follows:

(a) "To promote public confidence in the processes for resolving complaints made by members of the public and in investigations under Part 6,

(b) To improve public understanding of the role and functions of the Police Ombudsman, and

(c) To ensure that his or her functions are performed in a timely, efficient and effective manner and in accordance with fair procedures".

A.2.2 Functions of the Police Ombudsman

The statutory functions of Fiosrú, the Police Ombudsman are set out in section 173 (2) of the PSCS Act 2024, which are:

(a) to receive complaints made by members of the public concerning members of garda personnel;

(b) to receive –

(i) referrals under sections 202(3), 203(1) and 205(7) and notifications under section 204(1), from the Garda Commissioner,

(ii) requests under section 205(2) and referrals under section 205(3), from the Minister;

(iii) referrals from the Authority under 205(5); and

(iv) Disclosures of relevant wrongdoing referred to in paragraph (a) or (b) of section 206(1);

(c) To carry out duties and exercise the powers conferred on the Police Ombudsman under Part 6 in relation to matters referred to in paragraphs (a) or (b);

(d) To undertake, in accordance with Part 6, investigations of other matters concerning members of garda personnel or the Garda Commissioner;

(e) To engage with An Garda Síochána to promote public understanding in respect of arrangements under section 201(1) for the handling of complaints suitable for resolution by An Garda Síochána;

(f) To report the results of investigations under Part 6 (including making such recommendations as appropriate) to the Garda Commissioner, the Minister or the Authority, as the case may be;

(g) Where section 214(1) applies, to report the results of investigations under Part 6 to the Director of Public Prosecutions and send him or her a copy of each investigation file;

(h) To prepare, in accordance with section 200(1), a draft list of categories of complaints suitable for resolution by An Garda Síochána;

(i) To make arrangements with the Garda Commissioner by protocols in writing pursuant to section 223(1) concerning the matters referred to in that section;

(j) To undertake research and analysis in order to identify trends and patterns arising from performance of his or her functions under Part 6;

(k) To ensure that the Office of the Police Ombudsman has appropriate policies, plans and actions in place to enable compliance with its obligations under section 42 of the Irish Human Rights and Equality Commission Act 2014;

(l) To make arrangements for the sharing of information by him or her with such other public bodies as he or she considers appropriate;

(m) To perform any other functions that are assigned to him or her by or under this Act or any other enactment.

A.2.3 Section 209, PSCS Act, 2024

Where a Designated Officer of Fiosrú is appointed to undertake an investigation pursuant to section 208 (1) of the PSCS Act, 2024, the Designated Officer in accordance with section 209 of the PSCS Act, 2024, is afforded all the powers, immunities, privileges and duties which exist for members of An Garda Síochána.

Fiosrú Officers have the same policing powers as the Gardaí. Accordingly, any exceptions under the Applicable Data Protection Legislation which restrict the disclosure of data obtained by An Garda Síochána will also apply to information obtained by Fiosrú under section 208 of the PSCS Act, 2024 whilst Fiosrú is conducting a criminal investigation.

A.2.4 Section 191 of the PSCS Act, 2024

Section 191 enshrines the confidentiality of information obtained by Fiosrú and we cannot disclose information, "where that disclosure is likely to have a harmful effect and the person knows or believes that the disclosure is likely to have such effect". So, if sharing or disclosing information would impede an investigation or would result in the identification of a complainant, the subject of an investigation or the subject of any matter under investigation

by the Police Ombudsman or An Garda Síochána, whose identity at the time is not public knowledge, we are prevented from doing so.

There are certain circumstances where we can disclose personal information. Section 191 (4) of the PSCS, Act 2024 allows Fiosrú to disclose information in certain limited circumstances, subject to any legal considerations which may arise. For example, we can disclose information to the Garda Commissioner, the Director of Public Prosecutions, the Comptroller and Auditor General, to members of the Houses of the Oireachtas or to a court. This part of the Act also allows for disclosures to be made if that disclosure is authorised by law. For example, under the Children First Act, 2015 we can disclose information to Tusla, the Child and Family Agency if we have reasonable grounds for concern that a child may have been, is being or is at risk of being abused or neglected[9].

A.2.5 Section 216, PSCS, Act 2024

This Policy is without prejudice to the rights of interested parties to be kept informed of the progress and results of an investigation pursuant to section 216 of the PSCS Act, 2024.

Interested parties may be provided information under section 216 through the relevant Fiosrú Officer.

A.3 The Official Secrets Act, 1963

In addition, the Official Secrets Act, 1963 imposes further obligations of non-disclosure on Fiosrú with regard to "official information". Under the Official Secrets Act, 1963 official information is defined as:

> "*any secret official code word or password, and any sketch, plan, model, article, note, document or information which is secret or confidential or is expressed to be either and which is or has been in the possession, custody or control of a holder of a public office, or to which he has or had access, by virtue of his office, and includes information recorded by film or magnetic tape or by any other recording medium*".

Any disclosure by Fiosrú which is contrary to the above requirement constitutes a criminal offence. Fiosrú may justify the disclosure of information if such disclosure is duly authorised by a Minister of Government or State authority or if it is in the interest of the State to communicate it.

A.4 The Freedom of Information Act, 2014

The Freedom of Information Act, 2014 (FOI Act) provides that every person has the following legal rights:

- the right to access official records held by Government Departments or other public bodies as defined by the FOI Act;

[9] Section 14 of Children First Act 2015

- the right to have personal information held on them corrected or updated where such information is incomplete, incorrect or misleading, and
- the right to be given reasons for decisions taken by public bodies that affect them.

Any official information held by public bodies can be sought under the FOI Act but in our case, any information concerning any of our investigations is not covered by the FOI Act. This means that administrative records, statistical information or any other information not directly concerning a Fiosrú investigation or examination may be released.

A.4.1 Access

Access to personal information relating to other people (i.e. people other than the person making the request) is generally prohibited under Data Protection Legislation but is provided for in certain circumstances under the FOI Act. For example:

- where the public interest in disclosure outweighs the individual's right to privacy;
- where the person to whom the information relates has consented to the release;
- access in certain circumstances to a parent/guardian of personal information relating to a minor or a person with a disability which renders them incapable of exercising their rights under the FOI Act;
- access in certain circumstances of personal information relating to a deceased person and,
- where disclosure would benefit the person to whom the information relates.

It is important to remember in Fiosrú's case, that the above circumstances only apply to information which is subject to the FOI Act i.e. not to information contained in case files or investigation files.

The nature of the restrictions and prohibitions reflect, in part, the difference in focus between the FOI Act and the Applicable Data Protection Legislation. The purpose of the FOI Act is to enable members of the public to obtain access to records held by FOI bodies to the greatest extent possible consistent with the public interest and the right of privacy. However, under Data Protection Legislation, protection of an individual's privacy is paramount and there is no general "public interest" test which could override this right by permitting release of an individual's information to anyone other than that individual except where consent to such release has been given.

It should be noted that while the FOI Act defines personal information as information about an identifiable individual whether living or deceased, the Data Protection Legislation only applies to data relating to living individuals.

A.4.2 Balance of Legal Obligations

There are serious criminal implications of Fiosrú breaching section 191 of the PSCS Act, 2024 or the Official Secrets Act 1963, so every individual within Fiosrú who processes personal data and is considering disclosure, must act with particular caution. Fiosrú recognises that individuals have the right to access their personal data and, in each case, we will balance the obligations placed on us under the above legislation and the rights of individuals under the Applicable Data Protection Legislation to ensure we are compliant with both, where possible.

Document Control

Document Details	
Document Authors	Data Protection Officer
Document Owner	Data Protection Officer
Document Approval	Director of Administration
Maintenance	Data Protection Unit
Distribution	This Document will be published on Orion and on the Fiosrú website.

Revision Details			
Revision No.	Revision Summary	Date	Revised by
0.1	Draft version	11/11/2024	DPO
1.0	SMT Approved	12/11/2024	Director of Administration
0.2	Draft version	14/07/2025	DPO
1.1	SMT approved	16/07/2025	