CIGIREACHT AN GHARDA SÍOCHÁNA
GARDA SÍOCHÁNA INSPECTORATE

Garda Síochána Inspectorate
Data Protection Policy

File Name:	Data Protection Policy
Version Number:	2.00
Effective From:	January 2021
Maintained By:	Head of Corporate Affairs
Date of last Review:	22 January 2024
Approval Status:	Approved
Approver:	Chief Inspector
Next Review Date:	January 2025

Contents

1. Data Protection Policy 2

2. Scope 2

3. Introduction 2

4. Controller Contact Details 3

5. Key Definitions 3

5.1 Personal Data 3

5.2 Data Controller 3

5.3 Data Processor 4

5.4 Processing 4

5.5 Filing System 4

5.6 Pseudonymisation 4

5.7 Anonymisation 4

5.8 Personal Data Breach 4

6. Application of Data Protection Principles by the Inspectorate 5

6.1 Lawfulness, Fairness and Transparency 5

6.2 Purpose Limitation 6

6.3 Data Minimisation 6

6.4 Accuracy 6

6.5 Storage Limitation and Retention 6

GSI Retention Schedule 7

6.6 Integrity and Confidentiality 7

7. Processing of Personal Data by the Inspectorate 8

7.1 Section 118 of the Garda Síochána Act 2005 9

7.2 Personal Data 9

7.3 Special Category Data 9

7.4 Data relating to Criminal Convictions and Offences 10

7.5 Website 10

7.6 CCTV 10

7.7 Third-Party Processors 11

8. Data Protection Impact Assessment/Risk Assessment 11

9. Personal Data Breaches 11

10. Data Subject Rights 12

10.1 Right to be Informed and Right of Access 12

10.2 Right to Rectification 12

10.3 Right to Erasure 12

10.4 Right to Restriction of Processing 13

10.5 Right to Data Portability 13

10.6 Right to Object to Processing 13

10.7 Right not to be subjected to Automated Decision Making 144

10.8 Complaints 144

10. Standard Operating Procedures 15

1. Data Protection Policy

The Garda Síochána Inspectorate ('the Inspectorate') is committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the Data Protection Acts 1988, 2003 and 2018.

The Inspectorate is a 'data controller' and, as such, has significant responsibilities for ensuring the privacy of individuals (data subjects) and the protection of personal data processed. This Data Protection Policy provides information about the ways in which the Inspectorate, collects, stores and uses personal data relating to data subjects in accordance with the data protection principles set out below.

2. Scope

This policy applies to all personal data collected, processed and stored by the Inspectorate in respect of all individuals, (i.e. staff, stakeholders and service providers). This includes:

- All electronic and paper records;
- CCTV images in the premises occupied by the Inspectorate; and
- Logs or registers in relation to access to the Inspectorate's premises by staff, visitors, contractors and under the contact tracing requirements in response to Covid-19.

To ensure that the Inspectorate meets its obligations under section 42 of the Irish Human Rights and Equality Commission Act 2014, this document has been screened to confirm that human rights standards are met and that the principles of legality, necessity, proportionality, accountability, equality and non-discrimination underpin the application of the document. This certifies that human rights and equality issues are fully considered in all Inspectorate policies and procedures.

3. Introduction

The Garda Síochána Inspectorate is a statutory body, independent in its operation, set up under the Garda Síochána Act 2005. Section 117 of the Act sets out the objectives and functions of the Inspectorate. It states:

"The objective of the Garda Síochána Inspectorate is to ensure that the resources available to the Garda Síochána are used so as to achieve and maintain the highest levels of efficiency and effectiveness in its operation and administration, as measured by reference to the best standards of comparable police services."

This is achieved by carrying out inspections and measuring performance by reference to the best standards of comparable police services. These inspections are either self-initiated, or requested by the Minister for Justice or the Policing Authority.

4. Controller Contact Details

The Inspectorate is the controller for the personal data it processes. In accordance with Article 37 of GDPR, the Inspectorate has appointed a Data Protection Officer. This role is performed by the Head of Corporate Affairs (PO). For enquiries, people can contact the Inspectorate in a number of ways, which are set out on the contact page of the Inspectorate's website. Data protection queries should be forwarded to dporequests@gsinsp.ie

5. Key Definitions

5.1 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.

5.2 Data Controller

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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

5.3 Data Processor

Processor mean a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

5.4 Processing

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.

5.5 Filing System

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

5.6 Pseudonymisation

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

5.7 Anonymisation

Anonymisation of data means processing it with the aim of irreversibly preventing the identification of the individual to whom it relates. Data can be considered effectively and sufficiently anonymised if it does not relate to an identified or identifiable natural person or where it has been rendered anonymous in such a manner that the data subject is not or no longer identifiable.[1]

5.8 Personal Data Breach

Personal data breach means 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.

[1] https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation

6. Application of Data Protection Principles by the Inspectorate

The Data Protection Principles as set out under Article 5 of GDPR require that personal data is:

1. Processed in a way that is lawful, fair and transparent;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and is limited to what is necessary;
4. Accurate and kept up to date;
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
6. Processed in a manner that ensures appropriate security of the data.

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

6.1 Lawfulness, Fairness and Transparency

The Inspectorate is obliged to process personal data in a lawful, fair and transparent manner. Article 6(1)(e) of GDPR states processing shall be lawful where;

> *"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"*

Section 38(1)(a) of the Data Protection Act 2018 further states that processing is lawful where it is required for:

> *'the performance of a function of a controller conferred by or under an enactment or by the Constitution.'*

Section 117 of the Garda Síochána Act 2005 sets out the objectives and functions of the Inspectorate.

> *"The objective of the Garda Síochána Inspectorate is to ensure that the resources available to the Garda Síochána are used so as to achieve and maintain the highest levels of*

efficiency and effectiveness in its operation and administration, as measured by reference to the best standards of comparable police services."

6.2 Purpose Limitation

The Inspectorate will not process personal data in a way that is incompatible with the purposes for which it has been collected. Personal data regarding the Inspectorate's staff will be used in the administration, staffing and resourcing of the organisation and may be shared with other Government organisations including, but not limited to, the National Shared Services Office, the Public Appointments Service, and the Office of the Revenue Commissioners etc.

6.3 Data Minimisation

The Inspectorate 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. The Inspectorate processes a minimal amount of personal data in the course of performing its functions, the majority of information processed by the Inspectorate is at an organisational level rather than personal data relating to an identified individual. Staff members must adhere to the Inspectorate's GDPR Standard Operating Procedures when collecting information.

6.4 Accuracy

The Inspectorate will ensure that the personal data it processes is accurate and, where necessary, kept up to date. Data subjects have the right to have inaccurate data held by the Inspectorate updated or erased, as appropriate.

6.5 Storage Limitation and Retention

The Inspectorate will ensure that personal data is not retained for longer than it is required and will be properly destroyed/deleted when it is no longer needed. In this regard, it is important to note that the Inspectorate has limited control in relation to record destruction due to obligations which arise under the National Archives Act, 1986 and the Freedom of Information Act, 2014. Employee records are subject to the Department of Justice's HR Retention Policy

On rare occasions personal data that is not appropriate to the Inspectorate's business requirements may be received from a member of the public. The staff member responsible for monitoring external correspondence should review all correspondence received for the existence of any personal data and should bring it to the attention of their line manager or the Data Protection Officer, following which an appropriate response should be sent to the sender. For

example, where the material was intended for another recipient the sender should be advised accordingly and the email or letter deleted from the system and any paper copies of the letter or email should be shredded.

GSI Retention Schedule	
Inspection related material containing personal data	Review material for secure disposal or transfer for archive purposes 12 months after report publication.
Document Libraries	Retain records for compliance with the National Archives Act 1986.
Files	Retain records for compliance with the National Archives Act 1986.
Written Correspondence	Retain records for compliance with the National Archives Act 1986. Return letters which contain personal information to the sender unless it is directly related to the work of the Inspectorate.

6.6 Integrity and Confidentiality

The Inspectorate will maintain the highest standards of technical and physical security to ensure that it protects personal data while we hold and process it. This responsibility is discharged in structural terms by the IM&T Unit of the Department of Justice on the Inspectorate's behalf but primarily by the actions of staff members. This will be done by ensuring:

- Access to information is given to staff at the appropriate authorised level;
- All computer systems are password protected; passwords must never be disclosed to any individual including other employees in the Inspectorate or the Department;
- All portable devices used to transport data are password protected and encrypted;
- All premises will be kept secure, in particular when they are unoccupied;
- Awareness sessions are arranged for staff to ensure that they are aware of their responsibilities under GDPR;

- Individual staff members have a key role in keeping data safe and secure through this policy in conjunction with the Department of Justice's Acceptable Usage of ICT Resources Policy.
- In the event of theft of a mobile device, the ICT section of the Department should be immediately contacted by the user and asked to remotely wipe the device urgently.
- Where staff are working remotely with paper records, to take steps to ensure the security and confidentiality of these records such as by keeping them locked in a filing cabinet or drawer when not in use, disposing of them securely (e.g. shredding) when no longer needed, and making sure they are not left somewhere where they could be misplaced or stolen.
- Where possible, staff should keep a written record of which records and files have been taken home, in order to maintain good data access and governance practices.
- Make sure that any device has the necessary updates, such as operating system updates (like iOS or android) and software/antivirus updates.
- The DPC have more guidance on working remotely here

Further to the 'integrity and confidentiality' requirements of GDPR, staff of the Inspectorate are also subject to the non-disclosure requirements of the Official Secrets Act 1963 and Section 118(3) of the Garda Síochána Act 2005.

7. Processing of Personal Data by the Inspectorate

Some examples of the purposes for which the Inspectorate may collect personal data are:

- Information requested for the purpose of an inspection.
- Stakeholder engagement – including personal data of stakeholders that engage with the Inspectorate during the course of performing its functions.
- Queries – including personal data received from individuals who have raised queries with the Inspectorate.
- Job applications – including personal data received from persons applying for roles within the Inspectorate; and
- The Inspectorate may also process personal information in relation to its staff and former staff, such as information relating to educational and training qualifications, disability status and trade union membership. This information is normally provided by the employees in question and processed for the purposes of personnel administration. Processing of this

information may be processed solely by the Inspectorate or in conjunction with the National Shared Services Office (NSSO) or the Department of Justice's HR Unit.

7.1 Section 118 of the Garda Síochána Act 2005

In accordance with Section 118 of the Garda Síochána Act 2005, the Inspectorate have agreed and implemented written protocols for requesting and receiving information in the possession of the Garda Síochána. Section 118(1) states:

> *"As soon as practicable after the commencement of this section the Inspectorate and the Garda Commissioner shall by written protocols, make arrangements to ensure that the Inspectorate receives any information requested by it which is in the possession of the Garda Síochána and which, in the opinion of the Inspectorate, is necessary for the performance of its functions."*

7.2 Personal Data

Depending on the subject matter of the inspections undertaken, it may be necessary for the Inspectorate to process personal data for a number of different purposes which arise from its statutory functions under Section 117 of the Garda Síochána Act 2005. **In the majority of cases, information is gathered at an organisational level for statistical purposes rather than an individual level.** In such circumstances, safeguards are in place to protect the fundamental rights and freedoms of data subjects, such measures include the statistical analysis of aggregated anonymised datasets rather than datasets containing personal data.

The Inspectorate may also process personal data where data subjects contact or request information from the Inspectorate directly, and personal data received by the Inspectorate indirectly.

7.3 Special Category Data

The Inspectorate may occasionally process special category data. Special category data may include personal data relating to racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning health; and data concerning a natural person's sex life or sexual orientation.

This includes special category data received by the Inspectorate where data subjects contact or request information from the Inspectorate directly, and special category data received by the Inspectorate indirectly.

Depending on the subject matter of the inspections undertaken, it may be necessary for the Inspectorate to process special category data during the course of performing of its functions. Where individual information is gathered, this will most often be as a result of stakeholder engagement through interviews. At the time the data is collected, it will be made clear that the information gathered will be anonymised in the Inspectorate's inspection reports in order to preserve the fundamental rights of data subjects.

7.4 Data relating to Criminal Convictions and Offences

In the course of performing its functions, the Inspectorate may occasionally process data relating to criminal convictions and offences. This includes personal data relating to criminal convictions and offences where data subjects contact or request information from the Inspectorate directly, and personal data relating to criminal convictions and offences received by the Inspectorate indirectly.

Where individual information is gathered, this will most often be as a result of stakeholder engagement through interviews. At the time the data is collected it will be made clear that the information gathered will be anonymised in the Inspectorate's inspection reports in order to preserve the fundamental rights of data subjects.

7.5 Website

The Inspectorate's website (www.gsinsp.ie) uses certain cookies. The Website & Cookie Policy can be accessed here.

7.6 CCTV

The Inspectorate operates CCTV at its office located at 87 St Stephen's Green, Dublin 2, DO2 K230. Cameras are placed so as to record external areas and are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property. The Inspectorate's CCTV Policy can be accessed here.

7.7 Third-Party Processors

In the context of the Inspectorate, this means information that is being processed on behalf of the Inspectorate by the Department of Justice, the National Shared Service Office (including Peoplepoint and PSSC), and Financial Shared Services (FSS).

Should a business need be identified to engage additional service providers, it will be subject to a privacy impact assessment. The Inspectorate must ensure the provisions relating to the engagement of third party processors as set out in Article 28 of GDPR are complied with.

8. Data Protection Impact Assessment/Risk Assessment

In accordance with recognised good practice, the Inspectorate will consider conducting a Data Protection Impact Assessment (DPIA) for any major new project involving the use of personal data e.g. an inspection. If a DPIA is not deemed necessary, the Inspectorate shall record the rationale for this decision in a document outlining data protection considerations including putting appropriate safeguards in place to mitigate any risks identified for that specific inspection.

9. Personal Data Breaches

GDPR defines a personal data breach as meaning *'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*'.

Staff of the Inspectorate will notify the Inspectorate's Data Protection Officer (DPO) where they identify or suspect a breach of personal data. In accordance with GDPR, the DPO will notify the Data Protection Commission without undue delay where a breach is likely to result in a risk to the rights and freedoms of the data subject(s) involved.

The DPO will also assess if the breach is likely to result in a high risk to the data subject(s) involved. Where a high risk is identified, the DPO will arrange for the data subjects to be notified.

10. Data Subject Rights

Subject to Section 60 of the Data Protection Act 2018 and any associated Regulations, Article's 12 to 22 of GDPR specifies the following rights for data subjects:

- right to be informed
- right of access
- right to rectification
- right to erasure
- right to restrict processing
- right to data portability
- right to object to processing
- rights in relation to automated decision making and profiling

10.1 Right to be Informed and Right of Access

Data subjects have the right to be informed by the Inspectorate about the collection and use of their personal data. In addition, they have the right to access their personal data as appropriate. Where the Inspectorate receives a Subject Access Requests (SARs) it will be responded to within the one month period as required under Article 12 of GDPR.

10.2 Right to Rectification

Data subjects have the right to have inaccurate personal data held by the Inspectorate rectified and to have incomplete personal data updated so that it is complete. On receipt of a request from a data subject for rectification of their personal data, the Inspectorate will take reasonable steps to ensure that the data held is accurate and will ensure that data is rectified, where necessary.

10.3 Right to Erasure

Article 17 of the GDPR provides for the right of data subjects in certain circumstances to have their personal data erased ('right to be forgotten'). The right to erasure is not an absolute right and does not apply in circumstances where the Inspectorate's processing of personal data is necessary in particular:

- for the performance of a function of the Minister or a task carried out in the public interest;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- where the data is required for the establishment, exercise or defence of legal claims.

Where a data subject is of the opinion that elements of personal data held by the Inspectorate are incorrect, they may make a request in writing to have such data permanently erased. The Inspectorate will review all such requests and, where appropriate, will erase the data in question.

10.4 Right to Restriction of Processing

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

- the data subject contests the accuracy of their data. The restriction will apply for a period enabling the Inspectorate to verify the accuracy of the personal data;
- the processing is unlawful and the data subject does not wish to have the data erased, but rather wishes to restrict its' use;
- the Inspectorate no longer requires the data in question but the data subject seeks its' retention in order to establish, exercise or defend a legal claim; or
- the data subject has objected to the processing of their data by the Inspectorate. The restriction will apply pending verification on whether the Inspectorate's legitimate grounds for processing overrides the data subjects concerns.

As a matter of good practice, the Inspectorate will restrict the processing of personal data whilst a review of the accuracy of the data and/or the legitimate grounds for processing the data is carried out. This restriction of processing will take into account any Regulations made under Section 60 of the Data Protection Act 2018.

10.5 Right to Data Portability

In cases where the Inspectorate has collected personal data from a data subject by consent or by contract, that data subject can request the Inspectorate to provide the data in electronic format in order to provide it to another Data Controller. The Inspectorate will comply with all such legitimate requests.

10.6 Right to Object to Processing

Under Article 21 of the GDPR, data subjects have a right to object to the processing of their personal data in specific circumstances. Where such an objection is received, the Inspectorate will assess each case on its' individual merits.

10.7 Right not to be subjected to Automated Decision Making

Data subjects have the right not to be subjected to a decision based solely on automatic processing, including profiling, that have a legal or similarly significant effect on them. At present the Inspectorate does not conduct automated processing of personal data.

10.8 Complaints

Data subjects who may be concerned that their rights under the GDPR are not upheld by the Inspectorate can contact the Inspectorate's Data Protection Officer (DPO). The DPO will engage with the data subject in order to bring their complaint to a satisfactory conclusion. Where the complaint to the DPO cannot be resolved, the data subject will be informed in writing and will be further informed of their right to bring their complaint to the Data Protection Commission.

10. Standard Operating Procedures

The following are a list of standard operating procedures and relate to the specific work of the Inspectorate.

1. Data protection is a key consideration in the planning of data collection requests to the Garda Síochána for all inspections. To ensure compliance with GDPR requested personal data must be for specific, legitimate purposes.
2. Include a statement at the start of interviews that the Inspectorate will not record names of interviewees or attribute information to any source.
3. Do not ask for personal details (i.e. names, addresses, email addresses, phone numbers) when requesting individuals to fill out questionnaires.
4. When assessing and examining garda case files/PULSE reports off-site, do not copy personal details into notes.
5. When storing PULSE material or other garda issued material with personal data ensure that it is appropriately secured. Ensure paper records are kept in a locked cabinet at all times when not being used by staff members.
6. Exercise care when transporting any material with personal data which has been handed over or verbally relayed and written down. Always ensure that it is appropriately secure – i.e. in a locked briefcase.
7. No staff member should bring any work-related documentation with personal information outside of the office unless it is absolutely necessary for business reasons.
8. Exercise care when sending emails to ensure incorrect email addresses are not auto filled.
9. Use the four eyes principle when sending out personal data. Any letter or email which may contain sensitive personal data should be checked by one other person before it is sent.
10. Only use Inspectorate issued encrypted USBs/memory sticks for storing work related material.
11. Delete/shred information which is personal and which is being held beyond identified retention periods provided that it is not necessary for consideration under National Archives legislation.
12. Do not recycle paper (i.e. use the blank side of paper which has been printed on one side) which contains personal data. All recycled paper should be shredded and never used on files.
13. Do not save material containing personal information outside of encrypted platforms onto work issued phones or laptops.