



ShannonDoc

Data Protection Policy

General Data Protection Regulations

2018

Data Protection Acts

1988-2018

Procedure Name	Data Protection Policy		Procedure No.			GDP DPP 001 V 2.0
			Version	No.		
Issue No	Reviewed by	Approved by	Issue Date	Details of Change	Next Review Date	Responsible Person
1.1		Management	01/07/2022	Updated format	01/07/2024	Deirdre Walsh
2.0	ShannonDoc	Management	01/12//2018	Initial release of document		

INTRODUCTION

This Data Protection Policy is a Statement of ShannonDoc's commitment to protect the personal data and data rights of its service users and to enable them to exercise their rights in accordance with the General Data Protection Regulations 2018 (GDPR)

ShannonDoc, as an organisation provides an Out of Hours Family Doctor Service. In order to provide service users with the most effective and targeted range of services and supports and to meet the needs of its users, we are required to collect, process, store, retain and use personal data in both electronic and manual format for a variety of purposes. This data relates to Staff, Service Users, Doctors and other individuals and entities who interact with ShannonDoc Article 6 (1) Lawful Processing.

The General Data Protection Regulations GDPR 2018 and the Data Protection Acts, 1988, 2003 and 2018 known as the (Data Protection Laws) confer rights upon individuals and entities regarding their Personal Data and the responsibilities on those persons processing and storing Personal Data.

This Data Protection Policy outlines the obligations of ShannonDoc under the Data Protection Law and it details the steps to be taken to ensure compliance with those obligations.

This Policy applies to all ShannonDoc Employees, Member Doctors and to any other person who interacts with and uses the Service.

It is the responsibility of all Shannondoc Staff and users of the service to comply with and to familiarise themselves with the contents of this Policy. It is the responsibility of the ShannonDoc Management team to ensure that staff adhere and are compliant with all Data Protection regulations.

1. PURPOSE

This policy outlines measures in place to protect the rights and personal data of individuals and to enable them to exercise their rights in accordance with the General Data Protection Regulations (GDPR) 2018 and under the terms of this policy.

2. SCOPE

This Data Protection Policy extends to the entire organisation known as ShannonDoc.

3. REFERENCE DOCUMENTS

General Data Protection Regulations, 2018.
Data Protection Acts, 2018.

Privacy Statement	GDP SS	002
Record Retention Policy	GDP RRP	003
Data Breach Policy	GDP DBP	004
Closed Circuit TV Policy	GDP CCTP	005
Staff Privacy Notice	GDP SPN	006

4. DEFINITIONS

Controller or Data Controller

Any person or entity who either alone or with others control the purposes and means of processing personal data is regarded as a Data Controller. It should be noted that a Data Controller can be a number of legal entities such as Government Departments, companies or individuals. There can be Joint Controllers of Data, Article (7) GDPR Regulations 2018.

The data controller **determines the purposes for which and the way personal data is processed**. It can do this either on its own or jointly or in common with other organisations. This means that the data controller exercises overall control over the 'why' and the 'how' of a data processing activity.

Data Processor

A Data Processor refers to a person, company or other body which processes personal data on behalf of the data controller (excluding the data controller's own employees)

Personal Data

Personal Data is defined in Article 4, Section 1 of the GDPR Regulations as any information relating to an identified or identifiable natural person (the data subject) who can be identified, directly or indirectly in particular by reference to an identifier such as a name, identification number, location data, date of birth, an online identifier (such as an IP address) or to one or more factors specific to the physical, generic economic or social identify of that natural person.

Data Subject

A living individual who is the subject matter of the personal data. It should be noted that GDPR Regulations do not apply to deceased persons and to their data.

Data Processing

**Printed copies of this document are considered uncontrolled, unless otherwise specified.
Verify the revision before use.**

The term “processing” refers to any operation or set of operations performed on personal data. Processing includes collecting, storing, retrieving, using, combining, erasing, and destroying personal data, and can involve automated or manual operations.

Special Category Data

Special Category Data is defined in Article 9 of the General Data Protection Regulations (GDPR) 2018. Special Category Data is defined as personal data revealing:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data and biometric data processed for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Data concerning the person’s sex life or sexual orientation.

It is prohibited under the regulations to process this data belonging to an individual, however there are exemptions outlined in the regulations under Article 6, Section 1, Subsections (a) through (e), and under Article 9, Subsections (2) through (4).

5. PRINCIPLES OF DATA PROTECTION

All Personal Data shall be processed in accordance with the following principles, also known as the Quality Principles of Data Protection, according to Article 5 of GDPR Regulations 2018 as follows:

1. Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
2. Personal Data must be collected for a specified, explicit and legitimate purpose and not to be processed in a manner in ways incompatible with those purposes.
3. Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. Data should be kept accurate and up to date.
5. Data should not be kept longer than necessary.
6. Data must be kept safe and secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
7. The Data Controller must take into consideration people’s rights.

In general, the Data Controller is the entity that determines why and how personal data is processed. The controller must be responsible for, and demonstrate compliance with the Data Protection Principles, and is accountable for enforcing them.

6. RESPONSIBILITIES

The Data Protection Officer (DPO) has the responsibility to enforce this policy and ensure it is being complied with.

7. DATA PROTECTION OFFICER

Under Article 37, Section 1 of the GDPR Regulations, the Controller and the Processor shall designate the appointment of a Data Protection Officer.

The duties of the Data Protection Officer (DPO) are as follows:

- Provide training for staff in relation to GDPR.
- Support the organisation in respect to its compliance of GDPR regulations.
- Liaise with the Supervisory Authority.
- Review and enact GDPR compliance measure and policies.
- Act as an intermediary between the relevant stakeholders.
- Provide advice and support to staff members in relation to GDPR practice and compliance.

8. ADHERENCE TO GUIDELINES ISSUED BY THE OFFICE OF THE DATA PROTECTION COMMISSIONER

ShannonDoc must adhere to all guidelines issued by the Office of the Data Protection Commissioner and the Supervisory Authority. These include guidance on matters such as CCTV management and rulings in respect of complaints made to these bodies.

9. LAWFULNESS OF PROCESSING DATA (Article 6)

Data processing shall be lawful only if and to the extent that **one** of the following apply:

- a. The Data Subject has given consent to the processing of his or her personal data for one or more specific purposes.
- b. Processing is necessary for the performance of a contract to which the Data Subject is party to or in order to take steps at the request of the Data Subject prior to entering the contract.
- c. Processing is necessary for compliance with a legal obligation to which the Controller is subject.
- d. Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of Official Authority or power vested in the Controller.
- f. Processing is necessary for the purposes or the legitimate interests pursued by the Controller or by a third party. Exceptions as to what such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection or personal data, where the Data Subject is a child.

Printed copies of this document are considered uncontrolled, unless otherwise specified.

Verify the revision before use.

10. INFORMING PATIENTS OF THEIR PRIVACY RIGHTS

The organisation has put in place a Privacy Statement which advises patients of their privacy rights when providing personal data.

11. PRIVACY BY DEFAULT OR DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

If ShannonDoc engages in a new data processing activity or if the processing activity is likely to increase the risk of a data breach, then a Data Protection Impact Assessment will be carried out by ShannonDoc as the Data Controller.

A DPIA is the process which systematically considers the potential impact of a project or initiative on the privacy of individuals.

ShannonDoc also adopts privacy by design as a default approach.

12. GENERAL DATA PROTECTION REGULATION (GDPR) TRAINING FOR STAFF

1. Advice and training are provided on an ongoing basis.
2. Data Protection Breach training and guidelines is being provided for relevant personnel

Articles, advice, and points of interest are continuously placed on the 'Intranet' for staff to access. Significant amount of material, articles, audit templates, and advice has and continues to be placed on the RMS which is accessible by doctors.

Advice and training on how to comply with GDPR whilst working from home is being provided.

13. RECORDS MANAGEMENT PROCEDURE

The organisation has a Records Retention Policy (GDP 003) in relation to the storing and destruction of information and data.

Data is securely held and readily accessible and retrievable in the event of a Data Access Request under Article 15 of the GDPR Regulations and/or a Freedom of Information (FOI) request under the Freedom of Information Act 2014.

Data can be held in the following formats:

- Paper Records
- Employee Personal Data / manual / electronically
- Text messages
- Electronic files
- Emails
- Financial records

**Printed copies of this document are considered uncontrolled, unless otherwise specified.
Verify the revision before use.**

- Company records / legal requirements
- Board Papers / Minutes
- Regulators Reports
- Patient Data / outcomes / intakes
- Biometric Employee Data
- Ethnical information
- Operational Data / Policies
- Website / Intranet / RMS
- CCTV / CD's
- Micrographic Materials

The Records and Retention Policy enables the regular systematic destruction of records and requires a log of any such destruction to be kept.

14. CLOSED CIRCUIT TV FOOTAGE

ShannonDoc and its Treatment Centres are secure facilities for a variety of reasons and CCTV monitoring is necessary to protect the integrity of the service. It is necessary that data which is held is maintained and safely stored for the benefit of our service users. Care is taken to ensure that images are neither deleted nor modified without the permission or knowledge of the Data Controller.

All CCTV footage is automatically deleted after 30 days with the exception of a Garda request for CCTV footage. It should be noted that if a member of An Garda Síochána request data for the purposes of preventing a crime the information is GDPR exempt under Article 2, Section (d).

GDPR states 'Any person whose image is recorded on a CCTV system has a right to seek and be supplied with a copy of their own personal data from the footage'.

15. THIRD PARTY PROCESSORS AND DATA PROCESSING AGREEMENTS

A Data Processor is a third party (person, company or other body) which processes personal data on behalf of ShannonDoc.

Prior to engaging with Data Processors, ShannonDoc must ensure the following:

1. It is appropriate to engage the Data Processor
2. The Data Processor puts in place an agreement in writing (a Data Processing Agreement) that complies with the requirements under Data Protection Law.

If there are any changes to the way data is being processed or kept, the Data Controller must be advised immediately by the Data Processor.

If the Data Processor subcontracts any of the data processing then the Data Controller must be advised immediately.

If any data is processed or transferred outside of the EU, additional safeguards and procedures must be enacted.

**Printed copies of this document are considered uncontrolled, unless otherwise specified.
Verify the revision before use.**

16. TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

Data Protection Law stipulates that ShannonDoc, may not, except for limited exceptions, transfer personal data outside of the EEA to any third country unless said country is deemed by the European Commission to provide an adequate level of protection in relation to the processing of personal data. Such transfers are provided for in Articles 45 through 50 of the GDPR Regulations 2018.

Model Contract Rules have been developed in order to monitor and to provide for such transfers. The following are the most relevant exceptions:

- The Data Subject has explicitly consented to the transfer of data having been informed of the possible risks of such transfers for the data subject due to the absence of an adequate decision-making process together with appropriate safeguards.
- A Transfer Agreement incorporating the Model Clauses in the form.
- The transfer is made pursuant to a Code of Conduct or a Certification mechanism that has been approved by under applicable Data Protection Law together with binding and enforceable commitments of the Controller or if the Processor in the Third Party Country is applying, the appropriate safeguards as regards Data subject's rights.
- The Data Importer is subject to a framework approved by the European Commission to facilitate transfer e.g., EU and US Data Privacy shields which deals with Data Transfers to and from the United States.

17. DOCUMENTING AND MONITORING COMPLIANCE

Compliance is ongoing and is continuously monitored.

ShannonDoc holds an inventory and details on the data it holds:

- Categories of personal data held and processed
- The purposes of processing
- Categories of Data Subjects
- To whom the personal data relates
- Details of recipients of the personal data
- To whom personal data has been disclosed
- Data Access Request details
- Details of transfers
- Where possible, retention periods
- Contact details of the Controller

**Printed copies of this document are considered uncontrolled, unless otherwise specified.
Verify the revision before use.**

18. DATA SECURITY

ShannonDoc implements appropriate technical and organisational measures to ensure a level of security appropriate to the risks to personal data that may arise in connection with the processing activities ShannonDoc undertakes.

19. MANAGING DATA PROTECTION DATA BREACHES

ShannonDoc has a Data Breach Policy in place to detect, report, and investigate a personal data breach in accordance with GDPR 2018 Regulations and subject to the guidelines issued by the Office of the Data Protection Commission (DPC), the Supervisory Authority.

A breach may occur due to the release of personal or sensitive data under Article 9 without authority or consent. A breach may also occur due to inappropriate access to such data or sending data to unauthorised individuals.

If a breach occurs and there is harm to the data subjects, then said personal data breaches must be notified to the Supervisory Authority. This is mandatory and notification must be made **no later than 72 hours** after becoming aware of the breach.

Where there is a breach that is resolved within the 72 hour period with no harm to the data subjects, it does not have to be reported to the Supervisory Authority but must be recorded in the breach log.

If data is anonymised or encrypted as prescribed in the GDPR Regulations, the loss of material is not a breach, but should be recorded.

In the event of a data breach, measures are put in place to prevent reoccurrence. The findings resulting from the investigation and resulting recommendations will be sent to the Supervisory Authority.

All employees receive GDPR compliance training and advice with extensive material made available. Staff and Doctors must report all data breaches to the Data Protection Officer.

20. DATA ACCESS REQUESTS

A Data Subject has a right to access their data under Article 15 of the GDPR Regulations 2018, under Data Protection Acts 2018 and the Freedom of Information Act 2014.

All Data Access Requests must meet certain requirements specified in the aforementioned acts:

All Data Access Requests should be submitted to ShannonDoc in the following manner:

- Data Access Request must be made in writing. a verbal request is accepted but the subject is advised that the request should follow in writing (if confirmation is required)
- Data Access Request must contain proof of identity and proof of current address to ensure personal data is only released to the Data Subject.
- Data Access Requests should be dealt with as soon as possible. Ensure that all information is correct and any necessary supporting documentation is present.

If a Data Access Request is made for the personal data of a **public (GMS patient)**:

Supply **Form A**, which is found in GDP DPP 001 FR 01.

If a Data Access Request is made for the personal data of a **private patient**:

Supply **Form B**, which is found in GDP DPP 001 FR 02.

If a Data Access Request is made for the personal data of a **current, former, or retired employee**:

Supply **Form C**, which is found in GDP DPP 001 FR 03. Submit the completed form to the HR Manager of ShannonDoc and include with it the employee number and appropriate supporting documentation.

Important note in relation to Form A

Form A applies to GMS patients. ShannonDoc as an organisation comes under the remit of Section 6 and 10 of the Freedom of Information Act 2014. This gives it the status of a **service provider** to the HSE.

Therefore, **all** Freedom of Information requests made for a GMS patient must be made first to ShannonDoc who will then forward the request and the relevant patient outcomes to the HSE for processing.

21. RIGHT TO REFUSE DATA ACCESS REQUESTS

As per Section 37, Subsection 3 of the Freedom of Information Act 2014, ShannonDoc may deny a Data Access Request on the grounds that if released there would be good reason to believe it would be detrimental to their *“physical or mental health, well-being or emotional condition”*.

22. POINTS OF CONTACT

Data Subjects can contact ShannonDoc at its Headquarters in Limerick

If one wishes to make an access request or exercise one's rights as outlined under Data Protection Law or if one has any queries, they should contact the Data Protection Officer, Deirdre Walsh

Email: deirdrewalsh@shannondoc.ie

Phone: 061 459527

Postal Address Deirdre Walsh
Data Protection Officer
ShannonDoc H.Q.
St Camillus Hospital
Shelbourne Road
Limerick V94 5V24

Further information is available on the ShannonDoc website: www.shannondoc.ie

23. FURTHER INFORMATION

If one requires further information on Data Protection, they should contact the Offices of the Data Commissioner (The Supervisory Authority)

Lo Call Number 1890 252 231

Email dpo@dataprotection.ie

Postal Address Data Protection Commissioner,
Canal House,
Station Road,
Port Arlington,
Co Laois R32 NP 23