Data Protection Policy

General Data Protection Regulations

GDPR 2016 / 679 – 2018

Data Protection Acts 1988, 2003 & 2018

Issue No.	Reviewed By	Approved By	Approval Date	Details of Change	Originator
Issue 01	Management	SouthDoc	1/11/2018	All amendments completed and updated.	Matt Breslin

Author:	SouthDoc Data Protection Officer
	General Data Protection Regulations GDPR 2016 / 679 - 2018 Data Protection Act - 2018
Creation Date:	01.11.2018
Review Date:	01.11.2020
Related Policies:	Data Breach Policy Data Access Request Policy Document Retention Policy Privacy Impact Statement Data Protection Impact Statement Data Breach Management Policy Staff Privacy Notice

Table of Contents

1 INTRODUCTION

This Data Protection Policy is a Statement of SouthDoc's commitment to protect the rights and Personal Data of Individuals / Service Users and to enable them to exercise their rights in accordance with the General Data Protection Regulations 2018 GDPR and the terms of this Policy supports their rights.

SouthDoc as an Organisational Entity provides an Out of Hours Family Doctor Service. In order to provide individuals with the most effective and targeted range of services / supports and to meet the needs of Citizens we are required to:

- Collect, process, store / retain and use Data in both Electronic and Manual format for a variety of purposes, about its Staff, Service Users, Doctors and other individuals and entities who come into contact with SouthDoc 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 as well as responsibilities on those persons processing and storing Personal Data.

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

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

- It is the responsibility of all SouthDoc Staff and users of the service to comply with and to familiarise themselves with the contents of this Policy.

2 PURPOSE

This Data Protection Policy is a Statement of SouthDoc's commitment 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.

3 SCOPE

This Data Protection Policy extends to the entire Organisation / Corporate Entity known as SouthDoc which comprises of a number of Corporate Entities with the parent Company known as South West Doctors on Call Company Limited by Guarantee and under this Company SouthDoc Services Limited and South West Community Intervention Teams Limited (CIT)

SouthDoc Services Limited deals with the engagement of Locum Doctors and the Management of GP financial contributions.

4 DEFINITIONS

Controller or Data Controller:

Any person / entity who either alone or with others controls the purposes and means of processing of 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, see Article (7) GDPR Regulations 2018

Personal Data:

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

Data Subject: Is a living individual 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:

Data Processing has a wide definition and scope, it includes the following processes. It means performing an operation or series of operations. It covers collection, recording, storage, adaptation, or alteration of Data retrieved. Consultation, use disclosure by transmission, dissemination or otherwise making available alignment or combination restriction, erasure or destruction of Data as described under Article 4 (2) which applies to both electronic and manual Data.

Special Categories of Personal Data Article 9 (1) GDPR Regulations:

Article 9 (1) Relates to the processing of Personal Data, notably Special Category Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or Trade Union Membership. The processing of generic Data, biometric Data for the purpose of uniquely identifying a natural person. Data concerning health, a natural person's sex life or sexual orientation shall be prohibited. There are a number of exceptions to processing which are contained / outlined in Paragraph 1. They are also contained in Paragraphs 2 of 3 Article 9 and in Article 6 (1) sub sections (a) to (e)

5 PRINCIPLES OF DATA PROTECTION/DATA QUALITY PRINCIPLES

Principles of Data Protection Laws - Article 5

Article 5 contains seven principles relating to the Processing of Personal Data. They are also known as the Quality Principles of Data Protection

It should be noted that all Personal Data / Special Category Data processed and retained by SouthDoc in the course of its work is necessary and for the service it provides. This is and will be dealt with and processed in compliance with the principles relating to processing Personal Data as prescribed in Article 5 of the General Data Protection Regulations GDPR 2018

All Personal Data shall be processed in accordance with the following principles:

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 purposes 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.

This Policy sets out and prescribes how SouthDoc will handle, process and store Data, to include how Data Access Requests are dealt with from a Data Subject together with how to manage and deal with Data Breaches.

Data in this Policy means and applies to Personal and Sensitive Data under Article 9 (1).

SouthDoc as a Service Provider / Corporate Entity is committed to protecting Personal Data / Special Category Data as enshrined in the second title (Freedoms) of the Charter of Fundamental rights of the European Union which has full legal effect and applicability from the 11.12.2018

This Data Protection Policy should be read in conjunction with the Data Protection Act 2018 and Regulation EU No 2016 / 679 of the General Data Protection Regulations GDPR 2018.

SouthDoc has controls in place and there is a Policy in respect of the use of and storage of CCTV systems and the organisation has a CCTV Policy which is reviewed regularly and in compliance with Legal and Regulatory Requirements.

What is Data Protection?

Data Protection is about ensuring that a Person's Personal Records and Data is lawfully collected with their consent, processed safety and retained as long as necessary to achieve the purpose for which it has been collected. SouthDoc as a Data Controller carries out all duties and functions as set out in the Data Protection Acts and under the GDGR Regulations 2018. SouthDoc ensures that the gathering and holding of all Data is done solely within the terms of the Acts and the Regulations.

Appointment of a Data Protection Officer:

Under Article 37 (1) of the GDPR Regulations, the Controller and the Processor shall designate the appointment of a Data Protection Officer and one was appointed.

The Data Protection Officer: DPO, provides Staff Training in relation to GDPR, and supports the organisation in respect of compliance. The DPO liaises with the Supervisory Authority, reviews and puts in place GDPR compliance measures and policies. The DPO acts as an intermediary between the relevant Stakeholders, provides advice and support to staff members in relation to GDPR Practice and Compliance.

Policy in respect of adherence / compliance with guidelines issued from the Office of the Data Protection Commissioner / The Supervisory Authority.

It is the Policy of SouthDoc to adhere to all guidelines issued by the Office of the Data Protection Commissioners / Supervisory Authority. These include guidance on such matters as CCTV Management as well as rulings, guidelines in respect of complaints made to that office.

Lawfulness of Processing - Article 6

Data Processing shall be lawful only if and to the extent that at least **One** of the following applies.

(a) The Data Subject has given consent to the processing of his or her Personal Data for one of more specific purposes.

(b) Processing is necessary for the performance of a contract to which the Data Subject is Party 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, in particular where the Data Subject is a child.

Policy in respect of informing Patients of their Privacy Rights:

SouthDoc has put in place a Privacy Policy which advises patients of their Privacy Rights when providing Personal Data. **See Privacy Impact Statement link.**

Policy in relation to Privacy by default or design and Data Protection Impact Assessments (DPIA)

Data Privacy must be at the heart of all future projects.

If SouthDoc engages in a new Data Processing Activity or if the processing activity is likely to increase the risk of a Data Breach. A Data Protection Impact Assessment will be carried out by SouthDoc as the Data Controller. A DPIA is the process which systematically considers the potential impact of a project or initiative might have on the privacy of individuals. It allows organisations to identify potential privacy issues before they arise, it also accesses the likely impact that a processing project is likely to have on stakeholders and it comes up with measures, proposals which will mitigate reduce and eliminate the potential risks.

The General Data Protection Regulations (GDPR) introduces mandatory DPIA's for those organisations involved in high risk processing, profiling of individuals or monitoring a public accessible area would be an example or where a DPIA is needed or required. If a Data Controller engages in this type of processing a Data Protection Impact Assessment (D.P.I.A) is required.

SouthDoc will also adopt Privacy by Design as a default approach. Privacy by Design and the minimisation of Data have always been implicit requirements of Data Protection Principles. However, GDPR ensures both principles of Privacy by Design and the principle of Privacy by Default in law.

Policy in Respect of Records Management Policy to ensure the security and the ready access of Data:

It is the Policy of SouthDoc to have and to implement a Records Management Policy throughout the organisation, these records contain both information and Data respectively.

The Policy is designed to ensure that there is a standardised filing system in which Data is securely held and readily accessible and retrievable in the event of a Data Subject Access Request under Article 15 of the GDPR Regulations and or Freedom of Information FOI request under the Freedom of Information Act 2014.

It should be noted that Data / Information can be held in the following formats:

- Paper Records
- Employee Personal Data / manual / electronically
- Text messages
- Electronic files
- Emails
- Financial records
- 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 / Retention Policy has been designed to enable the regular systematic destruction of records in line with the Policy and a log of any such destructions will be kept. In order to ensure all traces of the record details are kept and if the records are also in manual form they also have to be deleted.

Policy in respect of General Data Protection Regulation GDPR training of staff:

It is the policy of SouthDoc to train staff across the organisation in Data Protection Law and Practice Training and back up assistance is ongoing in this regard. Articles and, advice and points of interest are continuously placed on the Intranet which is a Staff Notice forum which is updated regularly. Advice and training has been and is provided on an ongoing basis. A significant amount of material, articles, audit templates advice has and continues to be placed on the RMS which is easily assessable by Doctors. Data Protection Breach training and guidelines is being provided for relevant personnel. The provision of information, support and training are ongoing. It should be noted that if a Member of the Gardaí requests information/Data for the purposes of preventing a crime the information is GDPR exempt under Article 2 (d)

Policy in Respect of CCTV Footage:

SouthDoc has a Policy in relation to CCTV footage which is regularly reviewed. A distinction is made between Public and Private CCTV. All CCTV footage is automatically deleted after 30 days with the exception of a Garda request for CCTV footage. Article 2 (d) of the GDPR Regulations provides that if information is sought in relation to the prevention of to a crime it is exempt from GDPR provisions and SouthDoc is required to provide this information by law. SouthDoc as an organisation is mindful of their responsibilities in relation to CCTV which involves the collection and retention of Special Category Data under Article 9 of the GDPR Regulations. SouthDoc and the Treatment Centres are secure facilities for a variety of reasons and CCTV monitoring is necessary to protect the integrity of the Staff. It is necessary that Data which we hold 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.

Third Party Processors / Data Processing Agreements:

A Processor is a Third Party that processes personal Data on behalf of SouthDoc. There are a number of instances where Third Parties have access to personal Data that belongs to or is controlled by SouthDoc in order to provide a service to SouthDoc as a Data Controller / Processor.

Prior to engaging Data Processors, SouthDoc will ensure the following.

(a) Carry out due diligence to ensure that it is appropriate to engage the processor

And

(b) Ensure the Processor puts in place an Agreement in writing notably a Data Processing Agreement / Third Party Contract with the processor that complies with the requirements under Data Protection Law.

The Processors must ensure that they keep the Data being processed safe and secure at all times. If there are any changes the Data Controller must be advised immediately by the Data Processor. If the Data Processor sub-contracts any of the processing the

Data Controller must be advised. If any Data is processed or transferred outside of the EU additional safeguards and procedures must be put in place.

Transfer of Personal Data outside the European Economic Area EEA:

Data Protection Law stipulates / provides that SouthDoc may not (save for a limited number of exceptions) transfer Personal Data outside of EEA to any Third Country unless the Country is deemed by the European Commission to provide an adequate level of protection in relation to the processing of Personal Data. Such transfer is regulated under Articles 45-50 of the General Data Protection Regulations GDPR 2018.

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

(a) 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.

(b) A transfer Agreement incorporating the Model Clauses in the form.

(c) 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 **and / or**

(d) 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.

Documenting and Monitoring Compliance:

SouthDoc has Policies and Procedures in place to ensure and demonstrate its ongoing compliance under Data Protection Law / GDPR Regulations.

Compliance is ongoing and is continuously monitored. Practices and Procedures are reviewed regularly to ensure they are fit for purpose. SouthDoc holds an inventory and details on the Data it holds:

(a) Categories of Personal Data held and processed

(b) The purposes of Processing

(c) Categories of People / Data Subjects

(d) Who the Personal Data relates to

(e) Details of recipients of the Personal Data

(f) Personal Data has been or will be disclosed to

(g) Data Access Request details

(h) Details of transfers

(i) Where possible, time limits retention periods

(j) Contact details of the Controller

Data Security:

SouthDoc 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 SouthDoc undertakes.

Policy in Respect of Managing Data Protection Breaches

It is the Policy of SouthDoc to detect, report and investigate a Personal Data Breach in accordance with GDPR 2018 Regulations and subject to the Guidelines as issued by the Office of the Data Protection Commission (DPC) The Supervisory Authority. (See Data Breach Policy GDPR 002 Issue 01)

All Personal Data / Sensitive Data breaches must be notified to the Supervisory Authority Article 33 & 34. It is mandatory and notification must be **made not later than 72 hours** after having become aware of it. When a breach occurs, the proactive steps must be taken to mitigate the efforts of the breach and to ensure there is no harm to the Data subject is most important. How the breach is dealt with is more important than the breach itself. If the matter is resolved within 72-hour period and if there is no **harm to the Data subjects** the matter will be recorded in the breach log but does not have to be reported to the Supervisory Authority. Such breaches may occur in the event of the loss of a USB keys. Disks, laptops, digital camera and mobile phones. All other electronic devices on which Data is held as well as paper records containing Data. If the Data is anonymised or encrypted as prescribed in the Regulations, the loss of the material in that context is not a breach. However, the event should be recorded.

A breach may also occur due to the release of Personal Data or Sensitive Personal Data under Article 9 without Authority or Consent. A breach may occur due to inappropriate access to such Data on SouthDoc systems or sending Data to unauthorised individuals.

In the event of a Data Protection Breach measures are put in place to prevent such an incident happening again. The findings resulting from the investigation and recommendations will be sent to the Office of the Supervisory Authority. We will liaise with the Authority and take whatever actions which may need to be taken as a result.

SouthDoc as a Data Controller has overall responsibility for ensuring compliance with Data Protection Law.

All employees have received General Data Protection Regulations GDPR compliance training and advice. Extensive material has been prepared and made readily available to all staff. Any queries will be and are dealt with and staff are supported in relation to GDPR issues. Staff training pertaining to GDPR compliance has been made available to staff on an ongoing basis.

SouthDoc Staff have a duty and should be mindful of Data Protection Issues and have to be careful when dealing with sensitive Personal Data. Employees should note that there are circumstances and instances where a Data breach can equate to serious employee misconduct.

Staff and Member Doctors at SouthDoc must report all Personal Data Breaches to the Data Protection Officer at SouthDoc.

The Data Protection Officer at SouthDoc will assist staff in complying with Data Protection Legislation by providing and facilitating support, assistance, advice and training.

Any Data Breach incident will be logged and measures put in place to ensure a breach does not in the future occur and what protections can be put in place to prevent breaches.

Data Access Requests – Article 15

A Data subject has a right to access his / her Data under Article 15 of the General Data Protection Regulations GDPR 2018 and under Data Protection Legislation 1997 and 2018 together with the Freedom of Information Act 2014. It is a Policy of SouthDoc to have a central point of access for Data Access requests as well as providing assistance to applicants making such requests. It is helpful if applicants provide their date of birth when they are making any such request.

All Data Access Requests **must meet certain requirements** which are specified and presented under the GDPR Regulations and the Data Protection Acts.

In order to deal and process Data Access Requests in a more efficient and professional manner **the requests should be submitted in the following manner:**

- Data Access Requests must be made in writing.
- All requests must contain identification and proof of current address this is to ensure that Personal Data is only released to those entitled to receive it.
- Data Subject Access Requests will be dealt with as soon as possible. It is important to ensure the information is correct and accurate and each request should contain ancillary supporting documentation thus avoiding delays to the Data Subject or their Agents. If the applicant/agent wishes to make a Data Access request for a public (GMS) patient. They should complete **Form A** which can be assessed by clicking link in the document attached.

  Form A Data Access Request can be made available or downloaded to GMS Patients by completing the attached form. Click here to download.

  Form B which can be made available or downloaded for Private Patients by clicking the link on the document attached. Click here to download.

  Applicants should download and complete the appropriate Access Request Forms and email it to dpo@southdoc.ie together with the appropriate supporting documentation where it will be processed.

  It is important that all parts of the form be competed.

  Form C Current / Former / Retired Employees can access their Employee Data by completing **Form C** and submitting the completed form to the HR Manager at SouthDoc to include employee number together with the appropriate and requisite supporting documentation. Click here to download.

Note:

Please note in relation to Form A which applies to GMS Patients. SouthDoc as an Organisation / Entity, which comes under the remit of the Freedom of Information Act 2014 Section 6 & 10 SouthDoc provides a service for the Health Services Executive (HSE) and is therefore a service provider. In this regard, all Freedom of Information requests must be made to SouthDoc and the HSE will process them. SouthDoc will forward the requests and Patient Outcomes to the HSE.

It is the Policy of SouthDoc to examine each request and to ensure that the Data can be relayed and should be released and that restrictions on the release of Data under the Acts 1988-2003 and 2018 under Article 23 GDPR Regulations. In addition, Article 18 deals with the Right to Restrict the Scope of Processing. Some of the grounds of restriction are as follows:

1. National Security or Defence
2. Public Security
3. The prevention, investigation, detection or prosecution of clinical offences or the execution of criminal penalties
4. Other important objectives of general public interest of the Union or of a Member State
5. The Protection of Judicial Independence and Judicial Proceedings
6. The Protection of Data Subject or the rights and freedoms of others
7. The enforcement of Civil Law Claims

SouthDoc is committed to providing an Out of Hours Family Doctor Service to the General Public. If the release of medial information is likely to cause upset or harm to the Patient / Service User. In this instance, there may be grounds for not releasing the information/ Data to the applicant / patient particularly if it is likely to cause them harm. Section 37 of the Freedom of Information Act (FOI) 2014 deals with exemption and grounds for not releasing information to Data Subjects / Patients.

It is SouthDoc's Policy is to release the information to the Data Subject / Patients unless there are compelling reasons not to. In addition, there may be legislative prohibitions /constraints for non-disclosure.

11 Points of Contact

Data Subjects can contact SouthDoc at its Headquarters in Killarney.

If you wish to make an access request or exercise your rights as outlined under Data Protection Law or if you have any queries, please contact the Data Protection Officer at SouthDoc.

Email:	dpo@southdoc.ie
Phone:	064 6691974
Postal Address	Data Protection Officer, Floors 2 & 3 Hilliard House, High Street, Killarney, Co Kerry. V93 KODN

Further information is available on the SouthDoc website: www.southdoc.ie

12 Further information

If you require further information on Data Protection, please contact the Offices of the Data Commissioner (The Supervisory Authority)

Lo Call Number	1890 252 231
Email	dpo@dataprotction.ie
Postal Address	Data Protection Commissioner, Canal House, Station Road, Port Arlington, Co Laois R32 NP 23

The following pages contain the links which are attached to the Data Protection Policy. They should be able to accessed by clicking on the link.

1. Privacy Impact Statement
2. Form A GMS Patients
3. Form B Private Patients
4. Form C Employee Access Data Requests