# Data Protection Policy

## General Data Protection Regulations

## GDPR 2016 / 679 – 2018

## Data Protection Acts 1988, 2003 & 2018

| | |
|---|---|
| **Author:** | Westdoc Data Protection Officer |
| | General Data Protection Regulations<br>GDPR 2016 / 679 - 2018<br>Data Protection Act 2018 |
| **Creation Date:** | 24.09.18 |
| **Review Date**: | 24.09.20 |
| **Related Policies:** | Data Breach Policy<br>Data Access Request Policy<br>Document Retention Policy<br>Privacy Impact Statement<br>Data Protection Impact Assessment Statement<br>Data Breach Management Policy |

## Table of Contents



**Author:** Data Protection Officer

**Creation Date:** 24.09.18

**Review Date**: 24.09.20

**Related Policies:**
Data Breach Policy
Data Access Request Policy
Document Retention Policy
Privacy Policy
Data Protection Impact Assessment Statement
Data Breach Management Policy

# 1 INTRODUCTION

This Data Protection Policy is a statement of Westdoc'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 2018 GDPR and the terms of the Policy supports their rights.

Westdoc as an Organisational entity provides an Out of Hours Family Doctor Service for Urgent Medical Care to the General Public. In order to provide the most effective and targeted range of services / supports and to meet the need 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 Westdoc.

- 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 entities regarding their personal data as well responsibilities on those persons processing and storing Personal Data.

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

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

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

## 2 PURPOSE

This Data Protection Policy is a statement of Westdoc'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 Westdoc which is a company limited by Guarantee it provides Out of Hours Medical service to the General Public in Galway City and the surrounding Region.

Westdoc Services Limited deals with the engagement of Locum Doctors and the management of GP financial contributions.

## 4 DEFINITIONS

**Controller or Data Controller:**

Any person 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.

**Personal Data:**

Persona Data Is defined in Article 4 (1) of the GDPR Regulations 2018, It refers to any information relating to an identified or identifiable natural person (data subject) is one who can be identified, directly or indirectly in particular by reference to an identifier such as a name, number, location, date 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.

**Data Processing:**

Data Processing has a wide definition. It means performing an operation or series of operations. It covers collection, recording, organisation, structuring, storage, adaptation, or alteration retrieved. Consultation, use disclosure by transmission, dissemination or otherwise making available alignment or combination restriction, erasure or destruction under Article 4 (2) of the Data Protection Regulations GDPR . It also 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 and 3 of Article 9 and in Article 6 (1) (a) to (e) which deals with the lawfulness of processing of Data by a Data Controller in this instance Westdoc.

## 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.

It should be noted that all personal Data / Special Category Data processed and retained by Westdoc in the course of its work and the service it provides is and will be dealt 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 Westdoc will handle, process and store Data, include how Data Access Requests are dealt with from a Data Subject together with how to manage Data Breaches.

Data in this Policy means applies to Personal and Sensitive Data under Article 9 (1) of the GDPR Regulations 2018.

Westdoc 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 will have full legal effect and applicability from 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.

Westdoc has controls and a Policy in place in respect of the use of CCTV systems and the organisation has a CCTV Policy.

**What is Data Protection?**

Data Protection is about ensuring that a person's personal record data is lawfully collected or with their consent, processed safety and retained as long as necessary to achieve the purpose for which it has been collected. Westdoc as a Data Controller carries out all duties and functions as set out in the Acts and ensures that the gathering and holding of data is done solely within the terms of the Acts.

**Appointment of a Data Protection Officer:**

Under Article 37 (1) of the GDPR Regulations, the Data Controller and the Processor shall designate the appointment of a Data Protection Officer and one was appointed at Westdoc on the 27.11.2017.

**The Data Protection Officer** DPO, provides staff training in relation to GDPR, 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 Westdoc 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 vested in the Controller.

(f) Processing is necessary for the purposes or the legitimate interest's perused by the Controller or by a Third Party. Exceptions where 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:**

Westdoc has 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's:**

Data Privacy is at the heart of all future projects.

If Westdoc 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 need to be carried out by Westdoc 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 it is needed and required. If a Data Controller engages in this type of processing a D.P.I.A is required.

Westdoc 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 the Westdoc to have and 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 freedom of information request apply to the Personal Data of GMS Public Patients.

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, if it is manual form, it will also be deleted.

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

It is the policy of Westdoc to train staff across the organisation in Data Protection Law and Practice Training and back up assistance is ongoing in this regard. Articles, 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 to Doctors on an ongoing basis. A large amount of material, articles, audit templates advice has and continues to be emailed / fax to the Doctors via secure line. Data Protection Breach Training and guidelines is being provided for Staff and Doctors. The provision of information, support and training are ongoing.

**Policy in Respect of CCTV Footage:**

Westdoc has a policy in relation to CCTV footage which is constantly reviewed. A distinction is made between Public and Private CCTV. All CCTV footage automatically deleted after 30 days with the exception if the Gardaí request CCTV footage. Article 2 of the GDPR Regulations. It is received and given to the Gardaí, as we are required to do so by law. Westdoc as an organisation is mindful of their responsibilities in relation to CCTV which involves the collection and retention of special category data under Article of GDPR. Westdoc and the Treatment Centres are secure facilities for a variety of reasons and security CCTV monitoring is necessary to protect the integrity of the staff and to maintain and provide the service. Care is taken to ensure images and neither deleted nor modified.

**Third Party Processors / Data Processing Agreements:**

A Processor is a Third Party that Processes Personal Data on behalf of Westdoc. There are a number of instances where Third Parties have access to personal data that belongs to or is controlled by Westdoc in order to provide a service to Westdoc as a Data Controller / Processor. Westdoc needs to engage the services of a Third Party who acts as a Processor on behalf of Westdoc.

Prior to engaging Data Processors, Westdoc needs to 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 Westdoc may not (save for a limited number of exceptions) transfer personal data outside of EEA to any third country unless the third country is deemed by the European Commission to provide an adequate level of protection in relation to the processing of personal data. Such transfer are 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, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

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

(c) The transfer is made pursuant to a Code of Contact or a Certification mechanism that has been approved by under applicable Data Protection Law together with binding and enforceable commitments of the Controller or Processor in the Third Party Country is applying the appropriate safeguards as regards data subjects rights **and**

(d) The data importer is subject to a framework approved by the European Commission to facilitate transfer e.g., EV and VS Data Privacy shields which deals with Data Transfers to and from the United States.

**Documentation and Monitoring Compliance:**

Westdoc 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.

Westdoc 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 to

(d) Which the personal relates to

(e) Details of recipients to whom the

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

(g) Data access requests details

(h) Details of transfers

(i) Where possible, time limits retention periods

(j) Contact details of the Controller and

(k) Data Protection Officer

**Data Security:**

Westdoc 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 Westdoc undertakes. Westdoc continuously monitors and upgrades Data Security measures to ensure that the Data it holds safe and secure all times. In addition, all Staff are continuously reminded of the necessity to ensure that all Sensitive Data is kept Safe and Secure at all times.

**Policy in Respect of Managing Data Protection Breaches**

It is the Policy of Westdoc 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.

All Personal Data / Sensitive Data breaches must be notified to the Supervisory Authority under Articles 33 & 34. It is mandatory and notification must be **made not later than 72 hours** after having become aware of the Breach. 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 hours 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 Westdoc 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.

Westdoc 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 and 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.

Westdoc 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 must report all personal data breaches to the Data Protection Officer at Westdoc.

The Data Protection Officer at Westdoc 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 in an incident report will be completed by the relevant Staff member who will immediately contact the Data Protection Officer (DPO) at Westdoc who will ensured that Breach is managed effectively and compliantly, measures will be 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 Westdoc to have a central point of access for Data Protection requests as well as providing assistance to requests.

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 "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. Westdoc seeks appropriate supporting documentary evidence to ensure that the person seeking the information is the correct Person and therefore they are entailed to obtain the information sought. These checks are necessary as Westdoc undertakes to protect the integrity and security of the data Westdoc which it holds pretending to its Patients and Service Users. The supporting evidential requirements together with the request access forms allow Data Subjects to make a Data Access Request easily the system is designed to be user friendly.
- 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 the agent's wishes to 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 info@Westdoc.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 Westdoc 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. Westdoc as an organisation / entity, which comes under the remit of the Freedom of Information Act 2014 Section 6 and 10. Westdoc provides a service for the Health Services Executive (HSE) and is therefore a service provider. In this regard, all Freedom of Information requests FOI's must be made through the HSE and they will process it. Westdoc will forward the requests and Patient Outcomes to the HSE if necessary

It is the Policy of Westdoc to examine each request and to ensure that the data can be relayed and should be released and if there are any restrictions as outlined by law on the release of Data under the Acts 1988-2003 and 2018 and 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

Westdoc is committed to providing an Out of Hours Family Doctor service for urgent medical care 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.

The Policy is to release the information to the data subject / patients unless these are compelling reasons not to. In addition, these may be legislative prohibitions constraints for no disclosure.

## 11 Points of Contact

Data Subjects can contact Westdoc at its Headquarters in Galway City.

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 Westdoc.

Email: matt@Westdoc.ie

Phone: 091 747 700

Postal Address

Matthew Breslin,

Data Protection Officer,
Westdoc HQ,
Unit 18A,
Lisbon Industrial Estate,
Tuam Road,
Galway

And

Matthew Breslin,
Data Protection Officer,
SouthDoc HQ,
Floors 2 & 3,
Hiliard House,
High Street,
Killarney,
Co Kerry

**Email** matt@westdoc.ie
mbreslin@southdoc.ie
**Telephone 064 66 91974**

Further information is available on the Westdoc website: www.westdoc.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 | info@Westdoc.ie |
| Postal Address | Data Protection Commissioner,<br>Canal House,<br>Station Road,<br>Portarlington,<br>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 Statements
2. Form A GMS Patients
3. Form B Private Patients
4. Form C Employee Access Data Requests

**Data Access Note:**

This Policy has been designed for the Organisation and will be put on the website, there are four links. The three forms must be capable of being downloaded or being completed and the Data Access Request emailed with the supporting documentation scanned to support the request.

**All** Data Access Requests must be accompanied by Data Subject consent, ID and proof of address. Requests must have the option to submit either manually or electronically and manually.