DATA PROTECTION POLICY

ISSUED 19.05.2022

GDP 001 V 1.1

INTRODUCTION

This Data Protection Policy is a statement of Westdoc's commitment to protect the data rights of service users and enables them to exercise their rights as outlined in the General Data Protection Regulations (GDPR) 2018.

Westdoc 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 supports, we are required to collect, process, store, and use data in both electronic and manual formats for a variety of purposes. This data is about Westdoc's staff, service users, doctors, and other individuals and entities who come into contact with Westdoc.

GDPR 2018 regulations as well as the Data Protection Acts 1988-2018 confer rights upon individuals and entities regarding their personal data as well as responsibilities on those processing personal data. This policy will ensure Westdoc's compliance with these rights and responsibilities.

This Data Protection Policy applies to all Westdoc employees, member GPs, and to any other person who interacts with and uses the service. It is the responsibility of staff and service users to comply with and familiarise themselves with the contents of this policy.

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) 2019 and under the terms of this policy.

2. SCOPE

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

3. REFERENCE DOCUMENTS

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

GDP 002	Data Breach Policy
GDP 003	Record Retention Policy

4. DEFINITIONS

Controller or Data Controller
Any person or entity who either alone or with other controllers control 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, 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, number, location, DOB or to one or more factors specific to the physical, generic economic or social identify of that natural person.

Data Subject
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:

- Performing an operation or series of operations.
- 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 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. RESPONSIBILITIES

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

6. PRINCIPLES OF DATA PROTECTION

All Personal Data shall be processed in accordance with the following principles according to Article 5 of GDPR Regulations 2018:

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.

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.

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

Westdoc 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 as well as rulings in respect of complaints made to these bodies.

9. LAWFULLNESS OF PROCESSING DATA

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, in particular where the Data Subject is a child.

10. INFORMING PATIENTS OF THEIR PRIVACY RIGHTS

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

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

If Westdoc 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 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.

Westdoc also adopts privacy by design as a default approach.

12. RECORDS MANAGEMENT POLICY

The Organisation has a Records Management Policy (GDP 005) 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
- 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.

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

1. Advice and training is provided on an ongoing basis.

2. Data Protection Breach training and guidelines is being provided for relevant personnel.

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

4. Advice and training on how to comply with GDPR whilst working from home will be provided.

14. CCTV FOOTAGE

There is a distinction between public and private CCTV.

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).

Westdoc 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.

15. THIRD PARTY PROCESSORS AND DATA PROCESSING AGREEMENTS

A Data Processor is a third party that processes personal data on behalf of Westdoc.

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

1. Ensure it is appropriate to engage the Data Processor
2. Ensure 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.

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

Data Protection Law stipulates that Westdoc, 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.

Westdoc 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 to
- Details of recipients of the personal data
- To whom personal data has been disclosed to
- Data Access Request details
- Details of transfers
- Where possible, retention periods
- Contact details of the Controller

18. 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.

19. MANAGING DATA PROTECTION BREACHES

Westdoc 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 available to staff. Staff as well as Member 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, and under Data Protection Acts 2018 as well as 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 Westdoc in the following manner:

- Data Access Request must be made in writing.
- 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 **Download Section**.

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

Supply **Form B,** which is found in **Download Section**.

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 **Download Section**. Submit the completed form to the HR Manager of Westdoc and include with it the employee number and appropriate supporting documentation.

Important note in relation to Form A

Form A applies to GMS patients. Westdoc 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 Westdoc 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, Westdoc 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 Westdoc at its Headquarters in Killarney.

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 at Westdoc.

Email:	dpo@Westdoc.ie
Phone:	091 747 700
Postal Address	Data Protection Officer, Westdoc HQ, Unit 18A, Lisbon Industrial Estate, Tuam Road, Galway

Further information is available on the Westdoc website: www.westdoc.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@dataprotction.ie
Postal Address	Data Protection Commissioner, Canal House, Station Road, Port Arlington, Co Laois R32 NP 23