DATA BREACH POLICY

Issued 23.05.2022

GDP 002 V 1.1

INTRODUCTION

Westdoc as an organisation is acutely aware of its responsibilities as a data controller. The security and protection of Special Category Data, as outlined in Article 9 of the General Data Protection Regulations (GDPR) 2018, is paramount to the organisation. Special Category Data is defined as follows:

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- Genetic and biometric data for the purpose of uniquely identifying a person's data concerning health or data concerning a person's sex life or sexual orientation.

It shall be prohibited to process this data belonging to an individual, however there are exemptions outlined under subsections 2 through 4 of Article 9 as well as under subsections (a) through under Section 1 of Article 6 of the GDPR Regulations 2018.

Any data breach must be managed correctly and their effects must be contained. The protection and upholding the rights and freedoms of the data subject or subjects is always paramount to Westdoc.

1. PURPOSE

The purpose of this procedure is to document and implement the Data Breach Policy in accordance with the General Data Protection Regulations (GDPR) 2018.

2. SCOPE

This policy extends to the entire organisation known as Westdoc.

3. REFERENCE DOCUMENTS

GDP 002 FR 01	Data Breach Incident Form
GDP 002 FR 02	Data Breach Log

4. DEFINITIONS

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 a natural person's sex life or sexual orientation.

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

Data Breach

A data breach is defined in Article 4, Section 12, of the GDPR Regulations 2018 as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored, or otherwise processed."

5. RESPONSIBILITIES

The Data Protection Officer has the responsibility to enforce and ensure this policy is complied with. In the event of a data breach, it is the responsibility of the staff member aware of the breach to immediately contact the DPO.

6. DATA BREACH

There are three kinds of personal data breaches relevant to the Organisation. They are:

It should be noted that the Data Breach Protocol applies equally to both physical and electronic records.

There are three types of personal data breaches, which are:

1. **Confidentiality Breach**
   This occurs when there is inappropriate access control allowing unauthorised use of personal data. Examples of this breach are:
   - Obtaining personal information by deception
   - Misaddressing of emails, faxes, etc. (human error)
   - Sending material to the incorrect party
   - Leaving patient data on a screen in GP surgeries when and where it can be seen by unauthorised third parties.
   - Intentional or malicious data breaches by employees
   - Identity theft

   This list is not exhaustive.

2. **Availability Breach**
   This occurs where there is accidental or unauthorised loss of access or destruction of personal data.

3. **Integrity Breach**
   This occurs where there is an unauthorised alteration of personal data.

As Westdoc and CIT process Special Category Data, a protocol must be followed in the event of a data breach to ensure minimal if any harm is done to Data Subjects

7. PROCEDURE IN THE EVENT OF A DATA BREACH

1. Contact the Data Protection Officer at Westdoc HQ at:
   a. Email: dpo@Westdoc.ie
   b. Tel: 091 747 700

   If the DPO is unavailable, contact the General Manager at number above. Notification must be made immediately.
2. The Data Breach Incident Report (GDP 002 FR 01) must be submitted by the member of staff and the report must contain the following:
   a. Date and time of the breach.
   b. How the breach occurred.
   c. How the breach was detected.
   d. Number of individuals potentially affected by the breach.
   e. Type of personal data disclosed, e.g. name, address, PPSN, medical information.
   f. If the data has been secured or retrieved.

g. Measures implemented to mitigate the risk of reoccurrence.

3. If the data breach is likely to cause harm to the data subjects, the DPO must report the incident to the Supervisory Authority. If there is no harm to the data subjects, the breach does not have to be reported but must be logged.
4. Notification of a data breach is **mandatory** and must be made by the DPO to the Supervisory Authority **within 72 hours** of becoming aware. If the notification is not made within the 72-hour period, the reasoning for the delay must accompany the notification when it is made. The notification is made by the DPO on foot of the report from the staff member and is logged in accordance with Article 33 of the GDPR Regulations 2018.
5. The following data breaches are examples of breaches that do not need to be reported to the Supervisory Authority:
    a. Where data on a computer or physical information is lost or mislaid and the material is recovered with no harm to the data subject **or** the device is encrypted.
    b. Where a fax is sent to wrong place or person by mistake and the information is retrieved with no harm to the data subject.

6. PUBLISHED GUIDELINES

The Office of the Data Commissioner have issued guidelines for the transfer of patient information between medical professionals, found here.