PROCEDURE NAME	Data Breach Policy	**PROCEDURE NO.**	GDPR, 002
MANAGER RESPONSIBLE	Joanna Pollock	**VERSION NO.**	3.0
SIGNATURE		**APPROVALS DOCUMENT OWNER**	JP

VERSION HISTORY				
VERSION	**REVIEWED BY**	**ISSUE DATE**	**DESCRIPTION OF CHANGE**	**APPROVED BY**
2.0	Michéal O'Neill	23.05.2022	Updated format	MON
1.0	Máire Hussey, Úna Houlihan	01.11.2018	Initial release of document	MH, UH

1. INTRODUCTION

SouthDoc as an organisation is acutely aware of its responsibilities as a data controller. The security and protection of Personal Data and Special Category Data, as outlined in GDPR is paramount to the organisation.

Any suspected incident or breach must be managed correctly, and risks mitigated.

2. PURPOSE

The purpose of this document is to provide guidance on the process that must take place should an incident or breach occur.

3. SCOPE

This policy applies to all SouthDoc staff, students, contractors, sub-contractors, agency staff and authorised third party commercial service providers when receiving, handling, or processing personal data as defined by the GDPR.

4. DEFINITIONS

A list of terms used throughout this policy are defined in Appendix 1.

5. DATA BREACH

A data breach is the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data in either physical or electronic form.

Personal data breaches can be categorised into three categories:

1. **Confidentiality** breach, where there is an unauthorised or accidental disclosure of or access to personal data.
   Examples include:
   - Obtaining personal information by deception.
   - Misaddressing of emails.
   - Sending material to the wrong party.
   - Leaving patient data on a screen 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, where there is an accidental or loss of access to our destruction of personal data.
   Examples include:
   - A cyberattack which prevented access to and/ or destroyed records.

3. **Integrity** breach, where there is an unauthorised or accidental alteration of personal data.

A data breach may involve all three categories, depending on the circumstances.

6. PROCEDURE IN THE EVENT OF A DATA BREACH

If a suspected or confirmed data breach has occurred, staff members must report this immediately to the DPO, and provide a completed copy of the incident report.

The DPO must immediately assess the report and confirm if a data breach occurred or data breach incident.

If a data breach has occurred and is likely to cause harm to the data subjects, a report must be submitted to the Supervisory Authority, DPC.

If there is no harm to the data subjects, the breach does not have to reported but must be logged.

All notifications to the DPC must be made without undue delay, and no later than 72 hours after the DPO 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 breach notification must include:

- The nature of personal data breach.
- The categories and approximate number of individuals concerned.
- Categories and approximate number of personal data records concerned.
- Name and contact details of DPO or other contact point.
- Description of likely consequences of personal data breach.
- Description of measures taken or proposed to deal with personal data breach, including measures to mitigate possible adverse effects.

If the breach is likely to result in a high risk to an individual's rights and freedoms, you must also inform those individuals without undue delay.

The following are examples of data breaches that do not need to be reported to the DPC:

- 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.
- Where a fax is sent to the wrong place or person by mistake, but the information is retrieved with no harm to the data subject.

7. ASSOCIATED DOCUMENTS

The following documents will provide additional information:

- Data Protection Policy
- Data Breach Incident Report
- Mobile Computing or Storage Device Incident Report
- Data Breach and Incident Log

8. ROLES AND RESPONSIBILITIES

DPO
The DPO has the responsibility of ensuring this policy is complied with and the relevant notifications are made accurately without delay.

Others
All individuals covered under the scope of this policy must ensure that any breaches are reported immediately.

8. POINTS OF CONTACT

The first point of contact for any queries or requests should be directed to the DPO at SouthDoc Head Office.

Email: dpo@southdoc.ie

Phone: 064 6691974

Postal address: Data Protection Officer,
Floors 2&3 Hillard House,
High Street,
Killarney,
Co. Kerry
V93 K0DN

If one requires additional information on Data Protection, they should contact the Office of the Data Protection Commissioner (The supervisory authority).

Email: dpo@dataprotection.ie

Lo call number: 1800 437 737

Postal address: Data Protection Commission,
21 Fitzwilliam Square South,
Dublin 2,
D02 RD28

APPENDIX 1: DEFINITIONS

Consent
A freely given, specific, informed and inambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

Data
In this policy 'data' shall mean information which either:

- is processed by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should be processed by means of such equipment;
- is recorded as part of a relevant filling system or with the intention that it should form part of a relevant filling system;
- does not fall within any of the above, but forms part of a readily accessible record.

Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of a relevant filling system.

Data Controller
A person or organisation who determines the purposes and methods of processing personal data.

Data Processor
A person or organisation that holds or processes personal data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the personal data.

Data Protection
The protection of personal data.

Data Protection Commission (DPC)
The DPC is the Irish supervisory authority for the GDPR and also has functions and powers related to other regulatory frameworks including the Irish ePrivacy Regulations (2011) and the EU directive known as the Law Enforcement Directive.

Data Protection Officer (DPO)
The role within a company whose responsibility is to ensure that the company or organisation is correctly protecting individuals' personal data according to current legislation.

Data Subject
A living individual to whom personal data held relates, including: employees, patients, suppliers. It should be noted that GDPR do not apply to deceased persons and to their data.

Personal Data
Personal data is any information relating to an identified or identifiable living person (data subject) who could be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location, DOB, or to one or more factors specific to the physical, physiological, genetic, economic, cultural, or social identity of that individual.

Personal Data Breach
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.

Special Category Data
GDPR provides extra protection for certain categories of personal data, called 'special category data' – referring to data which reveals:
"Racial or ethic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

These categories of personal data shall not be processed unless a controller can avail of one of the exceptions under Article 9 (2) of the GDPR.