Data Breach 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 14	Management	SouthDoc	1/11/2018	All amendments completed and updated.	Matt Breslin

1 PURPOSE

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

2 DEFINITION

This Policy purports to provide clarity and guidance in managing and dealing with Data Breaches, together with minimising the effects and impact of such a Data Breach upon the Data Subject(s) in accordance with the provision of Article 34 (1) GDPR Regulations 2018.

3 SCOPE

This Policy extends to the entire Organisation known as SouthDoc.

4 PROCEDURE

Introduction:

SouthDoc as an Organisation is acutely aware of its responsibilities as a Data Controller. The security and protection of Special Category Data as outlined in the GDPR Regulations, Article 9 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 and the processing of genetic Data, biometric Data for the purpose of uniquely identifying a natural person's Data concerning health or Data concerning a natural person's sex life or sexual orientation. It shall be prohibited to process this Data belonging to an individual however, there are exemptions as outlined under sub sections 2 to 4 of Article 9 and under Article 6 (1) Sub -Sections (a) to (e) of the GDPR Regulations 2018.

Any Data Breach must be managed correctly and their affects must be contained. The protection and upholding the rights and freedoms of the Data Subject and or Subjects are always paramount to SouthDoc.

Managing a Data Breach

It should be noted that a Data Breach can have serious consequences for an Organisation and for all concerned including Staff and Service Users.

Effective Management of the breach is more important than the breach itself. It is vital that immediate and proactive steps are taken by the Data Controller to minimise the effects of the breach on the Data Subject or Subjects.

A Data Breach is defined under GDPR Regulations 2018 in Article 4 (12) 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".

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

It relates to a **type of security incident. Article 4 (12) only applies where there is a Breach of Personal Data.** It means that the Data Controller ensures compliance with the principles relating to the processing of Personal Data as outlined in Article 5 of GDPR Regulations. A notable distinction is made between Security Breaches Personal Data Breaches and Integrity Breaches they do not always follow each other.

There are three types of Personal Data Breaches as follows:

1 **"Confidentiality Breach"** occurs where there is inappropriate access control allowing unauthorised use. For example, in the context of a hospital, if critical patient medical Data is unavailable, even temporarily, this could present risk to the rights and freedoms of individuals which would come under the remit of **Article 34.** If operations / surgery had to be cancelled as a result. Please note the following Breach examples:

Hacking / Cyber Attack

- Infection by ransomware which would encrypt the Controller's Data until a ransom is paid
- Obtaining information by deception
- Misaddressing of emails / faxes / 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.
- Wilful / malicious Data breaches by employees
- Identity theft
- If an individual receives an email impersonating a particular Data Controller which contains Personal Data relating to the Controllers.

This list is not exhaustive, there may be other instances and scenarios where there is an unauthorised or accidental disclosure of or access to Personal Data.

2. "**Availability Breach" occurs wh**ere there is accidental or unauthorised loss of access or destruction of Personal Data.

3. **"Integrity Breach"** where there is an unauthorised or accidental alternation of Personal Data.

There are a number of typical examples of Data Breaches:

- Loss or theft of Data equipment on which Data is stored.
- Loss of unencrypted Data, where it is not possible to ascertain whether unauthorised persons have gained access to it.
- Loss of the Data Controllers' customer database where it is lost or stolen, loss or theft of documents / folders.
- A breach of security leading to the accidental or unlawful destruction or loss of the Data.
- Unforeseen circumstances such as a flood or fire which destroys information which could lead to Data Breaches, these events may effect an individual or individuals.

What to do in the event of a Data Breach?

1. In the event of a Data Breach staff should contact the Data Protection Officer, SouthDoc HQ who can be contacted via email at dpo@southdoc.ie Telephone 064 66 91974 or in the event that the Data Protection Officer is unavailable or on leave please the General Manager, Telephone 064 66 91974.

   Notification in the event of a Data Breach **must be made immediately** to the Data Protection Officer at SouthDoc HQ

2. A report must be submitted by the member of staff and the report must contain the following information:

   (a) The date and time of the Breach
   (b) How the Breach occurred
   (c) How the Breach was detected
   (d) Number of individuals effected by the breach (potentially)
   (e) Type of Personal Data disclosed e.g. name, address, PPS number, sensitive medical information
   (f) Whether or not the Data has been secured / retrieved
   (g) Measures to be implemented to mitigate the risk of reoccurrence of a similar type of incident in the future
   (h) What lessons have been learnt from events

3. Data Breach Notification is **Mandatory** and must be made by the DPC within **72 hours** after having become aware to the Supervisory Authority. If notification is not made within the **72-hour period** reasons for the delay must accompany the notification when it is made. In the event of a Data Breach the Staff Member shall complete a Data Breach Incident Report Form attached, GDPR, FR01, Issue 01.

4. Details of the Data Breach are completed by the Data Protection Officer on foot of the report from the Staff Member. The Breach Notification Form is completed and the Breach is logged in accordance with Article 33 of the GDPR Regulations 2018.

   The Data Protection Office provides guidance for the completion of the Data Breach Notification Form attached.

5. Where the Personal Data Breach is likely to result in a high risk to the rights and freedoms of the Natural Person, the Breach must be reported to the Office of the Data Protection Commission under Article 34 (1) of the GDPR Regulations 2018. The minimum sanction and containment of any harm/ distress to the Data Subject (s) is a vital aspect in dealing with any Data Breach.

6. There are instances where a Data Breach does not have to be reported to the Supervisory Authority, this would arise if there is no harm to the Data Subject but the incident must still be lodged using the Data Breach Log. The logging of the incident should contain a report as to how the Breach occurred, how it was dealt with, an account of remedial measures to contain and minimise the effects of the Breach.

   The log should also contain details of ongoing and future measures to avoid reoccurrence of a similar event.

   The retention and maintenance of the Breach Log is to comply with GDPR Regulations 2018 and for Data Audit purposes. A practical example of where a Data Breach occurs which needs to be logged and there is no harm to the Data Subject, in these instances the **Data Breach does not need to be reported to the Supervisory Authority examples of this are as follows:**

   (a) Where Data on a computer / manual information is lost or mislaid and the material is recovered with no harm to the Data Subject **or** if the device is encrypted.

   (b) If a fax is sent to the wrong place or to the wrong person in error and by mistake and the information is retrieved and there is no harm to the Data Subject.

It is the Policy of SouthDoc to manage any Data Breach that occurs and to assist and support staff in relation to them, while at the same time fully complying with Data Protection laws.

The Office of the Data Commissioner have issued guidelines for the transfer of patient information between Medical Professionals entitled “The Data Protection Rules in Practice”. See Guidelines attached.

Article 29 Work Party Guidelines outlines and provide a number of examples of Personal Data Breaches and they provide a number of useful guides pertaining to notification requirements to the Office of the Data Commissioner.

The distinction is clearly made between Data Breaches if there is harm, distress or a risk to the freedom of the natural person i.e. the Data Subject. **The Mandatory Requirement** is to report the Breach to the Office of the Data Commissioner which has to be complied with. If there is no harm to the Data Subject (s) then the Breach does not have to be reported but logged.

See reporting examples attached Article 29 Extract

7. Staff can report a Data Breach by completing the Data Breach Incident Form to the Data Protection Officer in SouthDoc as outlined.

This Policy should be read in conjunction with SouthDoc Data Protection Policy.

Appendix link attached

Data Breach Incident Form

Data Breach Notification Form

Guidelines on the completion of the Data Breach notification form

Data Breach notification requirements

Medical and Health Sector Guidelines from the Data Protection Commission

Data Breach Log