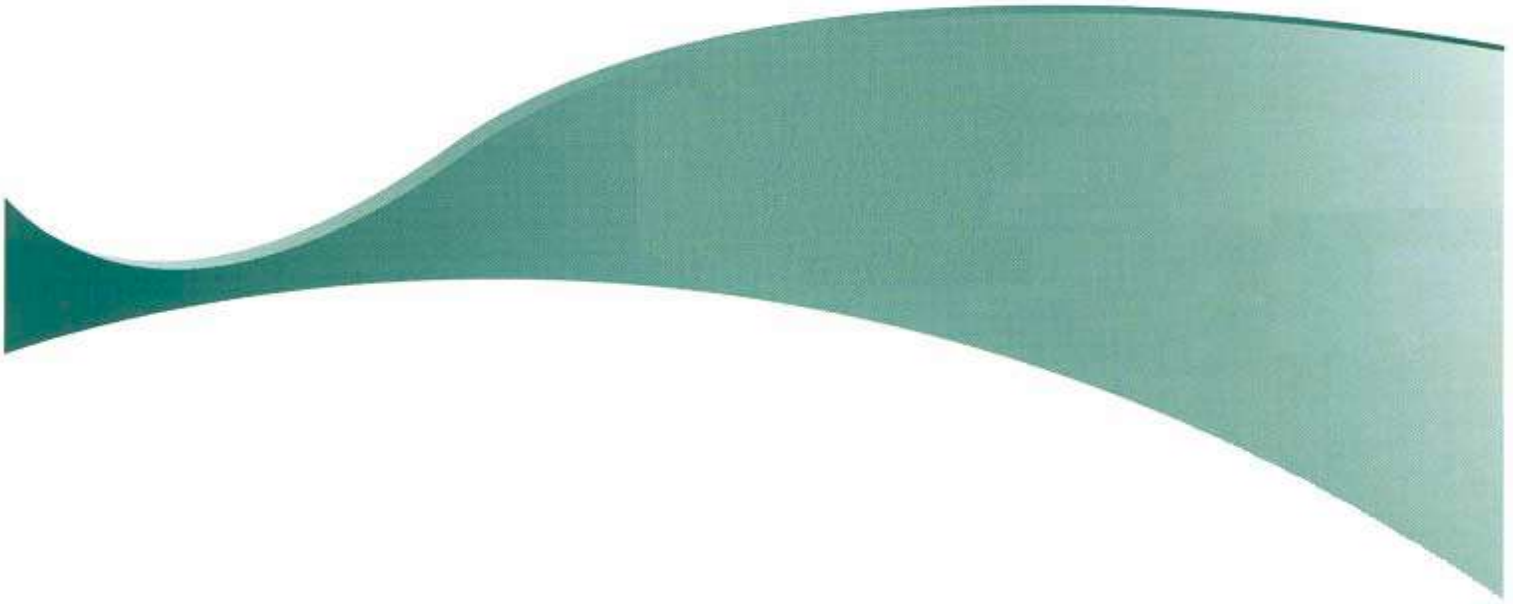
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Data Breach Process Guidance



June 2019

The purpose of this document is to provide guidance on the process that **must** take place should an incident or breach occur either within the HSE or externally by third party data processor.

'Personal data breach' means 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.

Under the General Data Protection Regulation (GDPR), all personal data breaches must be reported to the Data Protection Commissioner with 72 hours of first becoming aware of the breach.

The process flow map for the process is shown at the end of this guidance document

Roles	
DPO	Data Protection Officer – Monitor GDPR compliance
DDPO	Deputy Data Protection Officer – they are the regional managers in Consumer Affairs. They will inform and provide advice to staff about the data breach process.
Data Subject	Person who the personal data relates to. Will be notified of the breach if necessary.
DPC	Data Protection Commissioner – The data protection regulator
Relevant Manager	The manager of the member of staff who first becomes aware of the incident
Incident Identifier	Any member of staff who first becomes aware of the incident
External Data Processor	Must fill out external data breach incident report form

1. Incident Identified

All staff should be able to identify a breach or incident and should be aware of who to report the breach to should they have to report such a breach or incident. Early recognition and reporting of breaches is essential to ensure the **72 hr time limit for reporting to the DPC** is achieved.

2. Notify Relevant Manager

The relevant manager must be notified of the potential breach and will have to sign the Data Breach Incident Report form. It is the responsibility of the relevant manager to manage a breach that is incurred by a third party processor. The data processor has a responsibility to complete the External Data Breach Incident Report form and return immediately to the relevant manager. The relevant manager will then follow the process below.

3. Possible Data Protection Incident or Breach?

The manager will identify if the incident in question is potentially a data protection breach or incident. If it is definitely not a data protection incident or breach no further action is needed.

4. Data protection breach form completed and sent to DDPO

Data breach incident forms are available from https://www.hse.ie/eng/gdpr and should be completed as soon as possible when the incident is verified. All of the sections on the form must be completed by the staff member who identifies the incident and their line manager. The form must be sent to the DDPO and also, in the event of an information systems security breach, to the OoCIO.

5. Data Protection Incident or Breach?

The DDPO will confirm if it is a data protection incident or breach and advise accordingly.

Incident

6. DP Incident logged, Corrective actions advised

The incident should be recorded by the relevant manager. The relevant manager will liaise with the DDPO and in consultation with him/her, advise of corrective action that should be made to prevent the incident recurring.

7. Log incident, begin implementing corrective actions

The relevant manager should also log the incident and implement the corrective actions identified and any additional actions that were advised by the DDPO.

Breach

8. Log Breach, Advise of corrective actions

The DDPO should log the breach with the DPC and advise of any corrective actions that have taken place.

9. Start containment and recovery

The relevant manager should try to recover any data or file that has been compromised to mitigate as much risk as possible. Containment involves limiting the scope and impact of the breach of data/information. While the relevant manager must take the lead, advice and guidance is available from the DDPO and OoCIO.

The DDPO will:

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment and recovery exercise. For example, communication dept. Gardaí, management team etc.

The relevant manager should:

- Establish whether there is anything that can be done to recover losses and limit the damage the breach can cause. For example, changing access codes to server rooms or medical records libraries/ examining physical access etc.
- Implement the changes prescribed by the DDPO

The OoCIO will:

- Have a role in containment and recovery from an information systems point of view. For example, this might entail isolating a compromised section of the network or remotely wiping a mobile device.

10. Compile risk assessment – Compile breach report

In assessing the risk arising from the data breach to the data privacy rights and freedoms of the data subject, the relevant manager should, in consultation with the DDPO consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, the following points should be considered:

- What type of information/data is involved?
- How sensitive is the information/data?
- Are there any security mechanisms in place (e.g. password, protected, encryption)?
- What could the information/data tell a third party about the individual?
- How many individuals are affected by the breach?
- Have all of the data subjects affected by the breach been identified and are their contact details available?
- Is the breach likely to adversely affect the data privacy rights and freedoms of the data subjects concerned?

11. Large scale or highly sensitive Breach?

Does the breach affect a large number of people or does it significantly pose a risk to the rights and freedoms of the data subjects involved. If yes the DDPO should inform the DPO and the DPO will advise of any corrective actions as required. If not, the DDPOs should give instruction to the local relevant managers on corrective actions and how to prevent the breach from happening in the future.

12. Notify data subjects

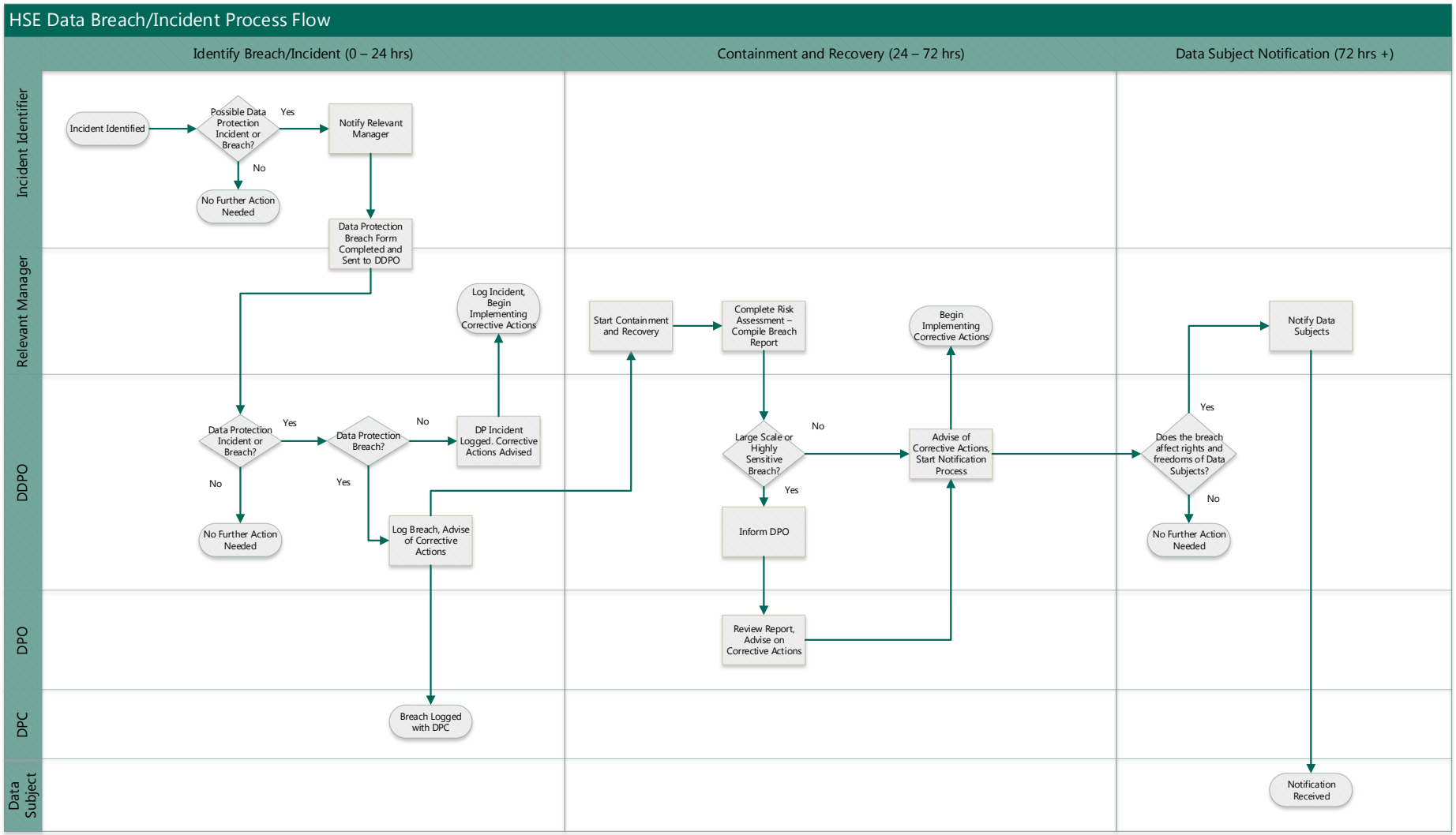
The relevant manager, following a discussion with the DDPO, should notify the data subjects as appropriate and should, in clear and plain language (written or verbal):

- Outline what has occurred with their personal data and apologise for the incident;
- provide name and contact details for further information;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the relevant manager to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

- Confirm that the DPC has been notified of the breach;
- Record notification to data subject.

Please note; Data Protection Breaches have to be reported to the Data Protection Commissioner. In that regard the Area Consumer Affairs/Regional Consumer Affairs officers are the only HSE officers designated to report a breach to the Data Protection Commissioner.

Deputy Data Protection Officer West, (excluding voluntary agencies) **Consumer Affairs, Merlin Park University Hospital, Galway.** • **CHO 1 – Cavan, Donegal, Leitrim, Monaghan, Sligo** • **Community Healthcare West – Galway, Mayo, Roscommon** • **Mid-West Community Healthcare – Clare, Limerick, North Tipperary.** • **Saolta Hospital Group**	Email: ddpo.west@hse.ie Phone: 091-775 373
Deputy Data Protection Officer Dublin North-East (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE Dublin North East, Bective St., Kells, Co Meath.** • **Midlands, Louth, Meath Community Health Organisation** • **Community Health Organisation Dublin North City & County** • **CHO 6 – Dublin South East, Dublin South & Wicklow** • **RCSI Hospital Group** • **National Children's Hospital**	Email: ddpo.dne@hse.ie Phone: Kells Office: 046-9251265 Cavan Office: 049-4377343
Deputy Data Protection Officer Dublin mid-Leinster (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE, Third Floor Scott Building, Midland Regional Hospital Campus, Arden Road, Tullamore, Co. Offaly.** • **Dublin Midlands Hospital Group** • **Ireland East Hospital Group** • **Community Healthcare Dublin South, Kildare & West Wicklow**	Email: ddpo.dml@hse.ie Phone: Tullamore Office: 057-9357876 Naas Office: 045-920105
Deputy Data Protection Officer South (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE South, Ground Floor East, Model Business Park, Model Farm Road, Cork. Eircode: T12 HT02** • **Cork & Kerry Community Healthcare** • **CHO 5 – Carlow, Kilkenny, South Tipperary, Waterford & Wexford** • **UL Hospital Group** • **South South-West Hospital Group**	Email: ddpo.south@hse.ie Phone: Cork Office: 021 – 4928538 Kilkenny Office: 056 -7785598.


HSE Data Breach/Incident Process Flow
Identify Breach/Incident (0 – 24 hrs)
Containment and Recovery (24 – 72 hrs)
Data Subject Notification (72 hrs +)
Incident Identifier
Relevant Manager
DDPO
DPO
DPC
Data Subject
Incident Identified
Possible Data Protection Incident or Breach?
Yes
No
Notify Relevant Manager
No Further Action Needed
Data Protection Breach Form Completed and Sent to DDPO
Log Incident, Begin Implementing Corrective Actions
Data Protection Incident or Breach?
Yes
No
Data Protection Breach?
No
Yes
DP Incident Logged. Corrective Actions Advised
No Further Action Needed
Log Breach, Advise of Corrective Actions
Breach Logged with DPC
Start Containment and Recovery
Complete Risk Assessment – Compile Breach Report
Large Scale or Highly Sensitive Breach?
No
Yes
Inform DPO
Review Report, Advise on Corrective Actions
Begin Implementing Corrective Actions
Advise of Corrective Actions, Start Notification Process
Does the breach affect rights and freedoms of Data Subjects?
Yes
No
No Further Action Needed
Notify Data Subjects
Notification Received