Feidhmeannas Seirbhíse Sláinte
Health Service Executive

General Data Protection Regulation (GDPR)
Data Breach Incident Report

Private & Confidential

Title:	HSE General Data Protection Regulation (GDPR) Data Breach Incident Report
Author:	Joe Ryan
Publication date:	May 2018
Review Date:	May 2020

Document History

Version	Owner	Author	Publish Date
1.0	HSE	Joe Ryan	May 2018
1.1	HSE	Joe Ryan	June 2019

About this incident report.

This incident report must be completed immediately (**IN BLOCK CAPITALS)** by HSE employees and their line manager whenever confidential or personal data held by the HSE is compromised leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed or whenever a HSE mobile storage device is lost or stolen.

The completed report must be forwarded immediately and no later than 24 hours after the incident, via fax or email (a scanned copy) to the employee's local **Consumer Affairs Office** (for incidents involving accidental disclosure, loss or theft of manual (paper based) data) or **ICT call centre / helpdesk** (for incidents involving accidental disclosure, loss or theft of electronic data or, the loss or theft of a HSE mobile computer or storage device). Contact details at end of report.

Section 1: Employee Contact Details	
Employee name:	
Employee personnel number:	
HSE Directorate / Service:	
Location	
Contact phone numbers: (include mobile number)	
Email address:	

Section 2: Incident Details	
At what time and on what date did the incident occur?	Is this an estimate?
Please enter the date and time the HSE became aware of the incident:	
Please explain the details of the incident	

Section 3: Data Details
For further advice before contacting individuals, please contact your local Deputy Data Protection Officer

What is the format of the data lost, stolen or accidently disclosed?

- ☐ Manual (paper based)
- ☐ Electronic

What is the Nature of the Breach?	What identifying details relating to individuals were disclosed (select all that apply)?
☐ Devise lost/stolen (encrypted) ☐ Device lost/stolen (unencrypted) ☐ Paper lost/stolen ☐ Disclosure (unauthorised ☐ Inappropriate disposal of paper ☐ Hacking ☐ Malware ☐ Phishing ☐ E-Waste personal data present on obsolete device ☐ Unintended online publication	☐ Data subject identity (name, surname, birth date) ☐ PPSN (or other national identification number) ☐ Contact details ☐ Identification data (passports, licence data etc.) ☐ Economic or financial data ☐ Location Data ☐ Criminal convictions, offences or security measures

Were Special Categories of Data Involved?

☐ Yes ☐ No

If 'Yes' is selected above, what types of special categories of data were involved (select all that apply)?

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Health data
- ☐ Genetic data
- ☐ Biometric data

Please give a detailed description of the data which was lost, stolen or accidentally disclosed (for example, client / patient medical records, business data, unpublished financial reports, unpublished medical research or employee personnel records). For medical or personnel records please include a description of record fields (for example name, address, PPS number, DOB, medical history etc.).

Number of Individuals Involved?	Number of records lost, stolen or accidentally disclosed?

Do you have a backup copy of the lost or stolen data records?
- ☐ Yes
- ☐ No

Were vulnerable individuals affected? (A vulnerable individual is a child or person who, by reason of physical or mental incapacity, is unable to act on their own behalf)
- ☐ Yes
- ☐ No

Were the affected Individuals notified?
- ☐ Yes
- ☐ No

If not, what is the proposed procedure?

Section 4: Mobile Computing or Storage Device Details
(Only complete this section for incidents involving the loss/theft of a HSE mobile computer or storage device)

What type of mobile computer or storage device which was lost or stolen along with the data?
(For example laptop, mobile phone, PDA, external hard drive, CD etc.)

Make / model of mobile computer device:

HSE asset tag of mobile computer device:
(if applicable):

Phone number of mobile computer device:
(if applicable)

Was the mobile computer or storage device password protected? ☐ Yes ☐ No	If Yes, please include length of password
Was the confidential or personal data stored on the mobile computer device encrypted? ☐ Yes ☐ No	What is the electronic format used to store the personal data on the mobile computer devices? (E.g. word, excel, pdf email etc.)

Was the storage of the confidential or personal data on the mobile computer device authorised by the designated HSE Information Owner?
- ☐ Yes
- ☐ No

If Yes, state the designated HSE Information Owners Name

State the reason(s) for storage of confidential or personal data on the mobile computer device?
What is the electronic file format used to store the confidential or personal data on the mobile computer device? (For example, MS, Word, Excel, PowerPoint, PDF, notepad, email, system extract etc.):

Section 5: Measures in Place
Please Describe the relevant technical / organisational measures that were in place prior to the breach?

Section 6: Follow Up Action
List follow up action taken to prevent repetition of the incident:

Section 7: Sign-Off	
Employee Signature:	
Line Manager Signature:	
Print Name:	
Contact Phone Number(s)	
Email Address:	
Date:	

Section 8: Contact Details	
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.

Incomplete or illegible reports will be returned to the sender