



Feidhmeannas Seirbhíse Sláinte  
Health Service Executive

# **General Data Protection Regulation (GDPR)**

## **Data Breach Incident Report**

To be completed by Data Processors  
when notifying the HSE as a Data Controller

**Private & Confidential**

**Document Information**

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 data processors whenever confidential or personal data held by them on behalf of 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 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 relevant data controller in the HSE with whom you have a contract.

<b>Section 1: Company Contact Details</b>	
Company name:	_____
Company address:	_____
Person assigned to deal with DP Breach:	_____
HSE Directorate / Service with whom you have a contract:	_____
Location	_____
Contact phone numbers: (include mobile number)	_____
Email address:	_____

<b>Section 2: Incident Details</b>	
At what time, and on what date did the incident occur?	Is this an estimate?
Explain the details of the incident	

<p>What is the format of the data lost, stolen or accidentally disclosed?</p> <p><input type="checkbox"/> Manual (paper based)</p> <p><input type="checkbox"/> Electronic</p>	
<p>What is the Nature of the Breach?</p> <p><input type="checkbox"/> Device lost/stolen (encrypted)</p> <p><input type="checkbox"/> Device lost/stolen (unencrypted)</p> <p><input type="checkbox"/> Paper lost/stolen</p> <p><input type="checkbox"/> Disclosure (unauthorised)</p> <p><input type="checkbox"/> Inappropriate disposal of paper</p> <p><input type="checkbox"/> Hacking</p> <p><input type="checkbox"/> Malware</p> <p><input type="checkbox"/> Phishing</p> <p><input type="checkbox"/> E-Waste personal data present on obsolete device</p> <p><input type="checkbox"/> Unintended online publication</p>	<p>What identifying details relating to individuals were disclosed (select all that apply)?</p> <p><input type="checkbox"/> Data subject identity (name, surname, birth date)</p> <p><input type="checkbox"/> PPSN (or other national identification number)</p> <p><input type="checkbox"/> Contact details</p> <p><input type="checkbox"/> Identification data (passports, licence data etc.)</p> <p><input type="checkbox"/> Economic or financial data</p> <p><input type="checkbox"/> Location Data</p> <p><input type="checkbox"/> Criminal convictions, offences or security measures</p>
<p>Were Special Categories of Data Involved?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If 'Yes' is selected above, what types of special categories of data were involved (select all that apply)?</p> <p><input type="checkbox"/> Data revealing racial or ethnic origin</p> <p><input type="checkbox"/> Political opinions</p> <p><input type="checkbox"/> Religious or philosophical beliefs</p> <p><input type="checkbox"/> Trade union membership</p> <p><input type="checkbox"/> Sex life data</p> <p><input type="checkbox"/> Health data</p> <p><input type="checkbox"/> Genetic data</p> <p><input type="checkbox"/> Biometric data</p>	
<p>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.).</p>	
<p>Number of Individuals Involved?</p> <div style="border: 1px solid black; width: 100px; height: 20px; margin: 5px auto;"></div>	<p>Number of records lost, stolen or accidentally disclosed?</p> <div style="border: 1px solid black; width: 100px; height: 20px; margin: 5px auto;"></div>
<p>Do you have a backup copy of the lost or stolen data records?</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	
<p>Were vulnerable individuals affected? (A vulnerable individual is a child or person who, by</p>	

reason of physical or mental incapacity, is unable to act on their own behalf) <input type="checkbox"/> Yes <input type="checkbox"/> No	
Were the affected Individuals notified? <input type="checkbox"/> Yes <input type="checkbox"/> No If not, what is the proposed procedure?	
<b>Section 4: Mobile Computing or Storage Device Details</b> (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? <input type="checkbox"/> Yes <input type="checkbox"/> No	If Yes, please include length of password  <div style="border: 1px solid black; width: 100px; height: 20px; margin: 0 auto;"></div>
Was the confidential or personal data stored on the mobile computer device encrypted? <input type="checkbox"/> Yes <input type="checkbox"/> No	What is the electronic format used to store the personal data on the mobile computer device? (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? <input type="checkbox"/> Yes <input type="checkbox"/> 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?	

**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:


## Contact Details

<p><b>Data Protection Officer (Corporate)</b> HSE, Dr. Steeven's Hospital, Steeven's Lane, Dublin 8.</p>	<p>Email: <a href="mailto:dpo@hse.ie">dpo@hse.ie</a> Phone: 01 6352478</p>
<p><b>Deputy Data Protection Officer West, (excluding voluntary agencies)</b> Consumer Affairs, Merlin Park University Hospital, Galway.</p> <ul style="list-style-type: none"> <li>• CHO 1 – Cavan, Donegal, Leitrim, Monaghan, Sligo</li> <li>• Community Healthcare West – Galway, Mayo, Roscommon</li> <li>• Mid-West Community Healthcare – Clare, Limerick, North Tipperary.</li> </ul> <p>Saolta Hospital Group</p>	<p>Email: <a href="mailto:ddpo.west@hse.ie">ddpo.west@hse.ie</a> Phone: 091-775 373</p>
<p><b>Deputy Data Protection Officer Dublin North-East (excluding voluntary hospitals and agencies)</b> Consumer Affairs, HSE Dublin North East, Bective St., Kells, Co Meath.</p> <ul style="list-style-type: none"> <li>• Midlands, Louth, Meath Community Health Organisation</li> <li>• Community Health Organisation Dublin North City &amp; County</li> <li>• CHO 6 – Dublin South East, Dublin South &amp; Wicklow</li> <li>• RCSI Hospital Group</li> </ul> <p>National Children's Hospital</p>	<p>Email: <a href="mailto:ddpo.dne@hse.ie">ddpo.dne@hse.ie</a> Phone: Kells Office: 046-9251265 Cavan Office: 049-4377343</p>
<p><b>Deputy Data Protection Officer Dublin mid-Leinster (excluding voluntary hospitals and agencies)</b> Consumer Affairs, HSE, Third Floor Scott Building, Midland Regional Hospital Campus, Arden Road, Tullamore, Co. Offaly.</p> <ul style="list-style-type: none"> <li>• Dublin Midlands Hospital Group</li> <li>• Ireland East Hospital Group</li> </ul> <p>Community Healthcare Dublin South, Kildare &amp; West Wicklow</p>	<p>Email: <a href="mailto:ddpo.dml@hse.ie">ddpo.dml@hse.ie</a> Phone: Tullamore Office: 057-9357876 Naas Office: 045-920105</p>
<p><b>Deputy Data Protection Officer South (excluding voluntary hospitals and agencies)</b> Consumer Affairs, HSE South, Ground Floor East, Model Business Park, Model Farm Road, Cork. Eircode: T12 HT02</p> <ul style="list-style-type: none"> <li>• Cork &amp; Kerry Community Healthcare</li> <li>• CHO 5 – Carlow, Kilkenny, South Tipperary, Waterford &amp; Wexford</li> <li>• UL Hospital Group</li> </ul> <p>South South-West Hospital Group</p>	<p>Email: <a href="mailto:ddpo.south@hse.ie">ddpo.south@hse.ie</a> Phone: Cork Office: 021 – 4928538 Kilkenny Office: 056 -7785598.</p>

**Incomplete or illegible reports will be returned to the sender**