

Data Security Breach – Incident Report

CONFIDENTIAL

The GDPR defines a “personal data breach” 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”.

Breach ID:

When did the breach take place?

Where did the breach take place?
e.g. Location of breach

When was the breach discovered?
e.g. Specific time & date

Who reported the breach?

Contact details of person who reported the breach?

Was the Data Protection Office immediately contacted?

Yes No

If YES, state by what means (e.g. phone, email etc.) and the time and date of the contact made?

If NO, was any other senior official e.g. CE, Director etc. contacted and if so, by what means (e.g. phone, email etc.) and the time and date of the contact made?

Were there any witnesses? If Yes, state Names & phone contact details

--

Please provide details of the breach:

What was the nature of the breach?
What categories of data subjects (e.g. students, adult learners, parents/guardians; other vulnerable groups, employees, board members; contractors etc.) were affected and/or potentially affected by the breach?
Approximate number of data subjects affected:
Categories of personal data/records (e.g. health data, education records, social care information, financial details, bank account numbers, passport numbers etc):
Approximate number of personal data records concerned:
Description of the likely consequences of the personal data breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy etc.):
Description of the measures undertaken (or proposed to be undertaken) by the ETB to address the breach (including, where appropriate, measures to mitigate its possible adverse effects):
Important note: where the exact details of any of the above are not yet known, this shall not delay a timely breach notification to the DPC. Further information can follow, when available: “<i>the information may be provided in phases without undue further delay</i>”¹.

¹ Article 33(4) GDPR.

Was the breached data protected through passwords, encryption etc.? Supply details below.

In your opinion, is the breach likely to be of a temporary nature? Can the personal information exposed be recovered?

Were any IT systems involved? (e.g. email, website, school admin system, VS Ware, Facility, apps). If so, please list them.

Is any additional material available e.g. error messages, screen shots, log files, CCTV footage?

Have you taken any action/steps so far to seek to stop/mitigate the risk either to the data subject/s who you think have been affected OR any other additional data subjects you consider may be affected? If YES, please describe below

**Have you spoken to someone in ETB management team at administrative head office level e.g. CE, Director, Head of IT etc?
If so, please advise whom you contacted, and a brief outline of the advice given by him/her.**

Have you made any contact with any external agencies e.g. Insurance Company, IT provider, Gardaí etc.? If YES, please describe below specifically whom you contacted and supply the name and contact details of same.

Any additional comments?

Signed:	
Your position in the ETB:	
Name of school, office, centre:	
Your contact number (ideally mobile number):	
Date:	
Time of completion:	

Thank you for your efforts in completing this form. The effort undertaken in its completion will help the ETB in its further investigation/analysis of the matter.

Please ensure this is forwarded directly to the ETB Data Protection Office

Data Protection Office, KCETB, Seville Lodge, Callan Road, Kilkenny

CONFIDENTIAL - THIS FORM HAS BEEN COMPLETED IN CONTEMPLATION OF LEGAL PROCEEDINGS

For your reference

Breaches can be categorised according to the following three well-known information security principles:

- (a) “Confidentiality breach” - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- (b) “Integrity breach” - where there is an unauthorised or accidental alteration of personal data.
- (c) “Availability breach” - where there is an accidental or unauthorised loss of access¹⁵ to, or destruction of, personal data.

Depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these. Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.


Incident Response DOs and DON'Ts for IT systems

DO'S

- immediately isolate the affected system to prevent further intrusion, release of data, damage etc.
- use the telephone to communicate. Attacker may be capable of monitoring e-mail traffic
- contact the ETB Data Protection Office without delay KCETB, Seville Lodge, Callan Road, Kilkenny
- preserve all pertinent logs, e.g. firewall, router and intrusion detection system.
- make back-up copies of damaged or altered files and keep these backups in a secure location.
- identify where the affected system resides within the network topology
- identify all systems and agencies that connect to the affected system
- identify the programs and processes that operate on the affected system(s), the impact of the disruption and the maximum allowable outage time.
- in the event the affected system is collected as evidence, make arrangements to provide for the continuity of services i.e. prepare redundant system and obtain data back-ups.

DON'Ts

- delete, move or alter files on the affected systems
- contact the suspected perpetrator
- conduct a forensic analysis.

For Breach Management Team Use Only	<i>Insert details in column below</i>
Details logged by:	
Data Protection Office Name:	
Time & date of receipt by ETB of this form	
Type of personal data breach e.g. <i>Confidentiality breach; integrity breach; availability breach (see examples)</i>	
Numbers of likely people affected by the breach	<i>Estimated number of data subjects affected?</i> <i>Types of data affected?</i>
Were special categories (e.g. sensitive personal data) compromised in the breach? <i>Special categories i.e.</i> <i>Racial or ethnic origin</i> <i>Political opinions</i> <i>Religious or philosophical beliefs</i> <i>Membership of a trade union</i> <i>biometric and genetic data,</i> <i>health</i> <i>sex life or sexual orientation.</i>	Yes <input type="checkbox"/> No <input type="checkbox"/> <i>Insert any relevant information below e.g. How many data subject(s) sensitive personal data has been affected?</i> <i>What type of sensitive personal data was breached?</i>
Severity of the breach <i>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.</i> Rate the breach opposite in terms of its likely severity on the rights and freedoms of affected or potentially affected data subject/s i.e. High Risk Medium Risk Low / No Risk* <i>* If it is assessed that there is “no risk”, the reasons for that decision must be recorded.</i>	

CE and or members of the senior management team to be notified	Yes <input type="checkbox"/> No <input type="checkbox"/>
IT Service Providers / IT support to be notified	Yes <input type="checkbox"/> No <input type="checkbox"/>
Insurance Company to be notified	Yes <input type="checkbox"/> No <input type="checkbox"/>
Gardaí to be notified	Yes <input type="checkbox"/> No <input type="checkbox"/>
Legal advisors to be notified (including LSSU as determined by ETB)	Yes <input type="checkbox"/> No <input type="checkbox"/>
Data Subjects to be notified? <i>How many?</i> <i>Is there a list of contact details for data subjects?</i> <i>If not, can we recover?</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Supervisory Authority to be notified? <i>Contact details for Supervisory Authority</i> Data Protection Commission Telephone: +353 57 8684800 +353 (0)761 104 800 Lo Call Number: 1890 252 231 Fax: +353 57 868 4757 E-mail: info@dataprotection.ie Postal: Data Protection Commission Canal House Station Road Portarlinton R32 AP23 Co. Laois	Yes <input type="checkbox"/> No <input type="checkbox"/> <i>If YES, list date and time of notification and any advice/instruction given by the Supervisory Authority:</i>
Any additional relevant additional details	
Signed by DATA PROTECTION OFFICE:	
Signed by CE / nominee:	
Date:	

CONFIDENTIAL - THIS FORM HAS BEEN COMPLETED IN CONTEMPLATION OF LEGAL PROCEEDINGS

Appendix 2 - Guidelines on Personal data breach notification under Regulation 2016/679

Source: [file:///C:/Users/d.keogh/Downloads/wp250rev01_enpdf%20\(2\).pdf](file:///C:/Users/d.keogh/Downloads/wp250rev01_enpdf%20(2).pdf)

Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However, if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber-attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, if the supervisory authority became aware of the

<p>that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.</p>			<p>incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.</p>
<p>v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else.</p> <p>The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.</p>	<p>Yes.</p>	<p>Only the individuals affected are notified if there is high risk and it is clear that others were not affected.</p>	<p>If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.</p>
<p>vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.</p>	<p>Yes, report to lead supervisory authority if involves cross border processing.</p>	<p>Yes, as could lead to high risk.</p>	<p>The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk.</p> <p>The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.</p>
<p>vii. A website hosting company acting as a data processor identifies an error in the code which controls user authorisation. The effect of the flaw means that any</p>	<p>As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay.</p> <p>Assuming that the website hosting company has</p>	<p>If there is likely no high risk to the individuals they do not need to be notified.</p>	<p>The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider).</p> <p>If there is no evidence of this vulnerability being</p>

<p>user can access the account details of any other user.</p>	<p>conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having “become aware” once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.</p>		<p>exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.</p>
<p>viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.</p>	<p>Yes, the hospital is obliged to notify as high-risk to patient’s well-being and privacy may occur.</p>	<p>Yes, report to the affected individuals.</p>	
<p>ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.</p>	<p>Yes, report to supervisory authority.</p>	<p>Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.</p>	
<p>x. A direct marketing e-mail is sent to recipients in the “to:” or “cc:” fields, thereby enabling each recipient to see the email address of other recipients.</p>	<p>Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).</p>	<p>Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.</p>	<p>Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.</p>