etb
Bord Oideachais agus Oiliúna
Mhaigh Eo, Shligigh agus Liatroma
*Mayo, Sligo and Leitrim*
*Education and Training Board*

| MAYO, SLIGO AND LEITRIM ETB POLICY NAME: |
|---|
| **Data Breach Protocol Policy** |

| POLICY CONTROL SHEET | | | |
|---|---|---|---|
| **Document reference number** | MSL-0002/2018 | **Document initiated by** | ETBI |
| **Revision number** | 001 | **Document drafted by** | ETBI (internally in MSLETB by Mary McDonald / Trevor Sweetman) |
| **Document reviewed by** | Corporate Services | **Document ratified by** | Policy noted by Board of MSLETB |
| **Date document ratified** | 07/06/18 | **Date document implemented** | 07/06/18 |
| **Assigned review period** | 3 Years | **Responsibility for implementation** | MSLETB |
| **Responsibility for review** | Corporate Services | **Next review date** | 1 year after implementation |
| **Original issued by** | ETBI | **Date of withdrawal of obsolete document** | Previous Data Breach Protocol policy withdrawn on 07/06/18 |
| **AMENDMENT HISTORY** | | | |
| **Date** | **Revision level** | **Details of amendment** | **Approval signature** |
| | | | |
| | | | |
| | | | |
| | | | |

etb
Bord Oideachais agus Oiliúna
Mhaigh Eo, Shligigh agus Liatroma
*Mayo, Sligo and Leitrim*
*Education and Training Board*

# DATA BREACH PROTOCOL POLICY

## Contents

## 1. Data Breach and Purpose of Protocol

1.1. **Focus**

Mayo, Sligo and Leitrim Education & Training Board has developed this personal data breach protocol. This is part of our strategic planning to ensure that Mayo, Sligo and Leitrim ETB is prepared to respond in a personal data breach situation. The focus of any breach response plan will be on prompt action in order to protect individuals and their personal data. Mayo, Sligo and Leitrim ETB is committed to:

(a) Notifying the Data Protection Commission (DPC) of a personal data breach without undue delay and not later than **72 hours** after becoming aware of it (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons).

(b) Notifying affected data subjects without undue delay, unless the personal data breach is unlikely to result in a high risk to the rights and freedoms of natural persons.

1.2. **Dissemination**

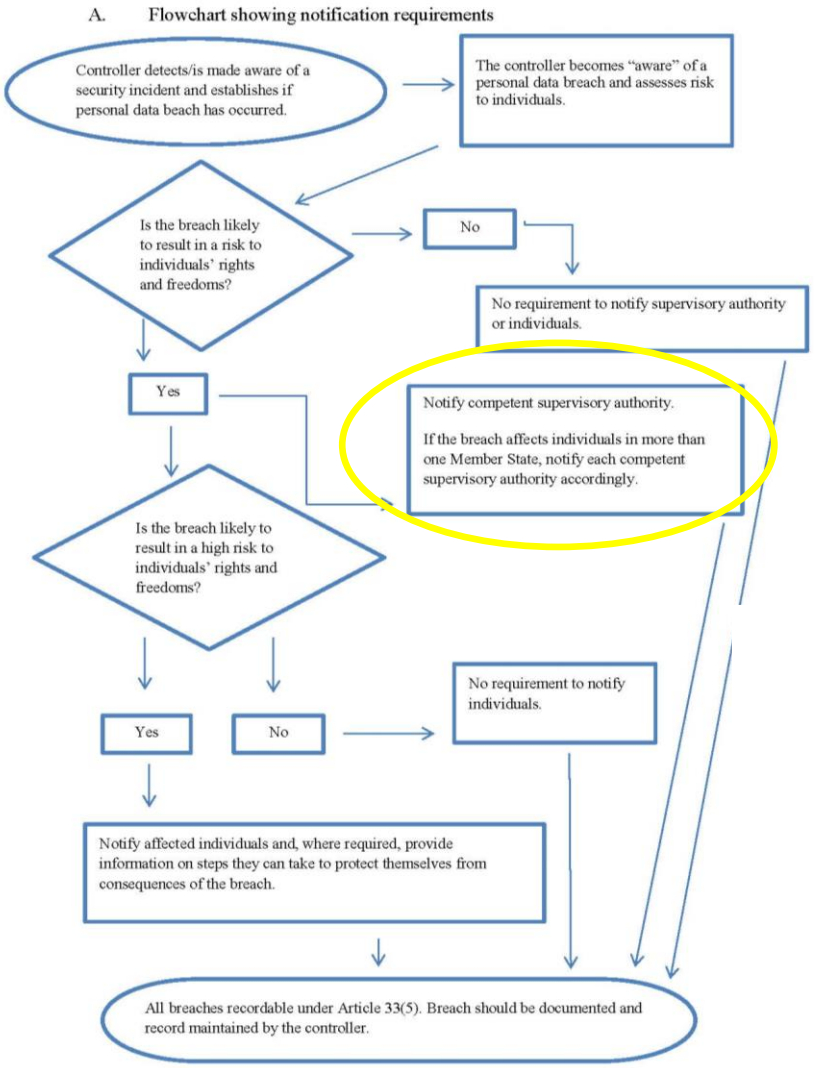
This protocol will be:

(a) circulated to all appropriate data processors. Data processors are required to alert the ETB immediately if the processor becomes aware of a breach of the personal data it is processing on behalf of the ETB

(b) advised to staff at induction and at periodic staff meetings/ training.

1.3. **Summary of steps to be taken**

The following flow-chart (taken from the Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017) summarises the steps to be taken:




1.4. **Definitions**

In this protocol, the following terms shall have the following meanings[1]:

1.4.1. "**Aware**": a data controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

1.4.2. "**Damage**": the personal data has been altered, corrupted, or is no longer complete.

1.4.3. "**Destruction**": the data no longer exist or no longer exist in a form that is of any use to the controller.

1.4.4. "**Loss**": the data may still exist but the controller has lost control or access to the data, or no longer has the data in its possession.

[1] Definitions taken from GDPR and WP250 ("Guidelines on Personal data breach notification under Regulation 2016/679).

1.4.5. "**personal data breach**": per Article 4(12) GDPR: "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".

1.4.6. "**Temporary loss of data**": an incident resulting in personal data being made unavailable for a period of time.

1.4.7. "**unauthorised or unlawful processing**" may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

1.5. **Reasons for breaches**

A data security breach can happen for a number of reasons, including:

- Human error.
- Loss or theft of paperwork, or any device containing data.
- Break-ins, burglary, mugging.
- Inappropriate access controls allowing unauthorised use/access.
- Equipment failure and inadequate system back-ups.
- A disaster such as flood or fire.
- Phishing or blagging (where information is obtained by deception or spoofing).
- Malicious attacks such as hacking or ransomware attack.

1.6. **Effects of breaches on individuals**

Personal data breaches can result in adverse effects on individuals which can result in physical, material, or non-material damage. This could include causing the data subject embarrassment, distress, or humiliation. Other adverse effect could include: "*loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, significant economic or social disadvantage*[2]*"* to affected individuals.

1.7. **Effects of breaches on the ETB**

Personal data breaches can also be damaging to the ETB as they can result in:

- Damage to the relationship of trust we have built with staff and students,
- Loss of, deletion of, or damage to personal data which is essential to the administration of the ETB,
- Damage to the reputation of Mayo, Sligo and Leitrim ETB
- Administrative fines in accordance with the provisions of Data Protection legislation, enforcement action, and/or litigation.

[2] Page 8, WP250.

## 2. Protocol

In case of a personal data breach, Mayo, Sligo and Leitrim ETB will follow the following protocol:

2.1. **Identify that there is an issue and alert the relevant people**

2.1.1. The Data Protection Officer (DPO[3]) shall be notified as soon as possible.

2.1.2. The DPO shall notify the Chief Executive as soon as possible.

> **Emergency contact numbers:**
> The interim Data Protection Officer (DPO) is Orla Reilly, Head of Corporate Services who can be contacted on 086 6069408 or 094 9024188. If you have any queries, please consult our Data Protection Policy (available at www.mayosligoleitrim.etb.ie/policies-procedures) or contact our DPO.

2.1.3. The DPO shall gather together a small team to assess the potential exposure/loss and undertake appropriate containment/mitigation/remediation measures. All staff and all data processors and/or joint data controllers are required to give all necessary assistance to the DPO and this team.

2.1.4. The DPO shall start a written chronology of events, recording all relevant matters, including:

(a) Date and time of notification of the breach (using the format DD/MM/YYYY and am/pm as appropriate).
(b) If the notification relates to a potential breach, details of any preliminary investigation (if required) in order to establish whether or not a breach has in fact occurred.
(c) Details of who reported the matter.
(d) Details of what was known/suspected at that initial stage.
(e) Details of what system/data-set is involved.
(f) Assessment of risk to the rights and freedoms of natural persons.
(g) Immediate actions undertaken (investigation, containment, mitigation, recovery, etc).
(h) Details of the team gathered to assist.
(i) Details of the tasks allocated to each team member.
(j) At the same time as (g), notification to DPC within 72 hours after having become aware.
(k) Notification to the affected individuals (if required) without undue delay

2.1.5. Regardless of whether (or not) a decision is made to notify the DPC, all documentation relating to documenting a (potential/reported/suspected) personal data breach including but not limited to the documentation required by Article 33(5) GDPR shall be stored on the ETB Risks Register.

[3] DPO appointed on an interim basis

2.2. **Containment, mitigation, and recovery**

2.2.1. Mayo, Sligo and Leitrim ETB will immediately seek to contain the matter (insofar as that is possible) and shall take all necessary steps to mitigate any further exposure of the personal data held.

2.2.2. Where the data breach relates to an IT system and/or electronic data, contact shall be immediately made with the data processor responsible for IT support in Mayo, Sligo and Leitrim ETB. Their advices and assistance should be sought in relation to appropriate measures of containment, quarantine, preservation of data and logs etc.

2.2.3. Depending on the nature of the breach/threat to the personal data, this may involve:

(a) a quarantine of some or all PCs, networks etc.
(b) directing staff not to access PCs, networks, devices etc.
(c) suspending accounts,
(d) audit of the records held on backup server/s,
(e) ascertain the nature of what personal data may potentially have been exposed.

2.2.4. Consider a quarantine of manual records storage area/s and other areas as may be appropriate.

2.2.5. In appropriate cases, immediate consideration should be given to retaining an IT forensics specialist and obtaining legal advice.

2.3. **Assess Risk**

2.3.1. The ETB shall undertake an assessment in relation to the risk: is the personal data breach likely to result in a risk to the rights and freedoms of natural persons?

2.3.2. Classification of that risk:

- No risk?
- Risk?
- High risk?

If it is assessed that there is "no risk", the reasons for that decision must be recorded.

2.3.3. When assessing risk, the ETB shall have due regard to the sensitivity of the data and the category of the data subject (e.g. child, vulnerable person) in order to ascertain whether they may be placed at greater risk because of the breach.

2.3.4. The ETB may not be required to notify the DPC and data subjects if the breach is unlikely to result in a risk to their rights and freedoms, e.g. the data were securely encrypted with state-of-the-art encryption, and the key was not compromised in any security breach.

2.3.5. Mayo, Sligo and Leitrim ETB shall have regard to the recommendations made by the European Union Agency for Network and Information Services (ENISA) for a methodology in assessing the severity of a breach[4].

2.3.6. If a decision is taken not to notify the DPC and/or affected data subjects, the justifications for that decision will be documented and stored on the ETB Risks Register.

## 2.4. Notification

2.4.1. **Reporting of incidents to the Data Protection Commissioner ("DPC")**: All incidents in which personal data and sensitive personal data has been put at risk shall be reported to the Data Protection Commission without undue delay and where feasible, not later than **72 hours** after having become aware of it unless it does not result in a risk to the rights and freedoms of data subjects.

| **DPC Contact details** | |
|---|---|
| Telephone: | 0761 104 800 |
| Lo Call Number: | 1890 252 231 |
| E-mail: | info@dataprotection.ie |
| Address: | Data Protection Commission<br>Canal House, Station Road, Portarlington<br>R32 AP23<br>Co. Laois |

2.4.2. At a minimum, the initial notification to the DPC shall contain the following:

- The nature of the personal data breach.
- The categories of data subjects (e.g. children, other vulnerable groups, people with disabilities, employees, customers).
- 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.
- Name and contact details of the DPO (from where more information can be obtained).
- 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

[4] Available at www.enisa.europa.eu/publications/dbn-severity

can follow, when available: "*the information may be provided in phases without undue further delay*[5]".

2.4.3 If the controller chooses to only notify the Data Protection Commission, it is recommended that the controller indicates, where appropriate, whether the breach involves establishments located in other Member States.

2.4.4 **Purpose of DPC notification**:

(a) **Avoid an Administrative fine**: Failure to notify the Data Protection Commission as required under the Data Protection Act 2018 may result in an administrative fine.

(b) **Advices**: so that the ETB can obtain advices from the DPC, and to ensure that the ETB's decisions about notifying (or deciding not to notify) affected data subjects can be justified.

2.4.5 **Notifying affected data subjects**

Following the risk-assessment conducted at 2.4.2, if the personal data breach is likely to result in a "high risk" to the rights and freedoms of natural persons, the ETB shall:

(a) Contact the individuals concerned (whether by phone/email etc) without undue delay.
(b) Advise that a data breach has occurred.
(c) Provide the data subjects with the detail outlined at 2.5.2 above.
(d) Where appropriate, provide specific advices so that the data subjects can protect themselves from possible adverse consequences of the breach (such as re-setting passwords).

2.4.6 The communication to the data subject shall not be required if any of the following conditions are met:

(a) the ETB has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the ETB has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

2.4.7 **An Garda Síochána**:

[5] Article 33(4) GDPR.

(a) Where data has otherwise been accessed without authority, the matter shall be reported immediately to An Garda Síochána.

(b) Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, further assistance should be sought from An Garda Síochána.

(c) Where data has been "damaged" (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself ("withholding information") pursuant to section 19 Criminal Justice Act, 2011. The penalties for withholding information include a fine of up to €5,000 or 12 months' imprisonment on summary conviction.

2.4.8 **Other bodies**: Where appropriate, contact may be made with other bodies such as the HSE, TUSLA, financial institutions, ETBI etc. (depending upon the nature of the data put at risk, e.g. if it contains sensitive information relating to children or vulnerable persons, such as child protection or safeguarding matters).

2.4.9 **Insurance company**: Mayo, Sligo and Leitrim ETB shall notify the insurance company with which the organisation is insured and advise them that there has been a personal data security breach.

2.5. **ETB Legal Advisors, including as appropriate, the Legal Services Support Unit, Education and Training Boards Ireland**

Mayo, Sligo and Leitrim ETB may notify its legal advisors and advise them that there has been a personal data security breach for the purposes of obtaining legal advices and defending, compromising or otherwise settling litigation.

2.6. **Post-event**

After the initial response measures have been addressed, a full review should be undertaken in a timely manner. These should include the following:

2.6.1 Review of the breach record per Article 33(5) – document maintained by the ETB in its Risk Register.

2.6.2 Details of learning outcomes, improvements, and safeguards should be identified.

2.6.3 The ETB board shall receive an appropriate briefing from the DPO (and/or such other external experts as may be retained to assist), and a copy of any investigation reports and any correspondence exchanged with the DPC and/or affected data subjects.

2.6.4 The ETB will give careful consideration to whether disciplinary procedures should be initiated, if relevant.

2.6.5 Where remedial actions are necessary, responsibility shall be allocated to individual(s): they shall be allocated responsibility for ensuring certain actions are completed within defined timeframes.

2.6.6 Staff should be apprised of any changes to this protocol and of upgraded security measures. Staff should receive refresher training where necessary.

# Appendix 1 - 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".

*(Please refer to **NOTES FOR PERSON COMPLETING DATA SECURITY BREACH INCIDENT FORM** on page 17 for reference.)*

| **BASIC DETAILS OF BREACH** | |
|---|---|
| **Breach ID** | |
| **When did the breach take place?** | |
| **Where did the breach take place?**<br>**(e.g. location of breach)** | |
| **When was the breach discovered?**<br>**(e.g. specific time and date)** | |
| **Who reported the breach?** | |
| **Contact details of person who reported the breach?** | |
| **Was the Data Protection Officer immediately contacted?** | |
| 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?**<br>**If Yes, state names & phone contact details** | |

| Please provide details of the breach:[6] |
| --- |
| **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:** |
| |

[6] **<u>Important note:</u> 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: "the information may be provided in phases without undue further delay".**

| **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):** |
| |
| **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 <u>OR</u> 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?**<br>**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 Mayo, Sligo and Leitrim 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 Mayo, Sligo and Leitrim ETB in its further investigation/analysis of the matter.

Please ensure this is forwarded directly to MSL ETB Data Protection Officer

The interim Data Protection Officer (DPO) is the Head of Corporate Services who can be contacted on 094 9024188. If you have any queries, please consult our Data Protection Policy (available at www.mayosligoleitrim.etb.ie/policies-procedures) or contact our DPO.

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

## NOTES FOR PERSON COMPLETING DATA SECURITY BREACH INCIDENT FORM

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 access 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 Officer without delay on 094 9024188
- 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 | |
|---|---|
| **Details logged by:** | |
| **DPO Name:** | |
| **Time & date of receipt by MSLETB of this form:** | |
| **Type of personal data breach**<br>*E.g. Confidentiality breach; integrity breach; availability breach (see examples)* | |
| **Numbers of likely people affected by the breach:**<br>*Estimated number of data subjects affected?*<br>*Types of data affected?* | |
| **Were special categories (e.g. sensitive personal data) compromised in the breach?**<br>Special categories i.e.<br>- Racial or ethnic origin<br>- Political opinions<br>- Religious or philosophical beliefs<br>- Membership of a trade union<br>- Biometric and genetic data<br>- health<br>- Sex life or sexual orientation. | **Yes** ☐ **No** ☐<br>*Insert any relevant information below e.g. How many data subject(s) sensitive personal data has been affected?*<br>*What type of sensitive personal data was breached?* |
| **Severity of the breach**<br>*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.*<br>**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.**<br>**High Risk**<br>**Medium Risk**<br>**Low / No Risk***<br>*** If it is assessed that there is "no risk", the reasons for that decision must be recorded.** |  <br>  <br>  |

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

## Appendix 2 - Examples of Personal Data Breaches and Who To Notify

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

### Guidelines on Personal Data Breach Notification Under Regulation 2016/679

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.<br><br>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.**<br><br>**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).<br><br>Appropriate records should be maintained by the controller. |
| **iv. A controller suffers a** | Yes, report to | Yes, report to | If there was a backup |

| Example | Notify the supervisory authority? | Notify the data subject? | Notes/recommendations |
|---|---|---|---|
| **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 that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.** | the supervisory authority, if there are likely consequences to individuals as this is a loss of availability. | 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. | 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.<br><br>However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32. |
| **v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else.**<br><br>**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.** | Yes. | Only the individuals affected are notified if there is high risk and it is clear that others were not affected. | 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. |
| **vi. A controller operates an** | Yes, report to | Yes, as could lead to | The controller should |

| Example | Notify the supervisory authority? | Notify the data subject? | Notes/recommendations |
|---|---|---|---|
| **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.** | lead supervisory authority if involves cross border processing. | high risk. | take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk.<br><br>The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider. |
| **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 user can access the account details of any other user.** | As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay.<br><br>Assuming that the website hosting company has 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 | If there is likely no high risk to the individuals they do not need to be notified. | The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider).<br><br>If there is no evidence of this vulnerability being 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. |

| Example | Notify the supervisory authority? | Notify the data subject? | Notes/recommendations |
|---|---|---|---|
| | processor). The controller then must notify the supervisory authority. | | |
| viii. **Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.** | Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur. | Yes, report to the affected individuals. | |
| ix. **Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.** | Yes, report to supervisory authority. | Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences. | |
| 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.** | 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). | Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences. | Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed. |