



cetb

Bord Oideachais agus
Oiliúna Chorcaí
*Cork Education and
Training Board*

Document:	Data Breach Protocol
Procedure No:	2020 v 1.0
Effective Date:	20 July 2020
Supersedes:	14 May 2018
Issued By:	Data Protection Officer
Review Date:	June 2021



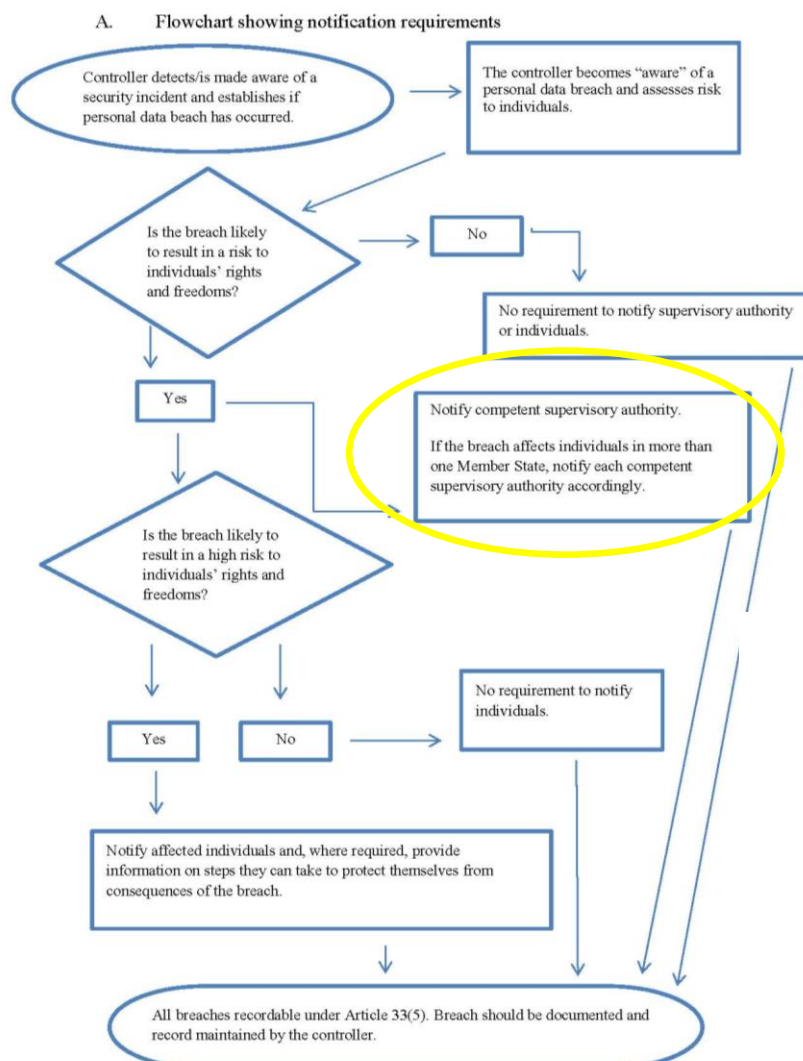
cetb
Bord Oideachais agus
Oiliúna Chorcaí
*Cork Education and
Training Board*

Data Breach Protocol

Version number	v.1.0
Policy drafted by	ETBI FOI/DP Forum
Approved by ETB Executive on	14 May 2018
Date on which it became operational	25 May 2018
Next review date	May 2019

1. Data Breach and Purpose of Protocol

- 1.1. Cork Education and Training Board (CETB) has developed this personal data breach protocol, as part of our strategic planning, to ensure that CETB 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. CETB 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. This protocol will be:
- (a) circulated to all appropriate data processors. Data processors are required to alert CETB immediately if the processor becomes aware of a breach of the personal data it is processing on behalf of CETB
 - (b) advised to staff at induction and at periodic staff meetings/ training.
- 1.3. 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 meanings¹:

- 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.
- 1.4.5. **“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. 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. 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 disadvantage²”* to affected individuals.

1.7. Personal data breaches can also be damaging to CETB 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 CETB;
- Damage to the reputation of CETB; and/or
- Administrative fines in accordance with the provisions of Data Protection legislation, enforcement action, and/or litigation.

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

² Page 8, WP250.

2. Protocol

In case of a personal data breach, CETB 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), 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 Data Protection Officer (DPO) for Cork ETB is **Sarah Flynn** and she may be contacted at dataprotection@corketb.ie or by telephone on **021/4907100**.

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 (see Incident Report Form at Appendix 1):

- (a) Date and time of notification of the breach.
- (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 CETB's Risk Register.

2.2. Containment, Mitigation, and Recovery

2.2.1. CETB 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 CETB. 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) auditing of the records held on backup server(s).
- (e) ascertaining 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. CETB 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, CETB shall have due regard to the sensitivity of the data and the category of the data subject (eg. child, vulnerable person) in order to ascertain whether they may be placed at greater risk because of the breach.

2.3.4. CETB 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, eg. the data were securely encrypted with state-of-the-art encryption and the key was not compromised in any security breach.

2.3.5. CETB 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 breach³.

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 CETB's Risk Register.

2.4. Notification

2.4.1. **Reporting of incidents to the Data Protection Commission (“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 affected.

DPC Contact details

Telephone: 0761 104 800
Lo Call Number: 1890 252 231
E-mail: info@dataprotection.ie
Address: Data Protection Commission
Canal House, Station Road, Portarlinton
R32 AP23
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 (eg. children, other vulnerable groups, people with disabilities, employees, customers).
- Approximate number of data subjects affected.
- Categories of personal data/records (eg. 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 (eg. identity theft, fraud, financial loss, threat to professional secrecy, etc).
- Description of the measures undertaken (or proposed to be undertaken) by CETB to address the breach (including, where appropriate, measures to mitigate its

³ Available at www.enisa.europa.eu/publications/dbn-severity

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: *“the information may be provided in phases without undue further delay⁴”*.

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) **To 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 CETB can obtain advices from the DPC and to ensure that CETB'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, CETB 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 2.4.2 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) CETB 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) CETB has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; and/or
- (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:**

- (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, eg. 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 S.19 of the Criminal Justice Act 2011. The penalties for withholding information include a fine of up to €5,000 or 12-months’ imprisonment on summary conviction.

⁴ Article 33(4) GDPR.

- 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, eg. if it contains sensitive information relating to children or vulnerable persons, such as child protection or safeguarding matters).
- 2.4.9 **Insurance Company:** CETB 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 of ETBI:** CETB 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 CETB in its Risk Register.
 - 2.6.2 Details of learning outcomes, improvements, and safeguards should be identified.
 - 2.6.3 CETB 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 CETB 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) for ensuring certain actions are completed within the 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.

Further Information

The Incident Report Form at Appendix 1 should be completed in respect of all data breaches or suspected data breaches.



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”.

All sections of this Incident Report must be completed.

Breach ID:

**When did the breach take place?
(where necessary an estimate can be made)**

e.g. Specific time & date

Have you estimated the details above?

Yes **No**

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 Officer 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 eg. CE, Director, etc. contacted and, if so, by what means (eg. phone, email etc.) and the time and date of the contact made?

--

Were there any witnesses? If Yes, state Names and Phone Contact Details

--

Please provide details of the breach:

How were you made aware of the breach?

--

What was the nature of the breach?

--

Please describe how the breach occurred.

--

Please advise the cause of the breach. *(eg Device/file lost or misplaced, employee error or omission, inappropriate access controls)*

--

Is the breach ongoing?

--

Date the breach ended.

What immediate actions did you take to minimise the impact of the breach?

What identifying details relating to individuals were disclosed (select all that apply)?

- Data Subject identity (name, surname, date of birth)
- PPSN (or other national identification number)
- Contact details (Address, Telephone number, Email address)
- Identification data (passports, licence data etc.)
- Economic or financial data
- Location data
- Criminal convictions, offences or security measures

Please insert any other details relating to individuals that were disclosed (beyond those categories listed above).

Were Special Categories of Personal data involved?

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 insert the number of affected individuals (where necessary estimates can be made):

Please insert the number of data records involved (where necessary estimates can be made).

(The number of records refers to each item of personal data that was disclosed):

Are data subjects in other member states likely to be affected?

Were vulnerable individuals affected? *(A vulnerable individual is a child or a person who, by reason of physical or mental incapacity, is unable to act on their own behalf).*

Does the breach involve personal data maintained for the prevention, detection, investigation, prosecution of criminal offences or the execution of criminal penalties in the State?

Please describe the relevant technical/organisational measures that were in place prior to the breach.

What deficiencies in these technical/organisational measures have been identified as a result of this breach?

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: “the information may be provided in phases without undue further delay⁵”.

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? (eg. email, website, student administration systems eg. VShare, PLSS, MIT, etc. If so, please list them.

⁵ Article 33(4) GDPR.

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

What measures have you taken / do you propose to take to (a) address the breach or (b) to mitigate the adverse effects?

Are the mitigating measures fully implemented?

Please provide further details in the event mitigating actions have not been fully implemented.

In your view what are the potential consequences of the breach for the affected individuals (select all that apply)?

- Loss of control of their personal data**
- Limitation of their rights**
- Discrimination**
- Identity theft**
- Fraud**
- Financial loss**
- Unauthorised reversal of pseudonymisation**
- Damage to reputation**
- Loss of confidentiality of personal data protected by professional secrecy**
- Other**

Where "Other" is selected above, please provide further details.

Have you secured/retrieved the breached personal data? Please provide details of how you have done so.

In the event you have not secured/retrieved the breached personal data, please outline why not below. In the event this breach involved an unauthorised disclosure, please confirm you have retrieved the data and/or received confirmation of its destruction.

Have you notified the affected individuals of the breach?

When will the affected individuals be notified?

How many affected individuals were informed?

How were the affected individuals informed?

Please outline the reasons for using this channel.

What information was communicated to the affected individuals? In particular, please indicate if you have related to affected individuals the steps they may take to mitigate any adverse consequences which have been caused or could be caused to them by this breach.

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

Have you made contact with any external agencies eg. 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 CETB:	
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 CETB in its further investigation/analysis of the matter.

Please ensure the completed form is sent directly to CETB Data Protection Office at:

dataprotection@corketb.ie.

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

For Breach Management Team Use Only	<i>Insert details in column below</i>
Details logged by:	
Data Protection Officer (DPO):	
Time & date of receipt by CETB 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? 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? 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* * If it is assessed that there is “no risk”, the reasons for that decision must be recorded.	  

Please provide risk assessment and scoring methodology for the breach (ENISA).	
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 Officer (DPO):	
Signed by CE / nominee:	
Date:	

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

Further Information and Guidance

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

DOs

- immediately isolate the affected system to prevent further intrusion, release of data, damage etc.
- use the telephone to communicate. The attacker may be capable of monitoring email traffic.
- contact the CETB Data Protection Office without delay at 021/4273377.
- preserve all pertinent logs, e.g. firewall, router and intrusion detection systems.
- 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; and
- in the event that the affected system is collected as evidence, make arrangements to provide for the continuity of services ie. prepare redundant system(s) and obtain data back-ups.

DON'Ts

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

Guidelines on Personal Data Breach Notification under Regulation 2016/679

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	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

<p>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.</p>			<p>became aware of the 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</p>	<p>As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay.</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>controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.</p>	<p>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 processor). The controller then must notify the supervisory authority.</p>		<p>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.</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>