

Breach Management Policy and Procedure

Document Title	Breach Management Policy and Procedure
Document Number	DP-Pol-083
Version	2.0
Department	Compliance and Risk
Owner/Responsible for Implementation	Manager, Compliance and Risk
Approving Body	Executive Board
Effective Date:	June 2022
Last Review Date:	October 2025
Next Review Date:	June 2028
Related Documents	DP-Pol-089 – Records Management Policy DP-Pol-090 – Data Protection Policy ED-Pol-088 – Programme Information & Data Management Policy DP-T-082 – Subject Access Request Assessment Template

Breach Management Policy and Procedure

Contents

<i>1. What is a Personal Data Breach?</i>	<i>3</i>
<i>2. RCPI's Commitment to the Prevention of Personal Data Breaches?</i>	<i>4</i>
<i>3. What must I do in the event of a Personal Data Breach?</i>	<i>4</i>
<i>4. How do I assess the extent of the consequences of the Personal Data Breach?</i>	<i>5</i>
<i>5. Do I need to notify the Data Protection Commissioner?.....</i>	<i>7</i>
<i>6. Do I need to communicate the breach to the Data Subjects?</i>	<i>7</i>
<i>7. How do I close out the Personal Data Breach?</i>	<i>8</i>
<i>8. Useful Links</i>	<i>9</i>
<i>Appendix 1 – WP29 Examples of Personal Data Breaches and Reporting Requirements.....</i>	<i>10</i>

Breach Management Policy and Procedure

1. What is a Personal Data Breach

A 'personal data breach' means that there has been accidental or unlawful access or disclosure, loss, damage, destruction or alteration of any information that could be used to identify an individual.

Such mishandling of personal data at any stage of the data processing is a personal data breach. Processing in this regard includes collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, transmission, dissemination, combination, restriction, erasure or destruction.

Any Personal Data Breach impinges on an individual's right to privacy.

Important

Any Personal Data Breach impinges on an individual's right to privacy. All Personal Data Breaches and near misses must be logged internally no matter how minor they may appear.

The benefit to RCPI of reporting minor breaches and near misses is that it helps mitigate and prevent more serious privacy issues.

2. RCPI's Commitment to the Prevention of Personal Data Breaches?

- 2.1 RCPI ensures, in accordance DP-Pol-090 – Data Protection Policy, that the appropriate technical and organisation measures are in place to protect personal data from unlawful or unauthorised processing and accidental loss, destruction or damage.
- 2.2 RCPI ensures that the appropriate contractual arrangements are in place with any processors/joint controllers used by RCPI to ensure that a breach is reported and RCPI is therefore in a position to comply with its obligations. (Processors must report a suspected breach immediately and co-operate with RCPI during the investigation, verification, resolutions and reporting of the breach within 72 hours).
- 2.3 RCPI ensures that, in the event of a data breach, a root cause analysis is carried out with a view to implementing effective preventative measures.
- 2.4 RCPI ensures that, in the event of a data breach, proportionate communication/training is issued to all staff with a view to preventing recurrence of the issue.

Breach Management Policy and Procedure

3. What must I do in the event of a Personal Data Breach?

Important

You must act without delay so that where possible, the breach can be shut down and where necessary, the DPC is informed within the required 72-hour deadline. This deadline applies from when a breach is suspected (not from when it is confirmed) and it applies regardless of weekends or national holidays.

- 3.1 Inform the Data Protection Officer if you have any concern that there may have been a data security incident of any kind (not just a confirmed Personal Data Breach).
- 3.2 Once there is a reasonable degree of certainty that a Personal Data Breach of any kind has occurred, RCPI must act promptly to contain the breach, recover the data if possible, notify the regulator and, where appropriate communicate with the affected data subjects.
- 3.3 While it is reasonable to undertake a short period of investigation to confirm if there has been a Personal Data Breach, acting upon breach must not be delayed. Where appropriate, the regulator must be informed within 72 hours and the data subjects may need to be informed of the steps they can take to protect themselves from the consequences of the breach.
- 3.4 The Data Protection Commission considers an organisation to be aware of a Personal Data Breach once there is a reasonable degree of certainty that an incident has occurred and expects to be informed within 72 hours. Failure to do so can result in sanctions or fines for RCPI.
- 3.5 There is no penalty for reporting a Personal Data Breach and later withdrawing the notification e.g. if an encrypted USB stick with critical information was misplaced and then found and there were no consequences of the temporary loss for the data subject.

4. How do I assess the extent of the consequences of the Personal Data Breach?

- 4.1 Immediately that a Personal Data Breach has been confirmed, a risk assessment must be carried out. The value of completing the assessment is that knowing the extent of the risk to the individuals will help RCPI to take effective steps to contain the breach and to determine if the regulator and the data subjects need to be informed.

Important

The primary consideration during the risk assessment is the protection of the privacy of the individual.

- 4.2 Convene a meeting of the appropriate people to assess the extent of the breach. You should include the DPO, the Department Manager, IT and Helpdesk.

Breach Management Policy and Procedure

4.3 Consider the following criteria of risk, assessing the likelihood and severity of adverse effects of the breach for the data subjects

- **Type of breach:**
 - Personal Data Breaches can be broadly described in three categories

Confidentiality	– unauthorised or accidental disclosure of personal data
Integrity breach	– unauthorised or accidental alteration of personal data
Availability breach	– unauthorised or accidental loss of access to personal data
- **The number of affected individuals:**
 - As a rule of thumb, the higher the number affected the higher the risk. Although, a breach of one person's data could have equally significant consequences.
- **Special characteristics of the individual:**
 - Are the data-subjects children or vulnerable individuals?
- **The nature, sensitivity and volume of personal data:**
 - The more data about an individual that is breached the more the risk to the individual.
 - Moreover, the combination of data that is mishandled could make the Personal Data Breach more high risk e.g. a customer home delivery list could reveal who has asked for their deliveries to be stopped for two weeks.
- **Ease of identification of individuals:**
 - How easy will it be for the data subjects to be identified by the mishandled?
 - Could this data be combined with other publicly available data to identify individuals?
 - Could the data subjects be identified either directly or indirectly by the breach?
- **Severity of consequences for the individual:**
 - How permanent is this breach?
 - What are the intentions of the party who may have had unauthorised disclosure of Personal Data to them? Has a system been hacked? Or, was the breach to a trusted organisation that can be trusted to follow instructions to contain or recover the data?
 - Are there risks to the rights and freedoms of individuals? According to the GDPR the risks are:
 - Discrimination
 - Identity theft or fraud
 - Financial loss
 - Damage to reputation
 - Loss of confidentiality of personal data protected by professional secrecy
 - Unauthorised reversal of pseudonymisation

Breach Management Policy and Procedure

- Any significant economic or social disadvantage
- Prevention of exercise of control over their personal data
- Revelation of racial / ethnic origin, political opinions, religious / philosophical beliefs, trade union membership, genetic data, data concerning health, data concerning sex life, criminal convictions / security measures
- **Analysis or prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements**
- **NB: If any of the personal data breached is Special Category Data, it must automatically be assumed that this breach is of high risk to the individual regardless of any other factors that may make the breach appear to be low risk. According to the GDPR special category data are:**
 - Race
 - Ethnic origin
 - Political opinions
 - Religious or philosophical beliefs
 - Trade union membership
 - Genetic data
 - Biometrics (where used for ID purposes)
 - Health data
 - Sex life
 - Sexual orientation

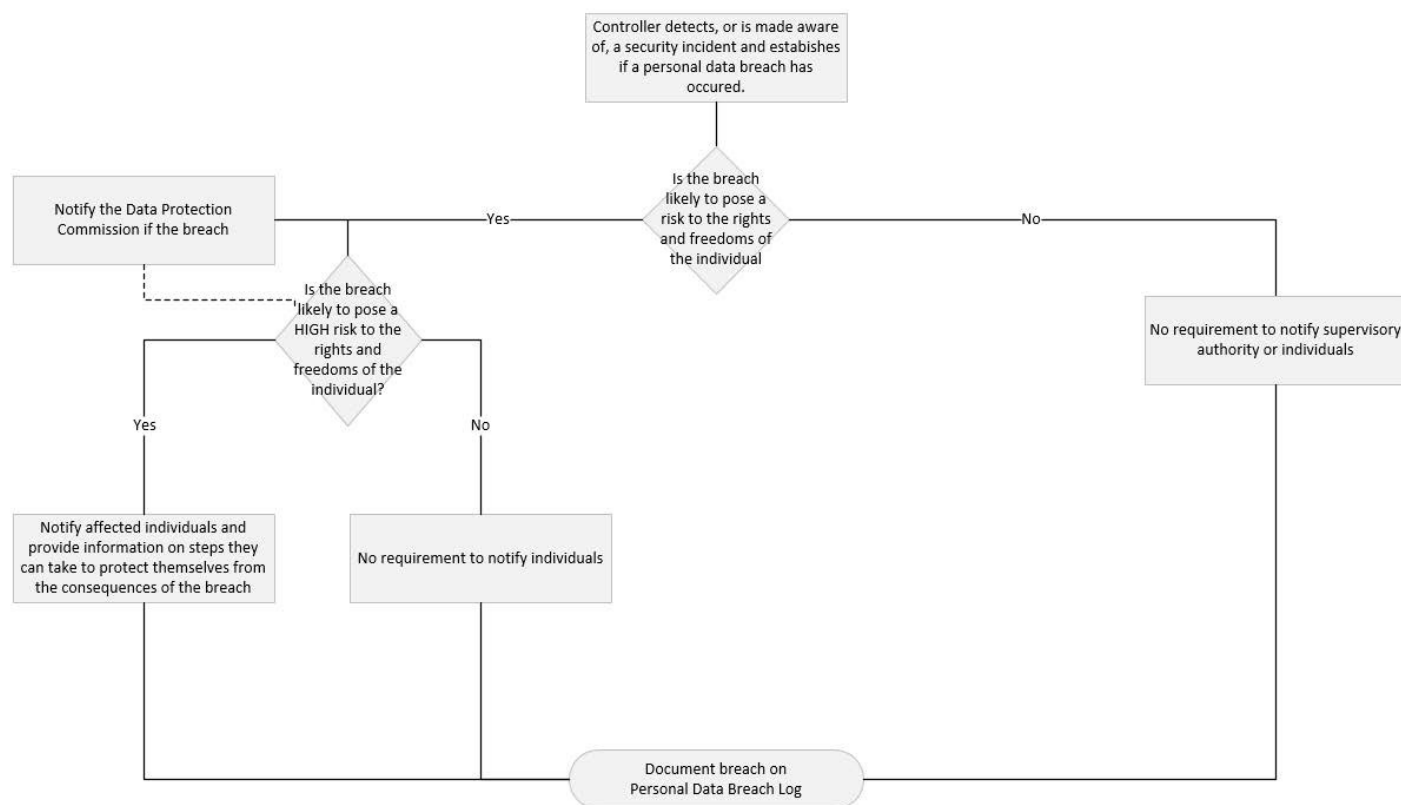
4.4 Where the likelihood of harm to the individual is low the breach may still, on consideration of all possible consequences, be reportable for other reasons.

5. Do I need to notify the Data Protection Commissioner?

- 5.1 If there is any risk whatsoever to the right to privacy of the individual, the breach must be reported to the Data Protection Commissioner.
- 5.2 A Personal Data Breach that poses a **risk** to the privacy of the individual must be reported to the Data Protection Commission. A Personal Data Breach that poses a **high risk** to the privacy of the individual must be communicated to the individual.
- 5.3 The breach must be reported without undue delay and within 72 hours of our becoming aware of the breach at the latest. If the notification is late, it must be accompanied by the reasons for the delay.

Breach Management Policy and Procedure

Note Personal Data Breaches at non-EU establishments where EU data is being processed are also bound by the notification obligations



- 5.4 If it is not possible to provide all the information about the breach in one go, it can be provided in phases without undue further delay.
- 5.5 The Data Protection Commissioner must be notified via the DPC Breach notification form which can be found, along with relevant email addresses, at <https://dataprotection.ie/docs/GDPR-Overview/m/1718.htm>

Important

Consult the Head of Public Affairs before submitting the Breach Incident Form to the DPC

6. Do I need to communicate the breach to the Data Subjects?

- 6.1 While a data breach that poses a **risk** to the rights and freedoms of the individual must be reported to the commissioner, a breach that poses a **high risk** must be reported to the individuals

Breach Management Policy and Procedure

Important

The purpose of informing the data subjects is to ensure that they are aware of the risks to them and that they can take the appropriate steps to protect themselves. Such action must, therefore, be prompt.

- 6.2 The notification to the individuals must include the following:
- A description of the nature of the breach
 - The name of the DPO or other relevant contact point
 - A description of the likely consequences of the breach
 - The actions taken by the controller to address the breach and appropriate measure to mitigate the breach e.g. that the breach has been notified to the regulator and appropriate advice has been received and specific advice to the individual such as resetting passwords
- 6.3 The data subjects should be contacted directly unless this would involve a disproportionate effort to do so. Where a bulk communication is required, it must be transparent in both language and channel e.g. including details of the breach as part of a press release would not be considered sufficient notification. Examples of appropriate channels would be emails, SMS, direct messaging, prominent banners on websites, postal notification and prominent advertisements in print media. Do not use the channel that sustained the security compromise.
- 6.4 On receipt of the Data Breach Notification the Data Protection Commission can advise, or order, that the data subjects be informed of the breach.
- 6.5 Where there is a high risk to the Data Subject, there are only three conditions under which the individual does not need to be informed:
- Appropriate technical and organisational measure are in the place to protect the data (i.e. state of the encryption)
 - Immediately following the breach steps were taken to ensure that the high risk to individuals was not likely to materialise
 - It would take disproportionate effort to inform the individuals. In the highly unlikely event that this condition appears to be applicable to an incident in RCPI, consultation with the DPO and approval by the CEO must be sought before it is applied.
- 6.6 RCPI acknowledges that while the regulator might advise on the notification of individuals, it is primarily the responsibility of RCPI to take steps to help individuals protect themselves in the event of a data breach.

Breach Management Policy and Procedure

7. How do I close out the Personal Data Breach?

- 7.1 All Personal Data Breaches, whether they have been reported to the Data Protection Commission or not, must be recorded on the RCPI Personal Data Breach Log. This is in part because the regulator may request to see information about our management of breaches under the principle of accountability in demonstrating compliance with Article 34 of the GDPR. Moreover, as part of the on-going risk assessment in the organisation, it helps us to identify and address the types of risks to which RCPI is exposed.
- 7.2 In completing the log you must include, the details of the breach, the cause, the personal data affected, the consequences of the breach, remedial action and the justification for decisions made (particularly where the breach was not notified or why there was a delay in notification).
- 7.3 Update the relevant DPIA and data processing logs to reflect the occurrence/resolution of the incident

8. Useful Links

Recommendations for a Methodology for the Assessment of the Severity of a Personal Data Breach -

<https://www.enisa.europa.eu/publications/dbn-severity>

Personal Data Breach Section of the Data Protection Commission website –

<https://www.dataprotection.ie/docs/GDPR-Overview/m/1718.htm>

Appendix 1 – WP29 Examples of Personal Data Breaches and Reporting Requirements

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 was 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 that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	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 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. 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 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.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. 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. 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.	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). 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.
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.