Breach Notification Form

Report a breach of personal data to the Data Protection Commission

Use this form if you are a Data Controller that wishes to contact us to report a personal data breach that has occurred, or you think may have occurred, in your organisation in circumstances where you have determined that the breach presents a risk to the affected individuals. If you are a publicly available electronic communications networks or services provider (Telco) please continue to report breaches using the form available at https://dataprotection.ie/secur-breach/ in accordance with Commission Regulation (EU) 611/2013.

If the breach you wish to notify DPC about is a cross-border breach, please complete the Cross-Border Breach Notification Form available at https://www.dataprotection.ie/docs/GDPR-Overview/m/1718.htm. *Note: a cross-border breach involves a breach of personal data that affects individuals in Ireland and another Member State or States , or processing which takes place in more than one Member State.*

If you are an individual that has been notified of a breach by an organisation and wish to raise a concern with the DPC, or suspect your personal data has been subject to a breach and wish to raise the matter with the DPC, you should use the following Raise a Concern Form available at https://www.dataprotection.ie/docs/Raise-a-concern/1716.htm

A personal data breach occurs when the data is accessed, disclosed, altered, lost or destroyed in contravention of an organisation's obligation to keep personal data in its possession safe and secure.

When completing this form, please do not include any of the personal data involved in the breach.

Refer to Appendix 1 for further guidance before submitting your notification.

[*] Represents questions that are mandatory (unless otherwise stated at Question 10)

Before entering any information into this form please complete the following steps:
1. Download the form and then save the form to your local PC
2. Close the form
3. Re-open the form from your local PC

Section 1 – Initial Information

1. What type of breach report do you wish to make?*

[Please enter one option]

2. How serious is the risk of the breach for affected individuals?* (Refer to Appendix 1 for guidance)

[Please enter one option]

Section 2 – About You

3. Please enter the name of your organisation*

4. Please enter your name*

5. Please enter your phone number*

6. Please enter your email

7. Please specify the sector within which your organisation operates

[Please enter one option]

8. Please enter your postal address (including your eircode)

9. Are you the DPO for your organisation*?

[Please enter one option]

10. If you are not the DPO, please enter the DPO's name and contact phone number (if any)

If you wish to update a previous breach report please now proceed directly to Section 6.

Section 3 – About the Breach

11. Please enter the date and time of the incident (where necessary an estimate can be made)*

12. Have you estimated the response to Question 11?*:

[Please enter one option]

13. Please enter the date and time that the incident was detected:

14. If you have not notified DPC of the breach within 72 hours of becoming aware of it, please outline the reasons for this.

15. Did you notify affected individuals?

[Please enter one option]

16. If you have not notified affected individuals please explain why:

17. Is the breach ongoing?*

[Please enter one option]

18. What is the nature of the breach?*

[Please enter one option]

19. Please describe how the breach occurred?*

Section 4 – About the Breached Data

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

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

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

22. Were special categories of data involved?*

[Please enter one option]

'Special categories' of data are listed below

23. 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

24. Please insert the number of affected individuals (where necessary estimates can be made)*

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

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

[Please enter one option]

If you responded yes, please complete the Cross Border Notification Form available at https://www.dataprotection.ie/docs/GDPR-Overview/m/1718.htm

27. Were vulnerable individuals affected?*

[Please enter one option]

Refer to Appendix 1 for the definition of a 'vulnerable' individual

28. 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 enter one option]

Section 5 – Measures in Place

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

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

31. Are the mitigating measures fully implemented?*

[Please enter one option]

32. Please provide further detail in the event mitigating actions have not been fully implemented*

33. 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

34. Where 'Other' is selected above, please provide further details:

35. Have you secured / retrieved the breached personal data?

Yes

36. 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.

Section 6 – Update a Breach Notification

37. Please insert your breach notification reference number (if you have been provided one by DPC)

38. Please outline the update you wish to provide DPC

Appendix 1 – Breach Notification Form Guidance

Where do I send this form?

Send your complete form to breaches@dataprotection.ie.

What do I include in the email subject line?

- For new breach notifications – *"new", organisation name, risk rating,* e.g. *new breach notification, [organisation name], severe risk*
- For updates to an existing notification – *"updated breach notification", organisation name, reference number (if any has been provided), e.g. updated breach notification, [organisation name], [reference number]*

Further guidance is provided below:

Relevant Question	Guidance
2. How serious is the breach for affected individuals?	In determining how serious you consider the breach to be for affected individuals, you should take into account the impact the breach could potentially have on individuals whose data has been exposed. In assessing this potential impact you should consider the nature of the breach, the cause of the breach, the type of data exposed, mitigating factors in place and whether the personal data of vulnerable individuals has been exposed. The levels of risk are further defined below: • **Low:** The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal • **Medium:** The breach may have an impact on individuals, but the impact is unlikely to be substantial • **High:** The breach may have a considerable impact on affected individuals • **Severe:** The breach may have a critical, extensive or dangerous impact on affected individuals.
27. 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.
28. 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?*	The EU Law Enforcement Directive (LED) provides for the free flow of personal data between competent authorities within the EU for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and the transfer of such personal data to third countries and international organisations. Personal data processed for the purposes listed above will be subject to the provisions of the LED.

Further guidelines on personal data breach notifications are available here - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052