Data Breach Policy and Procedure

Ref: IC011, v2

June 2024

An Bord Um
Chúnamh Dlíthiúil
Legal Aid Board
Providing access to justice since 1979

Policy and Procedure Document Summary

Document Governance and Management	
Document Name	Data Breach Policy and Procedure
Current Version	V2
Document Reference Number	IC011
Date Effective From	24th June 2024
Date Effective Until	23rd June 2025
Commissioning Directorate	Information & Communications Directorate
Commissioning Unit	Knowledge & Information
Document Owner (Director)	Gareth Clifford
Document Author	Dr. Brian Moss
Document Approver (Person or Group)	Executive Management Team
Note: Formal review may occur sooner if new legislative/regulatory or emerging issues/research/technology/audit etc. dictates sooner.	

Version Control				
Version No.	**Date Reviewed**	**Description of Change**	**Author**	**Approved by**
1	01/05/2020	Range of Changes	DPO	EMT
2	16/05/2024	Full Review	Brian Moss	Gareth Clifford

1. Purpose

This document sets out the policy through which the Legal Aid Board will respond to data breach incidents.

2. Scope

This policy applies to all breaches of personal data held by the Board, processed on its behalf, and in all functions of the Board.

3. Target Audience

This policy is intended for Board staff, clients, and service providers to the Board. A copy of this policy is available on the Board website www.legalaidboard.ie.

4. Roles and Responsibilities

The Legal Aid Board ensures compliance with the GDPR through its Corporate Governance Framework. The arrangements in place to oversee, monitor and ensure compliance with data protection legislation are set out below.

Data Protection section: advises on and monitors compliance with data protection legislation, taking timely action and making recommendations to improve the Board's performance where needed. The section manages subject access requests, breaches, and conducts data protection impact assessments where needed. The section also acts as the main contact point for the Data Protection Commission, the Irish supervisory authority on data protection. The Data Protection Officer role is located in the section and leads on these matters utilising staff support, assistance, advice, and training to enhance organisation-wide compliance with data protection.

Staff of the Legal Aid Board: all are individually responsible for reading, understanding, and complying with obligations of the GDPR, the Data Protection Act 2018, set out in this policy, and in all Board data policies in their daily work. All policies are available on www.legalaidboard.ie. Staff are also individually responsible for engaging with data protection training provided by the Board.

Processors: are those who undertake a range of actions including store, save, use, work on personal data from the Legal Aid Board. Such entities are responsible for complying with this policy in any activity undertaken under contract with the Board.

5. Definitions

- **Personal Data**: information relating to an identifiable living person who can be identified from those data; e.g. name, identification number, location data, an online identifier, etc.

- **Data Subject**: an individual whose personal data are processed.
- **Data Processor**: an organisation/ individual that processes personal data on behalf of a Controller.
- **Data Breach:** a loss in security leading to an accidental, unlawful destruction, loss, alteration, disclosure, or access to personal data that belongs to another person.

6. Personal Data Breach Policy

6.1 What does a breach look like?

A breach can be a Board client receiving another client's letter in error, a private practice solicitor getting the file of a different client or a Board staff member sending an email to an incorrect address.

6.2 Who can report a breach?

A breach involving personal data held by the Legal Aid Board should be reported by anyone who comes upon or receives personal data that is not their own. Persons including solicitors, Board clients, social workers, gardaí, and members of the public, for example, should report a data breach involving personal data processed by the Board to the Board's Data Protection section. Board staff must report a breach of any personal data held by the Board to the Data Protection section. All reports of a breach should be sent to dataprotection@legalaidboard.ie.

6.3 Why is a breach important?

A breach of personal data may result in physical, material, or non-material damage identity theft. Assisting with the recovery of any breached data is therefore important.

Given the above, a person reporting a personal data breach should not hold on to data they have received/ come upon in error or attempt to return it to the person who owns the data. This can cause legal issues. Instead, they should inform the Board's Data Protection section as soon as possible. The Data Protection section will assist in securing return of the data to the Board.

7. Personal Data Breach Procedure

The Procedure for dealing with a personal data breach is set out in Appendix 1. All staff, processors and contractors must comply with this procedure in order to ensure that a data subject's data protection rights under GDPR are met.

When a person wishes to report a suspected data breach, it is encouraged to contact the Board's Data Protection section (see below).

8. Contact Details

The Board's Data Protection unit and Data Protection Officer can be contacted at the details below. These are also published on the Board's website www.legalaidboard.ie

Data Protection Officer
Legal Aid Board
Quay Street,
Cahirciveen,

Co. Kerry
V23 RD36

Phone: (066) 947 1000
Email: dataprotection@legalaidboard.ie

9. Making a Complaint

A person dissatisfied with the Board's response to matters relating to its Data Breach Policy may then submit a complaint as follows:

Data Protection Commission
21 Fitzwilliam Square,
Dublin 2.
D02 RD28
Ireland

Phone: 01 765 0100
Email: info@dataprotection.ie
Web: www.dataprotection.ie

10. Monitoring, Enforcement, and Alteration

Compliance with this policy will be monitored by the DPO and the Executive Management Team members reporting to the Board Audit and Risk Committee.

The Board reserves the right to take action it deems appropriate where individuals breach this policy. Board staff who breach this policy may be subject to disciplinary action. The Board reserves the right to remedy a breach of this policy by contractors, sub-contractors and commercial service providers via contracts in existence with them.

The Board will amend this policy regularly but may amend this policy at any time to take account of business, legislative, or organisational changes.

Any changes to the policy will be notified on the Board website.

Appendix 1- Personal Data Breach Procedure

1. When a breach occurs

- The Data Protection section has two Forms in place to assist gather information on breaches reported by Board staff and those by external parties. The form for staff to report work-based matters is available on the internal notice board iLAB. The form for all other persons is available on www.legalaidboard.ie.
- The form should be completed as soon as a breach is identified and forwarded to the Data Protection section, dataprotection@legalaidboard.ie.
- The Data Protection section will log each data breach identified to it.
- Once a breach is identified, the Data Protection section will undertake to identify the details of the matter.
- This will require direct contact with and cooperation from Board staff and/ or external parties.
- The section will liaise with relevant work units of the Board to indicate necessary actions.

2. Local Unit role

- Where any local work Unit receives a data breach form / notification directly from a client / contractor / practitioner, they should forward this to the Data Protection section immediately in the first instance.
- A local work Unit must not look to address any other aspect of the data breach before reporting it to the Data Protection section and seeking its guidance.
- Many local work Units will have a Data Steward on staff. This role holder supports data protection activity within their workplace. In conjunction with the local manager, this person may be used to support preparation of the breach notification form and any subsequent effort to retrieve breached data.
- Each local work unit, not the Data Protection section, is responsible for retrieving any data breached. This is to minimise the impact of the breach. The organisation of this work should be decided at the local work Unit level (e.g. managing solicitor/ mediator/ assistant principal or equivalent).
- The Data Protection section will follow up with a local work Unit at intervals after an incident to ascertain what data retrieval was possible.
- A local Unit, under the local manager, should aim to identify how to minimise any future occurrence of the breach and breaches generally.

3. Processors

- Where a breach occurs in any entity processing data on behalf of the Board, that entity must complete the breach notification form once the breach has been identified.
- The entity must inform the Board Data Protection section, sending in the completed notification form.
- The Data Protection section will provide guidance on what should occur thereafter.

4. Data Protection section role

- The Data Protection section must determine the risk of the breach incident at the outset, based on DPC guidance.
- This Data Protection section must record this risk rating for any incident in its Breach Log.
- The section must consider reporting the breach to the Data Protection Commission if it is likely to result in a risk to a data subject or already has done.
- If the Data Protection section does intend to report a breach to the DPC, it must do this within 72 hours of first becoming aware of the breach.

- If the section is unable to report the breach to the DPC within 72 hours, it must explain why it was not able when finally reporting the breach.
- Where the Data Protection section notifies the DPC, it must set out the number of data subjects affected, the likely consequences, the measures to be taken in response.
- If the section does not intend to notify the DPC, it must record why not.
- Where the risk rating requires the Data Protection section to inform the data subject affected, it shall do this without undue delay.
- If the section does not intend to report a data breach to the data subject involved, it must record why not.
- A person / organisation not satisfied with the Board's reply may raise it with the Board. If this cannot be resolved, the person / organisation may complain to the Data Protection Commission.