# Data Protection Policy

## Ref: IC001, v3

May 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 Protection Policy |
| **Current Version** | v3 |
| **Document Reference Number** | IC001 |
| **Date Effective From** | 15th May 2024 |
| **Date Effective Until** | 14th May 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 | 1/6/2018 | Initial Development | DPO | EMT |
| 2 | 1/5/2020 | Range of Changes | DPO | EMT |
| 3 | 5/3/2024 | Full Review | Brian Moss | Gareth Clifford |
| | | | | |
| | | | | |

# 1. Purpose

This document provides a framework through which the Legal Aid Board (the Board) meets its requirements under the General Data Protection Regulation (GDPR) and Data Protection Act 2018. The Board may act as a Data Controller or Processor and is therefore responsible for ensuring the privacy of Data Subjects and the protection of all Personal Data it processes at all times.

# 2. Scope

The Board collects, processes, and stores personal data from service users, private practitioners, staff, and service providers. A non-exhaustive list of the forms of Personal Data which will apply includes personal details, special category, employment, financial and HR information. The Board uses these to undertake its legal advice and consultation, mediation, and corporate service functions. Such data are gathered and/ or processed manually, electronically in soft or hard-copy format.

This policy applies to all functions of the Board conducted by Board staff, Processors, or contractors.

# 3. 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.
- **Special Category Personal Data**: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, health data, sex life or sexual orientation, and criminal data.
- **Processing**: anything done with personal data, including collection, organisation, storage, adaptation, retrieval, disclosure, destruction, etc.
- **Data Controller**: the organisation/ individual that alone or jointly with others determines the why and how of processing personal data.
- **Data Processor**: the organisation/ individual that processes personal data on behalf of a Controller.
- **Data Subject**: an individual whose personal data are processed.
- **Data Breach**: the accidental or unlawful destruction, loss, disclosure, or access to Personal data.

# 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.

**The Audit and Risk Committee**: a committee of the Legal Aid Board, responsible for scrutiny of information governance matters and making recommendations for improvement to the Executive.

**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.

**The Executive Management Team**: this directs the Board's work on a daily basis, approving policies and actions, and directing local managers.

**Local Managers**: have responsibility for ensuring compliance with GDPR in the teams that report to them. They are assisted in this by Data Stewards located across the Board's network of offices.

**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.

**Department of Justice**: the Board is an agency of the Department of Justice. The Department may organise external data protection audits to monitor and ensure compliance with data protection legislation.

# 5. Data Protection Principles

The GDPR sets down several principles for the handling of personal data. This Data Protection Policy adheres to these principles, namely data will be:

1. processed in a way that is lawful, fair and transparent;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
3. limited to what is necessary;
4. be accurate and kept up to date;
5. stored for no longer than is necessary for the intended purposes;
6. processed in a manner that ensures appropriate security; and
7. visibly compliant with GDPR through appropriate policies and procedures.

The Board maintains a Record of Processing Activities (ROPA), as required under Article 30 GDPR. That written record sets out Board adherence to the above data protection principles for all categories of processing activities for which it is responsible.

When requesting personal data, the Board will be fully transparent in clear and plain language via its Privacy Policy/ Data Protection Notice as to how these data will be used. A copy of the Privacy Policy/ Data Protection Notice is available at www.legalaidboard.ie. The Board will ensure that the data are not used for any purpose other than that

originally specified and for which consent was given. A data subject has the right to withdraw their consent for use of the data and all data will be retained only for periods set down in the Board's Data Retention and Destruction Policy.

# 6. Lawful Processing of Data

Personal data are processed by the Board to meets its legal obligation under the Civil Legal Aid Act 1995 to perform its public sector tasks and functions. These functions are to provide legal aid and legal advice, mediation, and criminal legal aid or engage others to provide such service on its behalf in the public interest. Its public sector tasks extend to contracting in certain services and conducting research.

# 7. Rights of 'data subjects'

Data Subjects have the following rights under GDPR in relation to their personal data:

- **Right to be informed/right of access** A data subject has the right to be informed by the Board about the collection and use of their personal data. They also have the right to access their personal data by making a Subject Access Request.
- **Right to rectification where inaccurate or incomplete** A Data Subject has the right to have such data rectified.
- **Right to erasure where no longer necessary/ consent is withdrawn** This is not an absolute right and does not apply in circumstances where the Board's processing of personal data is necessary in certain circumstances (e.g. for a public interest task, to perform a conflict check, where a solicitor deems necessary, or for legal claims).
- **Right to restrict processing uncertain certain conditions** This right applies where a Data Subject queries the accuracy of data or its use, requests its retention for a legal claim, or objects to their processing. The Board will restrict the processing of personal data when reviewing the accuracy of the data and/ or the legitimate grounds for processing the data. The Board may refuse to comply with a request if it considers that it is manifestly unfounded or excessive.
- **Right to object to processing for specific purposes** A data subject has a right to object to the processing of their personal data in specific circumstances. Where such an objection is received, the Board will assess each case on its merits.
- **Right to data portability in an easy format or to transmit to another data controller** A data subject can request the Board to provide the data in electronic format in order to provide it to another Data Controller.

Further information on making any of the above applications can be found at www.legalaidboard.ie.

# 8. Data Protection by Design / Data Protection by Default

In alignment with the principles of Data Protection by Design and by Default, our organisation is committed to integrating data protection into our processing activities and business practices, from the design stage right through

the lifecycle of any data processing operation. These principles are enshrined in law under the GDPR (Article 25). This approach ensures that privacy and data protection are central considerations in the initial design specifications and throughout the operational process, promoting minimal data processing, privacy-friendly default settings, and end-to-end security.

- **Data Protection by design** means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.
- **Data Protection by default** means that the user service settings (e.g. no automatic opt-ins on customer account pages) must be automatically data protection friendly, and that only data which is necessary for each specific purpose of the processing should be gathered at all.

It is the responsibility of all Board staff to reflect on how data protection principles are actively reflected in any intended work task they undertake and that by default a task will collect, use, retain, and allow access to data only as is necessary for a designated work task. Data protection thinking should be applied at the commencement of a work task, should be applied to all stages of a work task, and be kept under review by any manager who has staff reporting to them.

# 9. Data Procedures

The Board has in place procedures to ensure its compliance with different GDPR aspects. These are set out below.

### Data Breaches

Data protection breaches may include but are not restricted to theft, accidental or intentional loss, misdirection, or disclosure of Personal Data. Where they become aware of such an occurrence, a staff member must inform the DPO. The DPO will log the breach, determine if there is a risk to the Data Subject, and, if so, notify the Data Protection Commission without undue delay and within 72 hours where necessary. The DPO will also provide direction to staff, make contact with the Data Subject as necessary, and, once the breach is finalised, will look to implement future preventative measures in conjunction with managers.

### Subject Access / Rectification / Restriction / Erasure Requests

As set out in Section 7 above, a client, service provider or staff member of the Board is entitled to request access, amendment, limitation or erasure of Personal Data the Board holds on them. All of these rights are subject to restrictions. A request for access, rectification, limitation, or erasure can be submitted to the Data Protection section. Designated forms for this purpose and to assist requesters can be found at www.legalaidboard.ie.

It assists the Board if a requester provides as clear detail as possible regarding the data of interest. Once received, the DPO will acknowledge the request and liaise with relevant work units of the Board to indicate necessary actions and reply.

### Data Agreements

The Board is entitled by law to transfer data to another entity under four scenarios. These are explained below.

**Data processing agreements** arise between the Board as Controller/Processor and another non-public sector entity as Processor/ Controller. These can involve Personal Data as the primary focus of the contract (e.g. interpreter services for clients) or as a secondary focus (e.g. window cleaning).

**Data sharing agreements** involve transfer of data to another public sector body in line with GDPR and the Data Sharing and Governance Act 2019 in order to assist research or service improvement or one or both bodies. A period of public consultation is required before signing any such agreement.

**Joint Controller agreements** entail two or more bodies agreeing to exchange data, both adopting the role of Controller and a third party possibly acting as processor (e.g. training provision for Board staff arranged by a government department that uses a third party to deliver the training).

All three agreements require identification of the Processor(s) and Controller(s) in the data transfer, a legally binding contract clearly setting out the subject matter, duration, nature and purpose of the data processing, the type of personal data being processed, the categories of data subjects whose personal data are being processed, and the obligations and rights of the Controller. In advance of any contract signing, the Board DPO must be contacted to undertake a review of data protection clauses in the contract and due diligence of the other parties.

The fourth scenario concerns **requests from a third party for Personal Data to assist it undertake an investigation**. This could be a police investigation into a possible criminal act (e.g. Board CCTV footage), health and safety incident, or insurance matter. All such requests must be made in writing to the Data Protection section, clarifying their reason, and data sought (for CCTV, including location, date, time, and identifying features of the person concerned). Other than receipt of a court order or warrant, there is no legal onus on the Board to grant such requests. All requests will be decided on a case-by-case base, given their merits.

### Security and Record Keeping

The Board implements technical and organisational measures to give effect to the principles of protecting Personal Data. These are:

- access controls to physical workspaces and IT systems;
- regular back-up of files and disaster recovery;
- access controls to IT drives per work unit, thereby limiting sight of files;
- limiting access to case tracking system and file to legal aid and mediation staff, further restricting this based on staff geographical assignment;
- auditing of access to client files to monitor and respond to security incidents;
- a Clean Desk approach across the organisation. This means that when away from their desk staff should remove all work documents, work mobile phones, and lock their computer screen. Staff members working remotely or from home are required to adopt similar measures;
- staff keeping all hard copy materials relating to business matters in manual filing systems and locking these when leaving an office during the day/ at end of the working day. When finished with a hard copy version of a document, it must be disposed of in confidentiality waste bins provided by the Board;
- staff not removing any files from their LAB workplace unless with the authority of an appropriate manager; and
- staff informing IT of any hardware that is broken or no longer needed.

### Data Protection Impact Assessment (DPIA)

The Board maintains a separate policy on data protection impact assessments (DPIAs) A DPIA is an assessment of the protections to personal data in any new proposed processing activity. The policy is available to view on the Board website www.legalaidboard.ie.

### Transfer of Personal data outside the EEA

The Board will only transfer data outside the European Economic Area in accordance with GDPR and only where appropriate safeguards are in place.

### Record of Processing Activities

A requirement of the GDPR, this is a written record of all categories of processing activities undertaken by the Board, their purpose, retention periods and transfer activity beyond the EEA. It will be reviewed on an annual basis.

### Confidentiality

Board staff must ensure that all information given in confidence in the course of work is well-protected. Information given in confidence is likely to cover personal and sensitive information that could cause reputational of financial harm if disclosed outside a work unit or outside the Board.

Confidential information must be protected by accessing it only where necessary, keeping it secure in the workplace, and, when out of the office, viewing and discussing it on a work pc/laptop or mobile phone only out of the sight and hearing of others. Such information must not be disclosed to colleagues or others unless relevant to processing the matter. Any print copies of such information should not be moved off-site unless necessary, should not be copied beyond required work use, must be returned to line managers/ other units as directed when no longer needed for a task, and disposed of in confidentiality waste bins when no longer needed. Staff must also not use confidential information for personal or others' benefit.

Information given in confidence can be shared with appropriate persons where it discloses a risk of harm to the information-giver or to others.

Further guidance to Board staff on confidential information is contained in internally available Administrative Procedures Handbooks.

# 10. 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

# 11. Making a Complaint

A person dissatisfied with the Board's response to matters relating to its Data Protection 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

# 12. Monitoring, Enforcement, and Alteration

Compliance with this policy will be monitored by the DPO and the EMT 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.