Data Protection Compliance Monitoring Framework

Ref: IC018, V2

September 2025

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

Framework Document Summary

Document Governance and Management	
Document Name	Compliance Monitoring Framework
Current Version	V2
Document Reference Number	IC018
Date Effective Until	12 September 2027
Date Set for Next Review	On next approval + 2 Years
Commissioning Directorate	Information & Communications Directorate
Commissioning Unit	Knowledge & Information
Document Owner (Director)	Tomás Keane
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	20/03/2024	New procedure	Brian Moss	Garrett Clifford
2	12/09/2024	Review all sections	Dr. Ellen Ganly	Dr. Brian Moss

1. Purpose

This document sets out the Legal Aid Board's rationale and procedure for adhering to GDPR at the organisational level and monitoring compliance with GDPR across the organisation and within local business units.

2. Application

This framework will be applied by the Data Protection section to all business units. Cooperation with the Data Protection section in completing the form is expected from all Directors and business unit leads.

A copy of this procedure is available on the internal knowledge repository iLAB.

3. Rationale

The EMT has adopted this Framework to ensure that GDPR compliance is to the fore in everything staff do on an ongoing basis and in the governance of information matters.

4. Responsibilities

Directors: are responsible for compliance with all Board policies within their Directorates and are the Board's Data Owners. They are responsible for keeping under review and adopting procedures that reflect GDPR requirements and Board data protection policies, and that make them intelligible to staff and attainable. Directors must ensure that data actions are led in Law Centres/ Mediation Offices by Managing Solicitors/ Mediators and/ or complied with by all staff.

Business unit leads are responsible for provision of any relevant data sought by the Data Protection section to complete the monitoring form (Appendix 2).

The Executive Management Team: oversees compliance with data protection across the Board's Directorates.

Data Protection section: co-ordinates data protection training to reinforce GDPR compliance across Directorates and the Board as a whole.

5. Idenitying and implementing compliance monitoring

GDPR makes several expectations of data controllers such as the Legal Aid Board. To ensure it remains compliant with those obligations, this Framework sets out how it will implement GDPR compliance (Appendix 1). Compliance monitoring in turn is the verification that such compliance is being carried out. In this Compliance Framework, the reporting of compliance monitoring takes two formats. The first format (Appendix 2) is for completion at the local business unit level upon request by the Data Protection section. It is intended to support and expand on areas addressed by the Internal Audit Unit but not to duplicate its work. The second format (Appendix 3), a Compliance Monitoring Report template, provides a format in which the Executive Management Team can consider and confirm for the Board its oversight of compliance with GDPR across the organisation within a defined period. Completion of both forms is intended to assist local business units and the EMT identify strengths and areas for further development in the overall data protection approach.

6. Contact Details

The Board's Data Protection section 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
48/49 North Brunswick Street,
Smithfield,
Dublin 7,
D07 PE0C.

Telephone: 01 6469 764
Email: dataprotection@legalaidboard.ie

Appendix 1- Compliance Framework

1. Governance and Accountability

- **Data Protection Officer (DPO):**
    - Appoint a Data Protection Officer as mandated by GDPR, with responsibility for overseeing data protection strategy, monitoring compliance, and acting as a point of contact for data subjects and the Data Protection Commission (DPC).
    - Ensure that the DPO operates independently and reports to the highest levels of the Legal Aid Board's management.
- **Data Protection Policies and Procedures:**
    - Develop, document, and regularly update data protection policies aligned with GDPR and Irish Data Protection laws.
    - Ensure policies cover all aspects of data processing, including data collection, storage, use, sharing, and disposal.
    - Establish clear roles and responsibilities within the Legal Aid Board for data protection and privacy.
- **Governance Framework:**
    - Create a governance structure that includes senior leadership oversight of data protection compliance.
    - Ensure the Board can address privacy and compliance issues regularly.

2. Risk Assessment and Management

- **Data Protection Impact Assessments (DPIAs):**
    - Conduct DPIAs for any new or existing high-risk data processing activities (e.g., large-scale processing of sensitive data, data sharing between agencies).
    - Implement measures to mitigate identified risks, ensuring compliance with data protection principles such as data minimisation and security.
- **Risk:**
    - Ensure data protection is considered as part of the organisations approach to risk.
    - Where identified, prioritises risks based on likelihood and impact, and establish mitigation actions for high-risk areas.

3. Data Inventory

- **Record of Processing Activities (RoPA):**
    - Maintain a detailed and up-to-date RoPA as required by GDPR, documenting the categories of personal data processed, purposes, data subjects, retention periods, and any data processing or sharing arrangements.

4. Training and Awareness

- **Staff Training:**

- Implement mandatory data protection training for all employees, ensuring awareness of GDPR principles, Board policies and procedures.
- Provide refresher courses and updates on new legal requirements or identified gaps as necessary.

- **Awareness Campaigns:**
  - Conduct internal awareness campaigns to promote a culture of privacy within the agency.
  - Use tools like newsletters, posters, and workshops to keep data protection at the forefront of staff priorities.

5. Monitoring and Auditing

- **Internal Audits:**
  - Establish a schedule for regular internal audits to assess compliance with GDPR, Irish Data Protection laws, and Board policies.
  - Conduct audits on high-risk areas.
- **Third-Party Audits:**
  - Audit third-party vendors or partners who process personal data on the Board's behalf to ensure they comply with data protection obligations.
  - Include data protection requirements in procurement processes and contract management.

6. Data Subject Rights Management

- **Procedures for Handling Data Subject Requests:**
  - Implement clear processes for managing data subject rights requests, including access, rectification, erasure, and data portability requests.
  - Adopt policies for handling third party access requests, including for CCTV.
  - Ensure that procedures are efficient and meet GDPR deadlines.
  - Provide staff with guidance on handling complex cases, such as data subject rights that conflict with legal obligations.
- **Transparency and Communication:**
  - Ensure that the Board's privacy notices and policies are clear, accessible, and regularly updated to inform data subjects of their rights. Ensure staff make all clients and suppliers aware of the Board's policies and GDPR.

7. Breach Reporting

- **Breach Reporting:**
  - Ensure up to date policies/procedures are in place to assist staff identify necessary actions when a breach occurs.
  - Inform Units how to mitigate/avoid future breaches at the point of reporting a breach.
  - Maintain a breach log to record all data breaches to enable analysis and prevent future incidents.

- Ensure that relevant breaches are reported to the DPC within 72 hours, as required by law.

8. Continuous Improvement

- **Feedback Mechanisms:**
  - Establish feedback channels for staff to report data protection concerns or suggest improvements.
  - Encourage a culture of continuous improvement in data protection compliance.

9. Documentation and Reporting

- **Accountability Documentation:**
  - Maintain detailed records of compliance activities, including DPIAs, RoPA, audit reports, training records and relevant logs.
  - Ensure that all documentation is readily available for inspection by the DPC or other relevant authorities.
- **Reporting to Leadership:**
  - Make available to the EMT as required updates on data protection risks, compliance status, and any significant issues that require attention or resources.
  - Make available to the EMT a template for reporting matters to the Board, or have the DPO complete such a template for submission to the Board.

10. Legal and Regulatory Engagement

- **Engage with data protection developments:**
  - Address any communication from the Data Protection Commission (DPC) and other relevant regulatory bodies.
  - Stay informed about regulatory guidance, decisions, and best practices that impact the Legal Aid Board's compliance obligations.
- **Legal Reviews:**
  - Advise the EMT to engage legal experts to review complex data protection issues or their interaction with other laws affecting the Legal Aid Board's operations.

Appendix 2 GDPR Compliance Self-Audit- please answer all questions in each section

	Answer
Last review date (if first review, indicate "no prior" opposite)	
Centre/ Office/ Unit	
Tambour units • How many on-site? • How many in use? • Functioning outer door and slots? • Locking key present?	
Offices • Are doors locked when staff are out? • Are doors locked at the end of working days?	
File rooms • Are doors locked during the working day? • Anything other than files kept in file rooms? • Access restricted/ given to all unit staff?	
Clear desks • Last date checked? • No of breaches in review period? • Observations on work unit?	
Sharing files with other Units/ Directorates • Any sharing of data in the review period? • If yes, was a data Controller identified in advance of sharing? • Is the data sharing ongoing/ completed?	
Staff use of files off-site • This is rare/ occasional/ frequent (indicate one choice opposite) • Was your permission sought from staff on each occasion? • Files recorded when returned? • Longest period of files off-site? • Category of staff using files off-site?	
Data destruction • Was disposal of data recorded in local register or in the DP section's Destruction Compliance Form template? • Date of last data destruction?	
Display and disposal of printed personal/ other data • Any data waste visible in standard bins? • Any data visible on photocopier/printers? • Any data visible on desks when staff not in the office? • Any data visible elsewhere in office?	
Confidentiality bins • Bin on-site in visible location? • Collection schedule in place? • Contact person on staff identified? • Last collection date? • Collection completed? • Staff advised to use bins over shredders?	
Data classification • What are the main categories of files in the unit?	

(e.g. client cases, work plans, finances) • List the number of file types in the unit per each category of the LAB Classification Policy (i.e. public, internal, confidential, restricted)	
Data access • Last date access permissions reviewed? • Any inappropriate/unauthorised access attempts in review period? • Any referral to HR/ IT?	
File review • No. of files examined in review period? • Any systemic data protection issues identified? (e.g. repeated issues in client meeting notes, in letters, in reports?)	
Subject Access requests • Number in review period? • All reported? • Yes/ No) • All addressed on time? • No. of live requests?	
Rectify, Restrict, Erase, Withdraw requests • Number in review period? • All reported to DP section? (Yes No) • All addressed on time? • No. of live requests?	
CCTV requests • Number in review period? • All reported to DP section? (Yes No) • All addressed on time? • No. of live requests?	
CCTV • Functioning camera in place? • Signage in place? • Signage visible to visitors?	
Translation and Interpreter services used Any use of services outside of those contracted by Board?	
DPIA • Any consideration of a DPIA in review period? • If yes, what was the issue? • What was the outcome?	
Team meetings • Date of last meeting? • Data protection raised at last meeting?	
Findings Any issues of concern about data protection compliance within he work unit?	
Confirmation that the unit is GDPR compliant	I confirm that data protection is being addressed by this Unit in its daily actions. **Name** **Date**
Next review date (Data Protection section to record)	

Appendix 3 GDRP Compliance Monitoring Report

---

1. Executive Summary

This report provides an overview of the Data Protection Compliance Monitoring Framework implemented by the Legal Aid Board to ensure compliance with the General Data Protection Regulation (GDPR) and Irish Data Protection laws. The framework includes governance structures, risk management strategies, and continuous monitoring mechanisms. This report details the current state of compliance, recent activities, identified risks, and future plans for enhancing data protection efforts within the Board.

---

2. Purpose and Scope

The purpose of this report is to provide an update on the implementation and effectiveness of the Data Protection Compliance Monitoring Framework. The scope of this report covers all personal data processing activities within the Legal Aid Board, including data collection, storage, usage, sharing, and disposal, as well as third-party processing arrangements.

---

3. Governance and Accountability

3.1 Data Protection Officer (DPO):

- **Current Status:** [Name] has been appointed as the Data Protection Officer (DPO). The DPO operates independently and reports directly to senior management.
- **Recent Activities:** The DPO has conducted regular reviews of compliance measures, liaised with departments, and managed data subject requests.
- **Next Steps:** Increase engagement with senior leadership to further embed data protection into strategic decision-making.

3.2 Data Protection Policies and Procedures:

- **Current Status:** Comprehensive data protection policies are in place, covering all aspects of data processing, including GDPR updates, revisions, and staff training requirements.
- **Recent Activities:** Policies were last updated on [Date] to align with recent regulatory guidance.
- **Next Steps:** Conduct a further review to incorporate findings from recent audits and new legal developments.

3.3 Governance Framework:

- **Current Status:** The Board's governance framework includes senior leadership oversight of data protection compliance.
- **Recent Activities:** The governance structure was reviewed and strengthened to ensure privacy issues are regularly addressed.
- **Next Steps:** Enhance reporting mechanisms to ensure the Board receives timely updates on data protection risks and initiatives.

---

4. Risk Assessment and Management

4.1 Data Protection Impact Assessments (DPIAs):

- **Current Status:** DPIAs are conducted for all high-risk processing activities, including [relevant projects].
- **Recent Activities:** DPIAs for [Project Name] were completed, and appropriate mitigation measures were implemented.
- **Next Steps:** Continue assessments for new projects and significant changes to existing processes.

4.2 Risk Register:

- **Current Status:** Current data protection risks
- **Recent Activities:** New risks related to third-party data sharing and processing agreements were identified and mitigated.
- **Next Steps:** Prioritise high-risk areas and enhance monitoring processes.

---

5. Data Inventory

5.1 Record of Processing Activities (RoPA):

- **Current Status:** The RoPA is up to date and compliant with GDPR requirements, covering data retention, destruction, and classification.
- **Recent Activities:** The RoPA was reviewed and updated to reflect new processing activities related to [specific program/project].
- **Next Steps:** Ensure quarterly reviews and prompt updates for operational changes.

---

6. Training and Awareness

6.1 Staff Training:

- **Current Status:** Mandatory data protection training is completed by all staff.
- **Recent Activities:** A refresher training session was conducted in [Month/Year], with a completion rate of [Percentage].
- **Next Steps:** Develop role-specific training for departments handling sensitive data and implement quarterly refresher courses.

6.2 Awareness Campaigns:

- **Current Status:** Internal awareness campaigns are conducted regularly, including information on GDPR updates, CCTV requests, rectification, and erasure rights.
- **Recent Activities:** A new campaign launched in [Month/Year] focused on secure data handling practices.
- **Next Steps:** Expand campaigns to include targeted messaging for high-risk areas, such as email security and mobile device usage.

---

7. Monitoring and Auditing

7.1 Internal Audits:

- **Current Status:** Regular internal audits assess GDPR and Board policy compliance.
- **Recent Activities:** The last audit, completed in [Month/Year], identified minor issues, which were addressed.
- **Next Steps:** Increase audit frequency for high-risk departments and follow up on previous recommendations.

7.2 Third-Party Audits:

- **Current Status:** Third-party vendors are regularly audited for data protection compliance, including external party data processing agreements.
- **Recent Activities:** [Number] audits were completed in [Month/Year], with all vendors found compliant.
- **Next Steps:** Expand the scope of audits for high-risk vendors and ensure GDPR requirements are included in procurement processes.

---

8. Data Subject Rights Management

8.1 Handling Data Subject Requests:

- **Current Status:** Efficient procedures are in place for managing data subject rights requests, including access, rectification, erasure, and CCTV requests.

- **Recent Activities:** [Number] requests were processed within the legal deadlines.
- **Next Steps:** Further streamline processes and explore automated systems for request management.

8.2 Transparency and Communication:

- **Current Status:** Privacy notices are clear, accessible, and regularly reviewed.
- **Recent Activities:** Notices were updated in [Month/Year] to reflect new data processing activities.
- **Next Steps:** Ensure all clients and suppliers are informed about Board policies and GDPR rights.

---

9. Breach Reporting

9.1 Incident Response Plan:

- **Current Status:** A robust breach response plan is in place and tested regularly.
- **Recent Activities:** The last test, conducted in [Month/Year], found the plan effective with minor adjustments required.
- **Next Steps:** Conduct regular testing and provide further training for breach management staff.

9.2 Breach Log and Reporting:

- **Current Status:** A breach log is maintained, and all reportable breaches are communicated to the DPC within 72 hours.
- **Recent Activities:** [Number] breaches were reported in [Quarter/Year], all managed per the response plan.
- **Next Steps:** Implement preventive measures and conduct trend analysis to identify common causes.

---

10. Continuous Improvement

10.1 Feedback Mechanisms:

- **Current Status:** Feedback channels allow staff to report concerns or suggest improvements.
- **Recent Activities:** [Number] feedback submissions led to [specific improvements].
- **Next Steps:** Promote feedback channels and ensure timely responses.

---

11. Documentation and Reporting

11.1 Accountability Documentation:

- **Current Status:** Compliance activities, including DPIAs, RoPA, audit reports, training records, and breach logs, are well-documented.
- **Recent Activities:** Documentation was reviewed and updated in [Month/Year].
- **Next Steps:** Ensure documentation remains accurate and inspection-ready.

11.2 Reporting to Leadership:

- **Current Status:** Regular updates on data protection risks, external data sharing, and overall compliance are provided to senior leadership.
- **Recent Activities:** The last report was submitted in [Month/Year].
- **Next Steps:** Enhance reporting with detailed trend analysis and emerging risk identification.

---

12. Legal and Regulatory Engagement

12.1 Engagement with Regulatory Bodies:

- **Current Status:** The Board maintains open communication with the Data Protection Commission (DPC).
- **Recent Activities:** Recent DPC guidance was incorporated into Board practices.
- **Next Steps:** Continue engagement with regulatory bodies and relevant industry forums.

12.2 Legal Reviews:

- **Current Status:** Legal experts are consulted on complex data protection issues.
- **Recent Activities:** A legal review conducted in [Month/Year] led to updated policies.
- **Next Steps:** Schedule further reviews to address upcoming regulatory changes.

---

13. Conclusion

The Legal Aid Board remains committed to ensuring compliance with GDPR and Irish Data Protection laws through a robust and continually evolving Data Protection Compliance Monitoring Framework. This report demonstrates progress in protecting personal data and highlights areas for further improvement. The Board will continue prioritising data protection, engaging with stakeholders, and refining processes to meet ongoing compliance challenges.

Submitted by: [Name] [Title] [Date] Next Report Due: [Date]