Data Protection Impact Assessment Policy

Ref: IC002, 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 Impact Assessment Policy
Current Version	v3
Document Reference Number	IC002
Date Effective From	15th May 2024
Date Effective Until	14th May 2026
Commissioning Directorate	Information & Communications Direction
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, including combining previous Data Protection Impact Assessment Policy & Procedure (202) into one document	Brian Moss	Gareth Clifford

1. Purpose

The policy is intended to explain how the Board plans, assesses, and implements and new data processing activity, and the obligations and rights that arise from such activity.

The Board will undertake a Data Protection Impact Assessment (DPIA) in order to identify and reduce the data protection risks in a proposed project. This is because the collection, use, storage, and destruction of personal data entails risks. Doing so will enable the Board to be confident in its personal data processing and for stakeholders to be confident in the Board's protection of their data.

2. Scope

This policy relates to the proposed processing of existing and new data by the Board in any project. Client data processed by individual Board solicitors and legal practitioners on its behalf does not constitute large-scale processing. Therefore, it is not subject to this policy.

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. Justification

The Board processes personal data to fulfil its tasks in the public interest, lawful authority, and to undertake research. These provide the legal basis for processing of data and the conditions under which the Board will conduct a DPIA to ensure such data are adequately protected.

5. Responsibilities

Board Business Units: at all times the business unit/ Directorate proposing the new data processing activity will be responsible for commencing, undertaking, and completing a DPIA. Local business units/ Directorates will also undertake the review of a DPIA where requested by the Data Protection Section.

Data Protection Section: will respond to a local business unit request about the need for a DPIA, address queries on DPIA contents, and review the final draft DPIA report. The Data Protection Section will also direct the commencement of any review of a DPIA in place. The Data Protection Section will act as the Board liaison with the DPC around any DPIA matters.

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.

The Board procedure for undertaking a DPIA is set out in Appendix 1.

The template for a DPIA is set out in Appendix 2.

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
Quay Street,
Cahirciveen
Co. Kerry
V23 RD36

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

7. Making a Complaint

A person dissatisfied with the Board's response to matters relating to its DPIA approach 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

8. Monitoring, Enforcement, and Alteration

Compliance with this policy will be monitored by the Data Protection section 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.

Appendix 1: DPIA Procedure

1. Where plans for Data Processing might pose a high risk to the rights and freedoms of data subjects (in particular through involving new technology), the proposing team must ask the Data Protection section about the need to conduct a DPIA and how it should be done.

2. Examples of where a DPIA might be required include new data collection on clients, new research, or combining/ linking or cross-referencing separate datasets or large-scale data processing. Large-scale processing is decided by reference to such factors as the number of data subjects concerned and the volume of data processed. A DPIA must be undertaken before commencing the proposed processing.

3. The local business is responsible for undertaking a DPIA. The Data Protection section will **assist** the proposing team throughout that process but does not complete the DPIA.

4. To determine the need for a DPIA, the local business unit is responsible for providing the data protection section with a description of the processing activities planned, the necessity and proportionality of the processing proposed, and an initial identification and assessment of any risks to the personal data that will be processed and the data subjects to whom the data belong.

5. Consultation with data subjects (e.g. clients, staff and contractors) may be necessary and the possibility should be considered by a project team. Any consultation should be undertaken at the earliest stage.

6. Using the information in point 4, a DPIA must expand on those items and propose any risk mitigation options.

7. A DPIA may determine that the high risk to the rights and freedoms of data subjects arising from a new form of data processing is unlikely to be minimised by available technology and costs of implementation. If this occurs, the Data Protection section will contact the Data Protection Commission, for consultation on the issues. The proposed processing activity should not be advanced any further until that consultation is complete.

8. A local business unit must act on any advice/ direction from the DPC.

9. A DPIA should be presented in a final report. This report must be made available for review by the Data Protection section before finalisation.

10. The local business unit is responsible for signing off on the DPIA final report.

11. The local business unit must ensure that any recommendations in the final report are implemented into the project plan so that it complies with GDPR and domestic legislation.

12. A summary version of the final report can be published on www.legalaidboard.ie. The local business unit must discuss this with the Data Protection section. Any published report will not disclose sensitive business data or procedures.

13. Where a proposed processing activity is similar in nature to an existing one or several similar processing activities proposed, only one DPIA may be required, if a DPIA is required at all.

14. Where there is a significant change to an existing data processing operation or the risk associated with it, a DPIA may be required.

15. The local business unit is responsible for keeping under review any DPIA in place and conducting a review of any DPIA in place. A local business unit must review a DPIA when requested to do so by the Data Protection section.

16. In any Data Processing Agreement in place where the Board is the Controller, a Processor should assist the Board to complete a DPIA and in any engagement with the Data Protection Commission around the issue that the DPIA covers.

17. Where, following initial assessment, there is uncertainty about the need for a DPIA, one shall be compiled. This reflects the Board's responsible approach to personal data. A DPIA will also serve to embed and foster data protection thinking across the Board.

18. The Board retains a template for DPIAs. This template should be followed in all cases by business units where it is determined that a DPIA is required.

19. The Board will retain a log of all DPIAs conducted.

Appendix 2: DPIA Template

Submitting Controller Details

Name of Controller	
Contact email	
Subject of	
Submission date	

Step 1. Identify DPIA Need

Does the project involve:	Yes	No	If Yes, explain
a. processing personal data?			
b. special category data or highly personal data?			
c. criminal offence data?			
vulnerable data subjects?			
d. children?			
e. new technological or organisational solutions?			
f. processing on a large scale?			
g. combining, comparing or matching data from different sources?			
h. processing personal data that could result in a risk of physical harm if breached?			
i. altering the current nature, scope or purposes of current processing?			

Explain broadly what the project aims to achieve and what type of processing it involves. (You may find it helpful to refer or link to other documents, such as a project proposal.)

Summarise why you identified the need for a DPIA.

Step 2. Describe the Processing- scope, context, and purpose

a. What is the lawful basis for processing[1]?	
b. Does the project entail 'further processing' beyond the original lawful basis for collecting data? If yes, please explain	
c. What is the i) type and ii) variety of data that will be processed?	
d. Would the data subjects expect their data to be used in this way?	
e. How will the data be collected?	
f. How often will data be collected?	
g. how many individuals are expected to be included?	
h. How will the data be used?	
i. Who will have access to the data?	
j. What security measures will be used to minimise access to data?	
k. Is it intended to share/ transfer the data to any third-party?	
l. Is it intended to use any data processors?	
m. How long will data be retained?	
n. How will data be stored?	
o. How will data be deleted?	

[1] Lawful bases for processing are set out in Article 6 GDPR

p. Are there any issues of public concern that need to be considered? If so, please clarify	
q. what affect could the processing have on individuals?	
r. What is it intended to achieve by processing the personal data in this way?	
s. What are the intended benefits of the processing?	
t. What training will staff be given before the project commences?	
u. Have staff been asked to revisit LAB data protection policies in advance of the project?	

Step 3. Consultation Process

The views of relevant stakeholders should be sought unless there is a valid and recorded reason not to do so.	
Who are the potential stakeholders for this project? (list internal and external ones)	
Indicate if you will/ will not seek stakeholder views	
Indicate why it is/ is not appropriate to seek stakeholder views	
If it is appropriate, how will you seek individuals' views?	
If it is appropriate, when will you seek individuals' views?	
Do you plan to consult information security or other experts? (e.g. legal practitioners other than those working for the LAB, academics)	
Is a general public consultation process necessary?	

Step 4. Assess Necessity and Proportionality

Describe compliance and proportionality measures	
Is the intended processing likely to achieve the project purpose?	
Is there another way to achieve the same outcome?	
How will the project prevent function creep?	
How will you ensure data quality	
How will you ensure data minimisation?	
What will individuals be told about the processing?	
How will data subject rights be signaled and protected?	

Step 5. Identify and Assess Risks

Describe any source of risk and how it might impact on individuals. For each risk include the associated i) compliance and ii) corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6. Identify measures to reduce risk

From Step 5 above, identify additional measures that the project team could take to reduce or eliminate medium or high risks.				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7. Sign-off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the DPC before going ahead
DPO advice provided:		DPO should advise on compliance, step 7 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, reasons must be provided
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA