Third-Party Data Request Procedure

Ref: IC003, v1

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	Third-Party Data Request Procedure
Current Version	v1
Document Reference Number	IC003
Date Effective From	15th May 2024
Date Effective Until	14th May 2026
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	21/3/2024	New procedure	Brian Moss	Gareth Clifford

1. Purpose

This document sets out the procedure to be followed when a third-party requests client / staff data from the Legal Aid Board. Third parties such as law enforcement or investigatory agencies can request such data. However, there is no legal obligation on the Board (or other agency) to provide such data.

These types of requests are different from requests for data from a person to whom the data belong, i.e. data subject access request. Information on those requests is contained in the Board Data Protection Policy.

Note: The procedure for responding to requests for client file or CCTV footage is similar. Pease read below for each different pathway.

2. Client File Request Procedure

In cases of data requested by the **Garda Síochána / regulatory agency**:

1. Client file data collected by the LAB can be used for investigation of specific crime under section 41(b) of the Data Protection Act 2018, i.e. can be disclosed to the Garda Síochána/ regulatory agency for the purpose of investigating a possible crime on/against LAB premises where such data are requested.

2. Generally, there is no legal obligation on the LAB to provide the data sought. The LAB can choose to do so. If it does disclose, the LAB must be satisfied that the processing is both necessary and proportionate.

3. If it does disclose data, the LAB must be satisfied as data controller that the data will be properly managed by the Garda Síochána/ regulatory agency.

4. If a court order / warrant is in place, the LAB must disclose the data sought. If either of the latter are in place, they also provide protection for the LAB in terms of data management and expectations once the material is disclosed to the Garda Síochána/ regulatory agency.

5. Where no court order / warrant is in place, a request for disclosure of data from the Garda Síochána can be in verbal form initially but the LAB staff member involved in the incident/ request must secure a formal, written request from the Garda Síochána/ regulatory agency. This is necessary before any final decision on the request can be made. Please note, the Garda Síochána possesses a template form for such requests, including a space to confirm the LAB consent to the request. Other agencies may possess a different form.

6. This written request will then be considered and decided upon by the LAB Data Protection section.

7. Where the Data Protection section decision is to grant the client file request, it will make arrangements only for the relevant parts of the client file to be accessed. This is in line with GDPR and will be decided in conjunction with Directorate staff who hold all files (e.g. Civil Operations or FMS staff). The whole contents of a client file should not be disclosed (e.g. if P1 in an FMS case has made an allegation of criminal conduct about P2, data on their finances, dependants, property, etc.) unless the grounds for this have been set out

by the Garda Síochána/ regulatory agency and the Data Protection section is satisfied with this. This is in line with GDPR principles.

8. Any client file data should be transferred to the Garda Síochána/ regulatory agency using SecureMail in the first instance. Failing that, the next preference is for ShareFile. ShareFile is available to all business units in the Legal Aid Board. Instructions for using ShareFile are set out on iLAB.

9. To transfer a file using ShareFile, the necessary client data should first be uploaded to the LAB network. This should be done in line with the Legal Aid Board IT Usage Policy. This means transfer of data from EOS/FMS case tracking system to the Home Drive of the LAB staff member.

10. Once uploaded, the client file data should be sent by the LAB staff member involved using ShareFile and only to a confirmed work email address for the investigating Garda/ regulatory agency, not a general email address.

11. While ShareFile does record access of files uploaded and shared, the Data Protection section will email the investigating garda asking them to confirm receipt. It will copy in the LAB staff member involved in the incident / the request.

12. In the event that the Garda Síochána/ regulatory agency cannot access ShareFile, the LAB staff member involved in the incident must inform the Data Protection section at dataprotetion@legalaidboard.ie.

13. The Data Protection section will then make arrangements with the IT Unit to transfer the relevant client file data to a password-protected USB stick. That will then be sent directly to the investigating garda/ regulatory agency staff member using a courier arranged by IT / Data Protection, reminding them of the GDPR obligations, and including the original written request from the Garda Síochána/ regulatory agency signed by the Data Protection section. If the original request from the Garda Síochána/ regulatory agency was not provided, the Data Protection section will include the email and an attachment on LAB headed paper confirming its consent to releasing the material.

14. If issued by USB, the password for the USB will be sent in an email to the investigating garda/ regulatory agency, outlining they should expect the materials by courier and the other contents of the courier-delivered package.

15. Section 70 of the Data Protection Act 2018 allows for the Garda Síochána/ regulatory agency to process the data. Where disclosed, any LAB data given to the Garda Síochána would then be subject to usual GDPR obligations.

16. The Garda/ regulatory agency request for client data will be recorded by the LAB Data Protection section, the data disclosed will be monitored, and it will undertake any data governance action where necessary.

3. CCTV Request Procedure

In cases of data requested by the **Garda Síochána / regulatory agency**:

1. CCTV data collected by the LAB can be used for investigation of specific crime under section 41(b) of the Data Protection Act 2018, i.e. can be disclosed to the Garda Síochána/ regulatory agency for the purpose of investigating a possible crime on/against LAB premises where such data are requested.

2. Generally there is no legal obligation on the LAB to provide the data sought. The LAB can choose to do so. If it does disclose, the LAB must be satisfied that the processing is both necessary and proportionate.

3. If it does disclose data, the LAB must be satisfied as data controller that the data will be properly managed by the Garda Síochána/ regulatory agency.

4. If a court order/ warrant is in place, the LAB must disclose the data sought. If either of the latter are in place, they also provide protection for the LAB in terms of data management and expectations once the material is disclosed to the Garda Síochána/ regulatory agency.

5. Where no court order/ warrant is in place, a request for disclosure of data from the Garda Síochána can be in verbal form initially but the LAB staff member involved in the incident/ request must secure a formal, written request from the Garda Síochána/ regulatory agency. This is necessary before any final decision on the request can be made.

6. This written request will then be considered and decided upon by the Data Protection section.

7. Where the Data Protection section decision is to grant the CCTV request, it will make arrangements for the CCTV footage to be accessed. Footage should only be accessed by or on the prior approval of the Data Protection section. It should not be accessed by a local business unit staff without first consulting the Data Protection section.

8. As of March 2024, the CCTV companies download CCTV footage directly from a local PC. This is done using USB sticks. The USB sticks should be retained only by the LAB staff member involved in the incident/ the request.

9. Any CCTV footage downloaded should be only be transferred to the Garda Síochána/ regulatory agency using ShareFile. ShareFile is available to all business units in the Legal Aid Board. Instructions for using ShareFile are set out on iLAB.

10. To transfer a file using ShareFile, the CCTV footage should first be uploaded to the LAB network. This should be done in line with the Legal Aid Board Computer Usage Policy. This means transfer of data from USB to ShareFile/ the Home Drive of the LAB staff member involved should be done by IT only.

11. Once uploaded, the footage should be sent by the LAB staff member involved using ShareFile and only to a confirmed work email address for the investigating Garda/ regulatory agency.

12. While ShareFile does record access of files uploaded and shared, the Data Protection section will email the investigating garda asking them to confirm receipt. It will copy in the LAB staff member involved in the incident/ the request.

13. In the event that the Garda Síochána/ regulatory agency cannot access ShareFile, the LAB staff member involved in the incident must inform the Data Protection section at dataprotetion@legalaidboard.ie.

14. The Data Protection section will then make arrangements with the IT Unit to transfer the footage to a password-protected USB stick. That will then be sent directly to the investigating garda, reminding them of the GDPR obligations, and including the original written request from the Garda Síochána/ regulatory agency signed by the Data Protection section.

15. If issued to the investigating garda by ShareFile, the LAB will make CCTV footage available to the Garda Síochána/ regulatory agency for a period of 30 days only from date of issue.

Both client file and CCTV footage requests should be responded to within one month of receipt.

In cases of data requested by the **other parties**:

- A third-party on behalf of a data subject should have the consent of the data subject e.g. an insurance company examining an incident in a LAB office;
- These will be considered on a case-by-case basis. In the case of third-party requests, those procedures above for requesting files and CCTV should be followed.
- A data subject. In the case of data subjects, a request should be recorded as a Data Subject Access Request, as per Data Subject Access Request procedure.

4. Log

In respect of law enforcement / regulatory agency requests for data or CCTV footage, a log should be retained by the Data Protection section setting out:

- Date of the request
- Person and organisation requesting
- Contact details of requester
- Description of the incident requested
- Whether a written (or just verbal) request was received
- Any relevant identifying number from the requester (e.g. PULSE number)
- Date request closed

5. 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

6. Making a Complaint

A person dissatisfied with the Board's response to matters relating to its Third Party Data Request Procedure 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

7. Monitoring, Enforcement, and Alteration

Compliance with this procedure 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 procedure. Board staff who breach this procedure may be subject to disciplinary action.

The Board will amend this procedure regularly but may amend this procedure at any time to take account of business, legislative, or organisational changes. Any changes to the procedure will be notified on iLAB.

8. Sources

Data Protection Commission (2023) DPC Guidance https://www.dataprotection.ie/sites/default/files/uploads/2023-12/CCTV%20Guidance%20Data%20Controllers_November%202023%20EN.pdf

Data Protection Commission (2022) Inquiry into An Garda Síochána IN-20-1-3 15 December 2022 https://www.dataprotection.ie/sites/default/files/uploads/2023-01/IN-20-1-3_AGS_Summary%20of%20decision%20for%20publication.pdf

Dublin City University section 41(b) requests (2023) https://www.dcu.ie/sites/default/files/inline-files/DPU%20Guide%20to%20Garda-Law%20Enforcement%20Requests%20-%20V1.0.pdf

Law Society Gazette (2020) I don't want to miss a thing- CCTV and data protection legislation https://www.lawsociety.ie/gazette/in-depth/cctv-data-protection