Australian Capital Territory

Legal Aid (Disclosure of Information) Guidelines 2022 (No 1)

Disallowable instrument DI2022–86

made under the

Legal Aid Act 1977, s 92AA (4) (Exceptions to secrecy provisions)

---

1 Name of instrument

This instrument is the *Legal Aid (Disclosure of Information) Guidelines 2022 (No 1)*.

2 Commencement

This instrument commences on the day after it is notified.

3 Disclosure of Information Guidelines

I make the 'Legal Aid Disclosure of Information Guidelines 2022' as provided in Schedule 1 of this instrument.

Shane Rattenbury MLA
Attorney-General
13 June 2022

Schedule 1

Legal Aid

Disclosure of Information Guidelines 2022

Introduction

Under section 92AA of the Legal Aid Act ('the Act'), Legal Aid ACT (the Commission) may disclose data or information about the affairs of a person. The CEO of the Commission must decide in which situations it is appropriate to make a disclosure of data or information, by balancing a range of factors in order to best protect human rights under the *Human Rights Act 2004* (ACT) ('the Human Rights Act').

The *National Legal Assistance Partnership 2020-25*, which commenced on 1 July 2020, provides quarantined Commonwealth Government funding to the Commission. As part of recipient's reporting obligations, the Commission is obliged to provide unit level data about the services provided to clients.

In some situations, for the purpose of conducting research, disclosing de-identified data or information about clients can be important to enable research which will contribute to improving the way in which the Australian legal system operates for access to justice for people into the future. Access to justice is an important part of enabling everyone's participation in the legal system to give effect to their right to recognition and equality before the law under section 8 of the Human Rights Act.

However, disclosure of data or information about the Commission's work and clients can present a risk of someone being able to identify clients and therefore is a limit on the clients' right to privacy under section 12 of the Human Rights Act. Under Section 28 of the Human Rights Act, human rights may be subject only to reasonable limits set by laws that can be demonstrably justified in a free and democratic society.

These guidelines are applicable to the Commission's disclosure of data and information in these circumstances, including under other agreements with the Commonwealth in relation to the provision of legal assistance services. These guidelines set out how the CEO of the Commission (the CEO) should assess whether a particular disclosure is permitted under the Act, and if it imposes a reasonable limit on the right. These guidelines must be followed under Section 92AA of the Act.

Stage 1 – determining the requirements of each disclosure

For disclosures made under national agreements in relation to the provision of legal assistance services (s 92AA(2)):

Under section 92AA (2) of the Act, the secrecy provisions under section 92 do not apply to disclosures made to a Commonwealth entity if:

- the disclosure is for the purpose of complying with a national agreement in relation the provision of legal assistance services, AND
- the disclosure is authorised, in writing, by the CEO under these guidelines AND
- the CEO is satisfied that the Commonwealth entity is required to apply the Australian Privacy Principles (APPs), AND
- the disclosure relates to information, communications, or documents made on or after 1 July 2021.

Therefore, disclosures made to comply with requirements under the national agreement in relation to the provision of legal assistance services are permitted by the Act.

Data collected prior to 1 July 2021 must not be disclosed.

Under national agreements made in relation to the provision of legal services, the entities to which disclosures will be made are typically the Commonwealth Attorney-General's Department, the Australian Bureau of Statistics (ABS), or both. As Australian Government agencies, these entities are bound by the APPs.

For disclosures to other Commonwealth entities, the CEO must be satisfied that the entity is required to apply the APPs.

Found in the *Information Privacy Act 1988* (Cth), the APPs are eleven binding principles which govern standards, rights, and obligations around the collection, use and disclosure of personal information.

Particularly relevant in this context are APP 1, which requires an entity to manage personal information openly and transparently; APP 6, which outlines the circumstances in which an entity may use personal information that it holds; and APP 11, which requires an entity to take reasonable steps to protect personal information it holds from misuse, interference, unauthorised access, loss, or disclosure.

The APPs apply to all entities which are:

- an agency or organisation
    - 'organisation' included sole traders, body corporates, partnerships, unincorporated associations, and trusts
- Australian Government agencies. This includes:
    - Ministers,
    - Departments,
    - any bodies established for public purposes under Commonwealth enactments,
    - a body established by the Governor-General, or by a Minister, other than by or under a Commonwealth enactment,
    - organisations registered under the Fair Work (Registered Organisations) Act 2009, or their branches,
    - a person holding or performing the duties of an appointment, being an appointment made by the Governor-General, or by a Minister, other than under a Commonwealth enactment,
    - a federal court,
    - the Australian Federal Police
    - a Norfolk Island agency,
    - an eligible hearing service provider, or
    - the service operator under the *Healthcare Identifiers Act 2010* (s 6(1))

The APPs do NOT apply to:

- State and Territory authorities, including
    - Ministers,
    - Departments/Directorates
    - Bodies established or appointed for a public purpose under State or Territory law,

    - Bodies established or appointed by Governors, the ACT Executive, or State Ministers
    - A State or Territory Court
    - A person holding or performing the duties of an appointment made under State or Territory Law, or made by a Governor, Executive or Minister
- Registered political parties,
- Small business operators (generally defined as an organisation with an annual turnover of less than $3,000,000 in a financial year)
- Service providers under a Commonwealth contract

The CEO must be satisfied that the use of the data or information is proportionate to the limitation on the right to privacy, that the entity has appropriate data management frameworks in place, and that any necessary conditions are imposed on the disclosure.

The CEO must also consider whether any other rights under the Human Rights Act, besides the right to privacy, may be limited by a disclosure.

The CEO must therefore still consider the questions raised in Stages 2 and 3.

For disclosures that are for the purpose of conducting research in relation to improving access to justice or provision of legal assistance services:

Under section 92AA (3) of the Act, the secrecy provisions under section 92 do not apply to disclosures made to an entity if

- the disclosure is for the purpose of conducting research in relation to improving access to justice, or the provision of legal assistance services; AND
- for the disclosure to a Commonwealth entity—the CEO is satisfied that the Commonwealth entity is required to apply the APPs, AND
- the disclosure is authorised, in writing, by the CEO under these Guidelines, AND
- the disclosure relates to information, communication or documents made on or after 1 July 2021.

Therefore, the following matters must be considered by the CEO:

<u>Is the entity required to apply the APPs or other privacy principles?</u>

For disclosures to Commonwealth entities, the CEO must be satisfied that the entity is required to apply the APPs (set out above).

For non-Commonwealth entities, the CEO does not need to be satisfied that the entity is required to apply the APPs.

However, the CEO should determine which privacy legislation, if any, is binding upon the entity seeking disclosure. This may include State or Territory legislation, regulations specific to a particular profession, and other internal regulations or guidelines (e.g. a university's research).

Of particular note are the ACT's Territory Privacy Principles (TPPs). Under the *Information Privacy Act 2014* (ACT), the TPPs apply to all ACT public sector agencies and contracted service providers (including subcontractors). They are substantially similar to the APPs.

If the entity has been selected by a State or Territory or Commonwealth government entity to complete the project, determine why.

The CEO must be satisfied that the legal and policy requirements upon the non-Commonwealth entity seeking disclosure are sufficient to ensure adequate privacy protection. This may include assessing the data security and internal frameworks of the entity under Stage 2.

Is the disclosure for the purpose of conducting research in relation to improving access to justice, or the provision of legal assistance services?

The CEO must consider:

- Is the objective related to research promoting access to justice or the provision of legal assistance services?
- What is the potential significance of the research to access to justice or the provision of legal assistance services?
- Is the research related to government initiatives? If so, how will it inform them? (E.g., information on certain demographics, policy development, submissions to Parliament.)
- Has the entity provided evidence or information to justify how the data will contribute to the research? Will the data be required or valuable to achieve the research?

However, even if the research does not result in immediate outcomes, it may nevertheless be of significance. (e.g., academic research on access to justice mechanisms).

Overall, the CEO must be satisfied that the project has a legitimate research objective related to improving access to justice or the provision of legal assistance services, and that the disclosure of has a rational connection to achieving this objective.

Has the entity defined the scope of the research for which it seeks to use the disclosure?

The project for which the entity seeks to use the disclosed information must be clearly defined and specify if any data sought will be unit level data, which would reveal information on characteristics of clients, or aggregated.

Among any other matters the CEO may consider relevant, the CEO must consider:

- With what level of detail will unit-level data be disclosed? If a high level of detail, does it require steps to be taken to ensure anonymity?
- Has the entity defined the end product of the project using the data (e.g., a report, an academic publication, etc.)? Will it be publicly available?
- How will the data be represented in the end product? (E.g., data tables aggregated data, or only modelling or conclusions?)

Overall, the CEO must be satisfied that the entity has clearly outlined the research project, and that the CEO has sufficient information to understand and consider the project and how the information will be used.

Is the use of the disclosed information proportionate to the right to privacy?

The CEO must evaluate the data to be disclosed against the right to privacy under the ACT Human Rights Act:

- Is there a risk a person or persons may be identifiable from the end product representation of data?
- Have other datasets been provided to the entity or released publicly in the past? Is there a risk that a person or persons may be identifiable by combining the end product with past datasets?
- What sensitivities are there about the information could be discerned about a person, if a person or persons was identified?
    - Sensitive data may include racial or ethnic origin, mental health or disability status, religious beliefs, criminal records, and more. Would a narrower dataset be sufficient to use to achieve the project's objective?
- Could the dataset or presentation of the data be modified to reduce the risk of identification? (E.g., not including postcodes or other identifiers etc.)
- Are there other safeguards available to prevent identification?

The CEO must be satisfied that the risk or limit on the right to privacy proportionate to the importance of the project's objective.

The greater the limitation on the right to privacy, the greater the justification for the limitation will need to be in order to be proportionate.

If the CEO has determined that other rights under the Human Rights Act may be limited by the disclosure, a further analysis of proportionality must be carried out.

Stage 2 – Assessing the entity's data management maturity

It is ultimately the entity's responsibility to properly safeguard the data's security. However, it is appropriate for the CEO to consider whether the entity demonstrates awareness and application of data governance and management principles.

Does the entity have a data governance framework?

- Has the entity's framework been provided to the CEO?
- Has the framework been recently reviewed or updated? If not, it is recommended that it be reviewed for currency.
- Is information about their framework publicly accessible?

The CEO must be satisfied that the data governance framework is fit for purpose, up to date, and accessible. The CEO must be aware of any other applicable frameworks to the entity, including Privacy Principles, University research requirements, etc.

Is data safely stored by the entity?

The CEO must consider:

- How is the data stored by the entity?
- Has the entity advised who in its staff will have access to the data?
- Does the entity have clear procedures and expectations for employees and volunteers about data management access and responsibilities? (E.g., a code of conduct)
- Does the entity have procedures to ensure that individuals who have data management responsibilities understand and have capacity to fulfil their responsibilities? (E.g., compulsory training, security clearances)
- Does the entity have physical security protocols to restrict data access?
- Does the entity have IT security protocols to restrict data access? (E.g., particular passwords, limited access to data software)

- Does the entity have procedures in place to monitor and respond to security risks? Does it have accountability mechanisms to ensure proper management?
- Has the entity provided information about what will be done with the data after the project is completed? (E.g., destruction, retention, transfer to other entities)
- Does the entity have a data breach response plan? Is it publicly available? If not, discuss with the entity.

Overall, the CEO must be satisfied that the entity has awareness of its data management requirements, and appropriate safeguards and protocols in place to manage the data safely.

If major issues are identified, the data should not be disclosed. However, if minor issues are identified, discuss them with the entity, and continue to Stage 3 to consider further limitations on disclosure of the data.

If no issues are identified in Stage 2, the CEO does not need to progress to Stage 3. If the CEO is satisfied that the disclosure meets all legislative requirements and is consistent with the Guidelines, the CEO may authorise the disclosure in writing.

Stage 3 – Terms of Data Disclosure

This Stage should only be considered if the CEO considers that disclosure is appropriate under Stage 1, and if minor issues in relation to maturity are identified under Stage 2.

What terms would be appropriate to manage issues of data management identified under Stage 2?

If the CEO is unsatisfied with minor elements of the entity's data management, it must consider if terms could be applied to the disclosure to ensure it is safely and appropriately disclosed. Consider:

- What would be appropriate to manage issues relating to specific datasets? E.g., making undertakings, imposing conditions on the use of data, etc.
- How will the datasets be provided to the entity? Is it a secure method?
- Is it possible to put limits on how the data is stored and used after the completion of the project?
- Can the CEO require the entity to provide a copy of the end product for review prior to release?
- What are the CEO's rights to the data once the disclosure is made? Consider terms detailing these rights.

Overall, the CEO must be satisfied that any issues identified during Stage 2 can be addressed by terms or restrictions on the use of the data. If the CEO is not satisfied that disclosure of the data is appropriate, the CEO must not disclose the data.

If the CEO is satisfied that the disclosure meets all required legislative requirements and is consistent with these Guidelines, the CEO may authorise the disclosure in writing.