Clarity Insight Privacy Policy

1. About this policy

This Privacy Policy explains how Clarity Insight Pty Ltd collects, uses, discloses and protects personal information in line with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

By dealing with Clarity Insight or using our website, you agree to your personal information being handled as set out in this policy.

2. Who we are and how to contact us

- Organisation name: Clarity Insight Pty Ltd
- Trading name: Clarity Insight
- Email: privacy@clarityinsight.au

3. What personal information we collect

The information we collect depends on how you interact with us. It can include:

- Name, job title and role
- Organisation and business contact details (email, phone, address)
- Information about your organisation's programs, services and funding priorities
- Feedback and information you provide in meetings, workshops, surveys or emails
- Limited information about program stakeholders or participants where needed for grant, evaluation or reporting work (preferably de-identified or aggregated)
- Technical data when you use our website (such as IP address, browser type, pages visited)

We do not routinely collect sensitive information. Where sensitive information (for example, Indigenous status or health information) is necessary and directly relevant to our work, we only collect it with consent or where permitted by law.

4. How we collect personal information

We collect personal information:

- Directly from you (for example, when you contact us, attend a workshop or provide documents)
- From client organisations and partners (for example, staff contact lists, program documentation, de-identified or aggregated program data)
- Automatically through our website and online services using cookies and similar technologies (for analytics and security)

Where we receive personal information about you from another party, we rely on them having the right to share it and, where practicable, we ensure you are aware this has occurred.

5. Why we collect and use personal information

We handle personal information only where it is reasonably necessary for our work, including:

- Delivering services: grant strategy and applications, program design and refinement, monitoring and evaluation, reporting to clients and funders
- Managing relationships: responding to enquiries, managing engagements and contracts, coordinating workshops and consultations
- Business operations: invoicing and payments, internal records, IT and cyber-security, compliance and risk management
- Service improvement: reviewing the effectiveness of strategies and programs, analysing de-identified data to understand trends, improving our tools and processes
- Communications: sending information about funding trends, resources or events where you would reasonably expect this or have opted in (you can opt out at any time)

6. Legal basis for handling personal information

Depending on the situation, we rely on one or more of the following:

- Performing a contract or engagement with you or your organisation
- Complying with legal and regulatory obligations
- Our legitimate interests in operating and improving our services in ways that are consistent with your reasonable expectations and privacy rights
- Your consent, where required (for example, for some evaluation activities or direct marketing)

7. When we disclose personal information

We do not sell personal information.

We may disclose personal information to:

- Client organisations and agreed partners where necessary to deliver contracted work
- Funding bodies, as part of agreed reporting and deliverables
- Service providers that support our operations, such as:
- secure cloud document storage and collaboration tools
- email and calendar services
- analytics and security tools
- accounting, invoicing and payment systems

These providers are engaged on the basis that they only use personal information to provide their services to us, protect it appropriately, and comply with privacy requirements.

We may also disclose information where required or authorised by law, court or tribunal order, or where reasonably necessary to establish, exercise or defend legal claims.

8. Overseas disclosure

We primarily store information in Australia. Some service providers we use may store or process information on servers located outside Australia (for example, in the United States, the European Union or the Asia-Pacific region).

Where personal information may be accessed from or processed in another country, we take reasonable steps to ensure it is protected in a way that is substantially similar to the APPs and is only used for agreed purposes.

If you prefer that your information is not processed offshore for a particular engagement, contact us and we will discuss available options. This may limit which tools or services can be used.

9. Data security and retention

We take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, modification or disclosure, consistent with APP 11. Measures include:

- Role-based access controls for systems containing personal information
- Use of reputable cloud platforms with encryption in transit and at rest (where available)
- Limiting access to staff and contractors who need information for their work
- Regular updates and security maintenance on core systems
- Secure destruction or de-identification of information when it is no longer required

We keep personal information only for as long as needed for the purposes described in this policy or as required by law (for example, up to 7 years for most client and financial records). After this, information is securely destroyed or de-identified.

10. Access to and correction of personal information

- You can request access to personal information we hold about you, or ask us to correct it if you believe it is inaccurate, out of date, incomplete or misleading.

To do so, email privacy@clarityinsight.au with:

- your name and contact details

what information you are seeking or wish to correct

We will respond within a reasonable time. In some cases we may need to refuse access or correction (for example, where giving access would unreasonably impact others' privacy or is restricted by law). If this happens, we will explain why, subject to legal constraints.

11. Data breaches

If a data breach occurs that is likely to result in serious harm to individuals, we will comply with the Notifiable Data Breaches (NDB) scheme under the Privacy Act.

This may include:

- taking urgent steps to contain and assess the breach
- notifying affected individuals as soon as practicable, with information about what happened and what they can do
- notifying the Office of the Australian Information Commissioner (OAIC) as required

12. Complaints and questions

If you have a question or concern about how your personal information has been handled, contact:

Email: privacy@clarityinsight.au

Include:

- your name and contact details
- what happened and when
- what outcome you are seeking

We will investigate and respond within a reasonable period.

If you are not satisfied with our response, you can contact the Office of the Australian Information Commissioner (OAIC):

- Website: https://www.oaic.gov.au
- Phone: 1300 363 992

13. Changes to this policy

We may update this Privacy Policy from time to time to reflect changes in law, guidance or our practices.

The latest version will always be available on our website and will show the "Last updated" date at the top.