



CSI Website Privacy Policy

Document number: CDPOL_027 **Issue/Revision:** Issue 1, Revision 0

Effective date: 2 September 2026 **Document owner:** Privacy Officer

Policy summary. CSI uses personal information to deliver credible certification and audit services, meet scheme and legal obligations, protect certification integrity and operate its business. CSI does not sell personal information, does not use third-party web tracking, and does not make certification decisions solely by automated means.

1. Who we are and what this policy covers

Certification Solutions International Pty. Ltd. (ABN 49 123 368 650) (CSI, we, us or our) is an Australian conformity-assessment and product-certification body. Our registered business is based in New South Wales, Australia, and we provide certification, assessment, audit and related services internationally.

This policy explains how CSI collects, holds, uses, discloses, transfers, protects and disposes of personal information in connection with our website, enquiries, quotations, applications, certification and surveillance activities, audits, complaints and appeals, events, recruitment, contracting, supplier relationships and other business dealings.

It applies to clients and prospective clients; certificate holders; manufacturers and suppliers; directors, employees and representatives of organisations; auditors, inspectors, technical experts, committee and panel members; laboratory and service-provider contacts; complainants, witnesses and appellants; job applicants; website visitors; and other people who deal with CSI. Separate collection notices, contractual terms or workforce notices may provide additional information for a particular activity. If they conflict with this policy, the more specific notice applies to that activity to the extent permitted by law.

CSI is usually the organisation responsible for deciding why and how personal information is handled. In some engagements CSI may process information on documented instructions from another organisation; the relevant contract or collection notice will explain that role.

2. Our privacy commitments

CSI manages personal information lawfully, fairly, transparently and only for defined purposes. We seek to collect only what is reasonably necessary, keep it accurate, protect it in proportion to its sensitivity, restrict access to people with a business need, and retain it only for as long as justified.

Our principal Australian obligations arise under the Privacy Act 1988 (Cth), including the Australian Privacy Principles. Where another privacy or data-protection law applies, including in New Zealand, the European

Certification Solutions International Pty Ltd ABN 49 123 368 650, PO Box 904 Fairfield, NSW 1860 Australia,

Ph: +61 2 9728 7608 Email: admin@csi-certification.com Web: www.csi-certification.com

External Document - Uncontrolled when downloaded/printed | CDPOL_027 | Issue 1, Rev 0 | Page 1 of 8

Economic Area, the United Kingdom, Canada, Singapore, California or another jurisdiction, CSI also applies the rights and safeguards required by that law.

Where it is lawful and practicable, a person may make a general enquiry anonymously or using a pseudonym. Identification will normally be required where it is necessary to provide certification services, verify competence or authority, manage safety or travel, comply with a scheme or legal requirement, investigate a complaint or protect the integrity of a certification decision.

3. Personal information we collect

The information CSI collects depends on the relationship and service. It may include:

- identity and contact details, such as name, job title, employer, postal address, email address, telephone number, signature and preferred language;
- professional and competence information, such as qualifications, licences, training, employment history, experience, authorisations and conflict-of-interest declarations;
- certification and audit information, including applications, correspondence, attendance records, interview notes, audit evidence, photographs or recordings where authorised, findings, corrective-action records, complaints, appeals, witness statements and certification history;
- business and transaction information, such as quotations, contracts, purchase orders, invoices, payment status, bank details supplied for payments, insurance information and records of services provided;
- site-access, travel and safety information, which may include identification documents, itinerary details, emergency contacts, dietary or accessibility requirements, and limited health or safety information where reasonably necessary;
- recruitment, employment and contractor information, subject to applicable workforce laws and separate internal notices;
- communications and technical information, such as emails, meeting records, call notes, device and browser information, IP address, website logs, pages viewed, timestamps, referring pages and enquiry-form content; and
- information required by a certification scheme, scheme owner, accreditation body, regulator, court, tribunal or other lawful authority.

CSI does not intentionally collect sensitive or special-category information unless it is reasonably necessary and a lawful basis or exception applies. Depending on the circumstances, this may include health or accessibility information, professional-association membership, criminal-history information, biometric information used for secure site access, or information revealing racial or ethnic origin, religious belief or political opinion. We seek express consent where required and apply additional safeguards.

4. How we collect information

We usually collect information directly from the individual through our website, forms, email, telephone or video calls, meetings, audits, inspections, applications, contracts, event registrations, recruitment processes and other dealings.

We may also receive information from the organisation a person represents; a certificate holder, manufacturer or supplier; auditors, technical experts, laboratories or subcontractors; referees and recruitment providers; scheme owners, accreditation bodies, regulators or government agencies; professional and public registers; publicly available sources; or another person involved in a complaint, appeal, investigation or certification activity.

If someone gives CSI personal information about another person, they should have authority to do so and should direct that person to this policy or the relevant collection notice. Where required, CSI will take reasonable steps to notify a person when information is obtained indirectly. If required information is not provided, CSI may be unable to respond, enter a contract, arrange an audit, assess competence, make or maintain a certification decision, or meet a scheme or legal obligation.

5. Why we use personal information and our legal bases

CSI uses personal information only when there is a valid purpose and lawful basis. The bases available depend on the jurisdiction and may include consent, steps requested before entering a contract, performance of a contract, compliance with law or a scheme obligation, protection of vital interests, and CSI's or another party's legitimate interests where those interests are not overridden by the individual's rights.

Purpose	Typical lawful basis
Respond to enquiries, prepare proposals, onboard clients and administer contracts	Pre-contract steps; contract; legitimate interests in operating CSI's services
Plan and conduct assessments, audits, testing, technical review, certification decisions and surveillance	Contract; legal or scheme obligation; legitimate interests in credible and impartial certification
Verify competence, authority, identity, independence and conflicts of interest	Contract; legal or accreditation obligation; legitimate interests in certification integrity
Maintain certification records and publish or verify certificate status	Contract; legal or scheme obligation; legitimate interests of regulators, markets and users of certification
Manage complaints, appeals, investigations, safety, fraud, misuse of marks and legal claims	Legal obligation; legitimate interests; vital interests; establishment, exercise or defense of legal claims
Invoice, receive or make payments, keep accounts and obtain professional advice	Contract; legal obligation; legitimate business interests
Operate, secure, diagnose and improve our website, systems and services	Legitimate interests in secure and reliable business systems
Send service notices and, where permitted, relevant business updates	Contract or legitimate interests for service notices; consent or other lawful permission for marketing
Recruit, engage and manage personnel, auditors, experts and suppliers	Pre-contract steps; contract; legal obligation; legitimate interests; consent where required

Where CSI relies on legitimate interests, those interests include delivering reliable conformity-assessment services; safeguarding impartiality, competence and the integrity of certification; protecting systems, people and property; preventing fraud and misuse; maintaining records and evidence; improving services; and communicating with business contacts. CSI balances these interests against the likely impact on individuals. Consent may be withdrawn at any time, but withdrawal does not affect processing already lawfully undertaken.

6. Certification confidentiality and public information

Confidentiality is central to CSI's certification work. Access to application, technical, audit and decision records is limited according to role, scheme requirements and need to know. Auditors, technical experts, panel members and service providers are subject to confidentiality and information-security obligations appropriate to their work.

Certification is also an assurance activity in which specified information may need to be verified or made public. CSI may publish or disclose a certificate holder's organisation name, trading name, manufacturing or certified-site details, certificate number, product or service scope, applicable standards or schemes, certificate status, suspension, withdrawal, expiry and related conformity information where required or permitted by a scheme, accreditation body, regulator, contract or law. CSI limits personal information in public registers and certificates to what is necessary for accountability and verification.

CSI's authorised personnel make certification and surveillance decisions in accordance with applicable scheme and accreditation rules. CSI does not make decisions producing legal or similarly significant effects about individuals solely by automated means.

7. Digital and AI-assisted tools

CSI may use approved digital and AI-assisted tools to support administration, search, translation, transcription, drafting, summarisation, document classification and quality checks. These tools support, but do not replace, professional judgement, technical review or certification decision-making.

When personal information is handled through such tools, CSI seeks to minimise or de-identify it where practicable, limits access, considers the provider's security and contractual terms, and applies human review. CSI will not intentionally use client personal information to train a publicly available general-purpose model unless the individual or responsible client has been clearly informed and a valid lawful basis applies.

8. When we disclose information

CSI may disclose personal information, to the extent reasonably necessary to:

- the client, certificate holder, manufacturer, supplier or other organisation connected with the relevant engagement;
- CSI personnel, contracted auditors, inspectors, technical experts, committee or panel members, laboratories and other conformity-assessment providers;
- scheme owners, accreditation bodies, regulators, government authorities and public or industry registers where required or authorised;

- technology, cloud hosting, website, email, communications, records-management, cybersecurity and support providers;
- banks, payment providers, accountants, insurers, travel providers, couriers, translators, professional advisers, debt-recovery providers and other business service providers;
- law-enforcement bodies, courts, tribunals or other parties when required or authorised by law, or when reasonably necessary to protect safety, rights, property or certification integrity; and
- a purchaser, successor or adviser involved in a proposed or completed corporate transaction, subject to appropriate confidentiality and legal safeguards.

CSi does not sell personal information for money. CSi also does not share personal information for cross-context behavioural advertising as those concepts are defined under applicable United States state privacy laws. If our practices materially change, we will update this policy and provide any required opt-out mechanism before the change applies.

9. International handling and transfers

CSi is based in Australia and performs international certification activities. Personal information may therefore be accessed, used, stored or disclosed outside the country in which it was collected. This can occur when the client, manufacturer, audit site, auditor, technical expert, laboratory, scheme owner, accreditation body, regulator or technology provider relevant to an engagement is located overseas.

Likely recipient or service locations include Australia, New Zealand, China, India, Malaysia, Singapore, the United Kingdom, countries in the European Economic Area and the United States. Additional project-specific locations may apply where a client, manufacturer, audit site, laboratory or competent authority is located. Where practicable, CSi identifies those additional countries in the relevant proposal, application, collection notice or engagement correspondence. A current description of likely overseas locations for a particular matter is available from the Privacy Officer.

CSi takes safeguards required by applicable law. These may include due diligence, access controls, confidentiality and data-processing terms, contractual requirements based on the Australian Privacy Principles, New Zealand comparable-safeguard requirements, approved standard contractual clauses for EEA or UK transfers, transfer risk assessments, data minimisation, encryption and other technical or organisational controls. Overseas laws may permit authorities to access information in circumstances different from those applying in the country of collection.

10. Website and online enquiries

When a person visits our website, the web server or hosting provider may automatically create basic technical and security logs, such as IP address, requested page, date and time, browser information and error or security events. CSi uses this limited information only to deliver, maintain and protect the website, diagnose faults and investigate suspected misuse.

CSi does not use third-party web tracking or behavioural-advertising technologies. Information submitted through an online enquiry is handled in the same way as an enquiry made by email, telephone or other direct contact.



Our website may link to third-party sites. CSI is not responsible for their content or privacy practices, and visitors should review the relevant third party's privacy information.

11. Direct marketing and business communications

CSI may send operational messages needed to manage an enquiry, application, audit, certificate, surveillance activity, account, complaint, appeal or contract. These are service communications rather than marketing.

Where permitted, CSI may also send information about relevant certification services, standards, training, events or industry developments. CSI will obtain consent where it is required and every electronic marketing message will provide a simple way to unsubscribe. An individual may opt out at any time by using the unsubscribe function or contacting the Privacy Officer. CSI will action the request within the period required by law and may retain a minimal suppression record so that the preference is respected.

12. Storage, security and data breaches

CSI holds information in electronic systems and, where necessary, paper records. We use administrative, technical and physical safeguards appropriate to the nature of the information and the risk, such as role-based access, authentication controls, backups, secure configuration, confidentiality obligations, provider assessment, staff awareness, incident response and secure disposal. No transmission or storage method is completely secure, and CSI cannot guarantee absolute security.

If a privacy or security incident occurs, CSI will assess and contain it, take remedial action, document the response and notify affected people, regulators, clients, scheme owners or other parties where required by applicable law or contract.

13. Retention and disposal

CSI retains personal information only for as long as it is reasonably needed for the purpose collected and to satisfy certification-scheme, accreditation, surveillance, contractual, tax, insurance, limitation-period, complaint, appeal, investigation and legal requirements.

Certification and assessment records are generally retained for the active certification period and for the longer period required by the applicable scheme, accreditation rule, legal limitation period or record-control procedure. Enquiry and unsuccessful-application records are kept only for a reasonable follow-up and accountability period unless a longer period is required. Basic website server and security logs are retained only for a limited operational period set by CSI or the hosting provider. When information is no longer required, CSI takes reasonable steps to securely destroy it or de-identify it, subject to lawful backup and archival cycles. Further information about the criteria applicable to a particular record is available from the Privacy Officer.

14. Accuracy

CSI takes reasonable steps to keep personal information accurate, complete, relevant and up to date, having regard to how it will be used. Individuals and client organisations should tell CSI when relevant contact, authority, competence, site or other personal details change.

15. Your privacy rights

Depending on the law that applies, an individual may have the right to:

- know whether and how CSI handles their information and obtain access to it;
- request correction of inaccurate or incomplete information;
- request deletion or de-identification, subject to certification, legal and other permitted retention requirements;
- restrict or object to particular processing, including direct marketing;
- withdraw consent where consent is the basis for processing;
- receive certain information in a portable format;
- opt out of sale, sharing or targeted advertising where such activities occur and the relevant law applies;
- limit certain uses of sensitive personal information where applicable;
- request human review of a solely automated significant decision, although CSI does not use solely automated certification decisions; and
- complain to CSI and to the privacy or data-protection regulator with jurisdiction.

To exercise a right, contact the Privacy Officer using the details below and describe the request. CSI may ask for reasonable proof of identity or authority and may need to consult the responsible client where CSI acts only on that client's instructions. CSI will respond within the timeframe required by applicable law. A right may be limited by law, privilege, confidentiality owed to another person, safety, certification-integrity requirements, legal claims or mandatory record-retention duties. If CSI refuses or limits a request, it will explain the reason and available review or complaint options where required.

CSI will not discriminate or retaliate against a person for making a lawful privacy request. Ordinarily no fee is charged. If the law permits a fee for manifestly unfounded, excessive or unusually burdensome requests, CSI will explain it before proceeding. An authorised agent may act where the applicable law permits and their authority can be verified.

16. Regional information

Australia: Individuals may request access and correction and complain about an alleged breach of the Australian Privacy Principles. If a complaint is not resolved, the individual may contact the Office of the Australian Information Commissioner at www.oaic.gov.au.

New Zealand: Where the Privacy Act 2020 applies, individuals may exercise the applicable information privacy rights and may complain to the Office of the Privacy Commissioner at www.privacy.org.nz. CSI applies the safeguards required for disclosures outside New Zealand.

EEA and United Kingdom: Where the EU GDPR or UK GDPR applies, CSI identifies a lawful basis, provides the applicable data-subject rights, and uses a recognised transfer mechanism where required. Individuals may complain to the supervisory authority where they live or work or where the alleged infringement occurred. The UK authority is the Information Commissioner's Office at www.ico.org.uk. Details of any locally required representative will be provided in the relevant collection notice or engagement documentation.



Canada: Where Canadian private-sector privacy law applies, CSi follows applicable accountability, consent, purpose limitation, safeguarding, access and complaint requirements. Individuals may contact the Office of the Privacy Commissioner of Canada at www.priv.gc.ca or the applicable provincial regulator.

California and other United States jurisdictions: Rights described in section 15 apply only when the relevant law covers CSi and the individual or processing. CSi does not sell personal information or share it for cross-context behavioral advertising. A person may use an authorised agent and may appeal a decision where the applicable law provides that right.

Singapore and other Asia-Pacific jurisdictions: Where an applicable data-protection law requires a designated contact, consent or another lawful basis, access and correction, protection, retention limitation, breach notification or comparable protection for overseas transfers, CSi applies those requirements to the relevant processing.

17. Children

CSi's website and services are intended for organisations and adult business users. CSi does not knowingly collect children's personal information through the website. If CSi must handle such information for a lawful certification, safety or complaint purpose, it will apply heightened safeguards and obtain parental or guardian consent where required.

18. Privacy questions and complaints

Contact the Privacy Officer with a question, request or complaint. Provide enough detail for CSi to investigate, but do not send unnecessary identity documents or sensitive information by ordinary email. CSi will acknowledge and investigate the matter and seek to resolve substantiated concerns. If unresolved, the person may contact a regulator identified in section 16 or another regulator with jurisdiction.

Privacy contact	Details
Position	Privacy Officer
Organisation	Certification Solutions International Pty. Ltd. (CSi)
Email	admin@csi-certification.com
Telephone	+61 2 9728 7608
Postal address	PO Box 904, Fairfield NSW 1860, Australia
Website	www.csi-certification.com

19. Changes to this policy

CSi reviews this policy regularly and when its services, technology, information handling or legal obligations change. The current version and effective date will be published on CSi's website. CSi will give any additional notice or seek consent required by law.