Rojone Pty Ltd Policy: Privacy Policy	Document Number: PL-GEN-020	
	Revision: B	**Effective Date:** 1 May 2026
	Approved by: L Brady	**Status:** Approved
	Classification: Controlled Document — PDF Only	**Department:** Management

1.0 Amendment Record

This document is controlled under Rojone's Quality Management System. Only the latest issue is valid. Printed copies are uncontrolled.

Issue	Author	Details of Change	Date	Authorised By
A	General Manager	New document. Issued to comply with the Privacy Act 1988 (Cth) as amended, the Australian Privacy Principles, and the Privacy and Other Legislation Amendment Act 2024.	01 May 26	Managing Director
B	General Manager	Section 14 was expanded to identify third-party online tools (Google Analytics, Google Tag Manager, Google reCAPTCHA, marketing platforms, hosting/CDN), corresponding cookie categories, overseas data flows, and opt-out mechanisms. Aligned with OAIC online-tracking guidance.	24 May 2026	Managing Director

2. Table of Contents

3. Purpose

Rojone Pty Ltd ("Rojone", "we", "us", "our") is committed to protecting the privacy of the personal information it collects, holds, uses, and discloses in the course of its business activities.

This Policy sets out how Rojone manages personal information in accordance with:

- the Privacy Act 1988 (Cth) ("the Act");
- the thirteen (13) Australian Privacy Principles ("APPs") set out in Schedule 1 of the Act;
- the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth);
- the Privacy and Other Legislation Amendment Act 2024 (Cth);
- any other applicable Commonwealth, State or Territory law, including the Defence Trade Controls Act 2012 (Cth), Security of Critical Infrastructure Act 2018 (Cth), and the Spam Act 2003 (Cth); and
- Defence security requirements applicable to Rojone as a Defence Industry Security Program (DISP) member.

This Policy applies in addition to, and does not limit, Rojone's obligations under contract or law.

4.0 Scope

This Policy applies to:

- all owners, employees, contractors, consultants, agency personnel, work experience participants and other workers engaged by Rojone (collectively, "Personnel");
- all personal information collected, held, used or disclosed by Rojone, whether in physical or electronic form;
- all Rojone systems, sites, vehicles and equipment;
- Rojone's interactions with customers, suppliers, principals, prime contractors, government and Defence stakeholders, job candidates, and members of the public; and
- any third-party performing services for or on behalf of Rojone where that party may access personal information held by Rojone.

Rojone has elected to apply the Australian Privacy Principles to employee records (notwithstanding the current employee records exemption under section 7B(3) of the Act) as a matter of best practice, in anticipation of further legislative reform, and to meet the expectations of Defence and prime-contractor customers.

5.0 Definitions

In this Policy:

Term	Meaning
APPs	The Australian Privacy Principles set out in Schedule 1 to the Privacy Act 1988 (Cth).
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether recorded in a material form or not.
Data Breach	Unauthorised access to, unauthorised disclosure of, or loss of personal information held by Rojone.
Privacy Officer	The General Manager of Rojone, who is accountable for the administration of this Policy.
Sensitive Information	A subset of personal information that includes information or an opinion about an individual: • racial or ethnic origin; political opinions; membership of a political association; • religious beliefs or affiliations; philosophical beliefs; • membership of a professional or trade association or union; • sexual orientation or practices; criminal record; • health, genetic or biometric information; and biometric templates.
Eligible / Notifiable Data Breach	A Data Breach that is likely to result in serious harm to one or more individuals and where Rojone has not been able to prevent that likely risk through remedial action, requiring notification under Part IIIC of the Act.
OAIC	The Office of the Australian Information Commissioner.
Defence Information	Information relating to Defence customers, programs, personnel or capability, including security-clearance information, which is also subject to the Defence Security Principles Framework (DSPF) and DISP obligations.

6.0 Our Commitment to Privacy

Rojone recognises that the appropriate handling of personal information is fundamental to maintaining the trust of our customers, employees, partners and the public. Rojone will:

- Collect only the personal information reasonably necessary for, or directly related to, our functions and activities;
- Be transparent about why we collect personal information and how it will be used;
- Protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure using reasonable technical, physical and administrative safeguards;
- Only retain personal information for as long as it is required for a lawful purpose or as required by law; and
- Respect the rights of individuals to access and correct their personal information, and to make complaints.

7.0 Personal Information We Collect

The kind of personal information Rojone collects and holds depends on the nature of the individual's relationship with Rojone. Examples include:

7.1 Customers and Customer Representatives

- Name, position and employer;
- Business contact details (address, email, telephone);
- Purchase history, quotations, technical requirements and correspondence;
- Payment and credit-account information (excluding full credit-card numbers, which are not retained by Rojone).

7.2 Suppliers, Principals and Contractors

- Name and position of contact personnel;
- Business contact details;
- Banking details for payment processing;
- Australian Business Number, insurance certificates and other business records;
- References and pre-qualification information.

7.3 Job Candidates

- Name, address, contact details, gender (where volunteered);
- Resume, qualifications, employment history and references;
- Eligibility-to-work documentation (e.g. citizenship, visa status – relevant to Defence and export-control work);
- Pre-employment screening outcomes (criminal record, security-clearance status), collected with consent.

7.4 Employees and Contracted Workers

- Identification, contact and emergency-contact information;
- Tax file number, superannuation details, bank-account details for payroll;
- Performance, training and development records;
- WHS records, including incident, injury and rehabilitation information;
- Security-clearance applications, sponsorship and clearance-status information;
- CCTV and access-control records; and
- ICT system access logs.

7.5 Visitors to Rojone Premises

- Name, employer, vehicle registration and visit purpose;
- CCTV recordings;
- Electronic access-control logs.

7.6 Website Users

- Information provided through enquiry, quote-request or subscription forms;
- Technical information such as IP address, device type, browser version and pages visited (see Section 14).

7.7 Sensitive Information

Rojone collects sensitive information only where the individual consents and the information is reasonably necessary for, or directly related to, one or more of Rojone's functions or activities (or where collection is otherwise required or authorised by law). Examples include criminal-record information collected for pre-employment screening and health information collected in connection with workplace health and safety.

8.0 How We Collect Personal Information

Where reasonably practicable, Rojone collects personal information directly from the individual to whom it relates. Methods of collection include:

- Paper or electronic application, enquiry and order forms;

- Email, telephone, video conference and face-to-face communications;
- Commercial transactions and contracts;
- The Rojone websites (www.rojone.com.au / www.shop.rojone.com) and supported online platforms;
- trade shows, conferences and industry events;
- CCTV and electronic access-control systems on Rojone premises;
- Publicly available sources (including company websites, professional networking platforms and business registers); and
- Third parties such as recruitment agencies, referees, credit reporting bodies and pre-employment screening providers.

At or before the time of collection (or as soon as practicable afterwards), Rojone will take reasonable steps to notify individuals of the matters required by APP 5, including the purposes of collection, the consequences if information is not collected, the types of third parties to whom information may be disclosed, and how to access this Policy.

If Rojone receives unsolicited personal information that it could not have lawfully collected under APP 3, the information will be destroyed or de-identified as soon as practicable, unless it forms part of a Commonwealth record or its retention is otherwise required or authorised by law.

9.0 Purpose of Collection, Use and Disclosure

Rojone collects, holds, uses and discloses personal information for purposes connected with its business activities, including:

- Providing quotations, products, services and technical support;
- Processing orders, payments and invoices;
- Managing customer, supplier and principal relationships;
- Responding to enquiries and complaints;
- Recruiting, screening, training and managing Personnel;
- Administering security clearances and Defence program obligations;
- Complying with export-control, sanctions and customs requirements;
- Conducting audits, due diligence, and quality activities (including under ISO 9001, AS9100, DISP and customer-imposed flow-downs);
- protecting the safety and security of Personnel, visitors and assets;
- undertaking marketing and business development (subject to Section 12); and
- meeting legal, regulatory, contractual and insurance obligations.

Rojone will not use or disclose personal information for any purpose other than the purpose for which it was collected (the primary purpose), unless:

- The individual has consented;
- The secondary purpose is related to the primary purpose (or, in the case of sensitive information, directly related) and the individual would reasonably expect such use or disclosure; or
- the use or disclosure is otherwise required or authorised by or under an Australian law or court/tribunal order.

10.0 Disclosure to Third Parties and Overseas Recipients

10.1 Domestic Disclosure

Rojone may disclose personal information to third parties, including:

- Related corporate entities;
- Service providers (e.g. payroll, banking, IT, cloud-hosting, accounting, legal, insurance, recruitment and pre-employment screening providers);
- Freight, logistics and customs brokers;
- Government agencies (including the Australian Taxation Office, the Department of Defence, the Australian Border Force and the OAIC) where authorised or required by law; and
- Prime contractors and Defence customers were required under contract.

Where Rojone engages a third-party service provider, Rojone will take reasonable steps to ensure that the third party handles personal information consistently with the APPs and any applicable Defence security requirements.

10.2 Overseas Disclosure (APP 8)

Rojone represents and works with overseas principals, suppliers and customers. Personal information (typically business contact information of Rojone Personnel and customer/supplier representatives) may be disclosed to overseas recipients located in countries including, but not limited to:

- United States of America;
- France;
- Germany;
- Finland;
- Switzerland;
- United Kingdom; and
- Singapore.

Before disclosing personal information to an overseas recipient, Rojone will take reasonable steps to ensure that the recipient does not breach the APPs in relation to the information (APP 8.1), unless an exception in APP 8.2 applies (for example, where the individual has consented after being expressly advised that APP 8.1 will not apply).

11.0 Defence, Security Clearance and Export-Controlled Information

As a DISP member and Defence supplier, Rojone collects and handles certain categories of personal information that intersect with Defence security requirements and export control law. These include:

- Australian Government Security Vetting Agency (AGSVA) clearance information for Personnel;
- Citizenship and eligibility-to-work documentation, used to assess access to controlled technology, controlled Goods and Defence-rated information;
- Pre-employment screening information; and
- Personal information contained in customer-supplied data sets and program records.

Such information is handled in accordance with this Policy and additionally in accordance with:

- The Defence Security Principles Framework (DSPF) and DISP requirements;
- The Defence Trade Controls Act 2012 (Cth);
- The Customs Act 1901 (Cth) and applicable sanctions regulations; and
- Contractual flow-downs from Defence and prime-contractor customers.

Where a conflict arises between this Policy and a lawful defence, security, or export-control obligation, the lawful obligation prevails. Personal information collected for security clearance, export screening, or Defence program purposes will not be used for unrelated commercial purposes.

12.0 Direct Marketing

Rojone may use personal information (other than sensitive information) to send marketing and business development communications about products, services, technical updates, and events. Rojone will:

- Comply with APP 7 and the Spam Act 2003 (Cth);
- Only send commercial electronic messages where consent has been obtained (express or inferred) and the message clearly identifies Rojone;
- Include a functional unsubscribe facility in each commercial electronic message; and
- Respect any opt-out request without undue delay.

Sensitive information will not be used or disclosed for direct-marketing purposes without the individual's express consent.

Opt-out requests may be made by using the unsubscribe link in an email, or by contacting the Privacy Officer (see Section 25).

13.0 Site Security, CCTV and Access Control

Rojone uses CCTV and electronic access-control systems at its premises for the purposes of:

- Protecting Personnel, visitors and members of the public;
- Protecting Rojone, customer and controlled assets, including export-controlled goods and Defence-rated material;
- Supporting the security obligations of Rojone as a DISP member; and
- Incident investigation.

CCTV and access-control records are retained for periods determined by Rojone's risk assessment and applicable Defence and contractual obligations and are accessed only by authorised Personnel. Signage is displayed at entry points to notify individuals that CCTV is in operation.

14.0 Website, Cookies, Analytics and Online Tracking

14.1 Information Collected via the Website

The Rojone website (www.rojone.com.au / www.shop.rojone.com) collects personal information in two ways:

- Information voluntarily submitted by users through enquiry, quote-request, subscription or contact forms (for example, name, email, telephone, company and enquiry content); and
- Technical information collected automatically through cookies, scripts and similar technologies, including IP address, approximate geographic location (derived from IP), browser type and version, operating system, device type, referring URL, pages visited, time on page, and timestamps.

14.2 Purposes of Collection

This information is used to:

- Administer, secure and improve the website;
- Understand how visitors use the website (aggregate analytics);
- Respond to enquiries and quote requests;
- Protect the website from spam, abuse and malicious activity; and
- Support Rojone's marketing and business-development activities.

14.3 Cookies

A cookie is a small text file placed on a user's device by a website. Cookies used on the Rojone website fall into the following categories:

Category	Description
Strictly necessary	Required for the website to function (e.g. session management, security, load balancing). These cannot be switched off.
Functional	Remember user preferences and improve user experience (e.g. language selection, form pre-fill).
Analytics/Performance	Help Rojone understand how visitors interact with the website in aggregate.
Security/Anti-spam	Detect and prevent malicious activity, fraud and form abuse.

14.4 Third-Party Tools and Services

Rojone uses the following third-party tools and services on its website. These tools may set cookies and may transfer technical and behavioural data outside Australia, including to the United States.

Tool	Provider	Country	Purpose
Google Analytics (GA4)	Google LLC	United States	Aggregated website usage analytics. IP addresses are collected; Rojone has IP anonymisation/IP truncation enabled where supported.
Google Tag Manager	Google LLC	United States	A tag management container that deploys and manages other website tags.
Google reCAPTCHA	Google LLC	United States	Protects website forms from spam and automated abuse. Collects device, browser and interaction signals.
Email/marketing platform	Mailchimp/HubSpot/SEMrush	United States	Sending newsletters, product updates and marketing communications to subscribers. Used only where consent has been obtained.
Website hosting / CDN	Hosting Bay/Maropost	Australia	Hosting, content delivery and basic security logging.

Each of these providers operates under its own privacy policy. Rojone has no control over, and does not accept responsibility for, the privacy practices of these third parties. Users should refer to each provider's privacy policy for further information.

14.5 How to Control Cookies and Opt Out

Users can manage cookies and analytics tracking in the following ways:

- Browser settings – most browsers allow users to view, manage, delete and block cookies. Refer to the browser's help documentation. Disabling strictly necessary cookies may affect website functionality.
- Google Analytics opt-out – users may install the Google Analytics Opt-Out Browser Add-on available at tools.google.com/dlpage/gaoptout to prevent their data from being used by Google Analytics.
- Do Not Track signals – the Rojone website does not currently respond to “Do Not Track” browser signals, as no consistent industry standard exists. Rojone keeps this practice under review.
- Marketing communications – users may opt out of marketing emails at any time using the unsubscribe link in each message, or by contacting the Privacy Officer (see Section 25).

14.6 Third-Party Links

The Rojone website may contain links to third-party websites, including supplier and principal websites, social-media platforms and industry resources. Rojone is not responsible for the privacy practices or content of those third-party sites. Users are encouraged to review the privacy policies of those sites before providing any personal information.

14.7 Overseas Disclosure via Online Tools

Use of the third-party tools listed in this Section involves the transfer of technical and behavioural information to overseas recipients (principally the United States). This is also reflected in Section 10.2 of this Policy. Where Rojone selects such providers, it does so based on recognised industry security and privacy standards.

15.0 Use of Artificial Intelligence and Automated Decision-Making

Rojone may use artificial intelligence (AI) tools and automated systems to support business activities such as drafting communications, analysing data, and processing transactions. Where AI or automated systems are used:

- Rojone takes reasonable steps to ensure that personal information is not entered into public-domain AI tools without appropriate controls;
- substantive decisions that significantly affect an individual (including decisions in relation to employment) are not made solely on the basis of automated processing without meaningful human review; and
- where Rojone uses automated decision-making that has a legal or similarly significant effect on an individual, this Policy will be updated to provide further transparency as required by emerging Australian privacy law.

This section will be reviewed in line with the Privacy and Other Legislation Amendment Act 2024 (Cth) and OAIC guidance.

16.0 Data Quality and Security

Rojone takes reasonable steps to ensure that the personal information it collects, uses, and discloses is accurate, complete, up to date, and relevant to the purpose for which it is used or disclosed.

Rojone protects personal information through layered safeguards, including:

- Physical security – restricted access, secure storage, CCTV and visitor management;
- ICT security – user authentication, role-based access control, encryption (in transit and at rest where reasonably practicable), patching, malware protection, logging and monitoring;
- Personnel security – pre-employment screening, training, confidentiality undertakings and (where required) security clearances;
- Supplier and third-party controls – confidentiality agreements, contractual privacy obligations and due diligence assessments; and
- Governance – documented policies, procedures and audit activity under Rojone's Quality and Security Management Systems.

17.0 Retention and Destruction of Personal Information

Rojone retains personal information only for as long as it is needed for the purpose for which it was collected or as required by law or contract.

Examples of retention drivers include:

- taxation records (minimum 5 years) under the Income Tax Assessment Act and related law;
- WHS and workers-compensation records (as required by State legislation);
- Defence and export-control records (as required by contract and the Defence Trade Controls Act 2012); and
- quality records (as required under ISO 9001 / AS9100D).

When personal information is no longer required (and is not contained in a Commonwealth record or otherwise required by law to be retained), Rojone will take reasonable steps to destroy the information or ensure that it is de-identified.

18.0 Access to and Correction of Personal Information

18.1 Right of Access

Subject to limited exceptions in the APPs, individuals are entitled to request access to personal information that Rojone holds about them. Requests should be made in writing to the Privacy Officer (see Section 25).

Rojone will respond to access requests within a reasonable period (and within 30 days where practicable). Rojone may recover its reasonable costs of providing access but will not charge a fee for making the request.

Rojone may refuse access where required or authorised by law (for example, where granting access would be unlawful, would unreasonably impact the privacy of another individual, or where the information relates to Defence security or export-controlled matters). Where access is refused, Rojone will provide written reasons and information about how to complain.

18.2 Right of Correction

If an individual considers that personal information held by Rojone is inaccurate, out-of-date, incomplete, irrelevant or misleading, they may request correction in writing to the Privacy Officer.

Rojone will take reasonable steps to correct the information. Where Rojone declines a correction request, it will provide written reasons and, on request, take reasonable steps to associate a statement with the information, noting that the individual considers it incorrect.

19.0 Anonymity and Pseudonymity

Where lawful and practicable, individuals have the option of not identifying themselves, or of using a pseudonym, when dealing with Rojone in relation to a particular matter. This option does not apply where:

- Rojone is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or
- it is impracticable for Rojone to deal with individuals who have not identified themselves (for example, in the context of contracts, Defence-program work, security clearances, or warranty and after-sales support).

20.0 Data Breaches and Notifiable Data Breaches

20.1 Reporting

All Personnel must report any actual or suspected Data Breach to the Privacy Officer as soon as practicable, and in any event within 24 hours of becoming aware of it.

Examples of Data Breaches include:

- Lost or stolen laptops, mobile devices, removable media or paper records containing personal information;
- Emails, mail or documents sent to the wrong recipient;
- Unauthorised access to systems or accounts (including by an employee acting outside the scope of their duties);
- Malware, ransomware or phishing incidents;
- Inadvertent disclosure of personal information in tenders, quotations, technical exchanges or social-media posts; and
- Any other incident or suspected incident in which personal information may have been compromised.

20.2 Assessment

Where Rojone becomes aware that there are reasonable grounds to suspect that there may have been an Eligible Data Breach, Rojone will carry out a reasonable and expeditious assessment to determine whether the breach is an Eligible

Data Breach. This assessment will be completed within 30 days of becoming aware of the suspected breach (or such shorter period as may be required by law).

20.3 Notification

Where Rojone is satisfied that there has been an Eligible Data Breach, Rojone will, as soon as practicable:

- Prepare a statement containing the matters required by section 26WK of the Act; and
- Notify the OAIC and the affected individual(s), or, where direct notification is not practicable, publish the statement on its website and take reasonable steps to publicise it.

20.4 Defence and Customer Notification

Where a Data Breach involves customer-supplied, Defence or export-controlled personal information, Rojone will also notify the affected customer in accordance with contractual requirements and DISP reporting obligations.

21.0 Complaints

Individuals who believe that Rojone has breached the APPs or this Policy may make a complaint to the Privacy Officer (see Section 25). Complaints should be made in writing and include sufficient detail to allow Rojone to investigate.

Rojone will acknowledge receipt within five (5) business days and provide a substantive response within 30 days of receipt, unless additional time is reasonably required and the complainant is notified.

If the complainant is not satisfied with Rojone's response, the complainant may refer the matter to the OAIC:

- Website: www.oaic.gov.au
- Telephone: 1300 363 992
- Post: GPO Box 5288, Sydney NSW 2001

22.0 Roles and Responsibilities

Role	Responsibility
Managing Director	Approves this Policy and maintains overall accountability for privacy compliance.
General Manager (Privacy Officer)	• Owner of this Policy. • First point of contact for privacy matters, access/correction requests and complaints. • Coordinates Data Breach assessment and notification. • Reports to the Managing Director on privacy compliance and incidents. • Oversees privacy awareness and training.
Quality / Compliance Manager	Maintains this Policy under the QMS, supports audit activity, and integrates privacy controls with ISO 9001 / AS9100D and DISP processes.
IT / ICT Lead	Implements and maintains technical safeguards, access controls, logging and incident-response capabilities.
Managers and Supervisors	Ensure that Personnel within their area understand and comply with this Policy.
All Personnel	Comply with this Policy; handle personal information only for proper business purposes; report actual or suspected Data Breaches in accordance with Section 20.

23.0 Breach of this Policy

Failure by Personnel to comply with this Policy may result in disciplinary action, up to and including termination of employment or engagement. Serious breaches may also attract personal liability under the Act and other applicable laws.

24.0 Related Documents and Legislation

24.1 Related Rojone Documents

- Information Security Policy
- Acceptable Use of ICT Policy
- Records Retention and Disposal Schedule
- Data Breach Response Procedure

- Code of Conduct
- Complaints Handling Procedure
- Defence Industry Security Program (DISP) Procedures
- Export Control Compliance Procedure

24.2 Applicable Legislation and Standards

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (Schedule 1)
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)
- Privacy and Other Legislation Amendment Act 2024 (Cth)
- Spam Act 2003 (Cth)
- Do Not Call Register Act 2006 (Cth)
- Defence Trade Controls Act 2012 (Cth)
- Security of Critical Infrastructure Act 2018 (Cth)
- Telecommunications (Interception and Access) Act 1979 (Cth) – where applicable
- Workplace Surveillance Act 2005 (NSW) – where applicable
- ISO 9001:2015 and AS9100D
- Defence Industry Security Program (DISP) requirements
- Defence Security Principles Framework (DSPF)

25. Contact – Privacy Officer

All enquiries, access requests, correction requests, complaints and Data Breach reports under this Policy should be directed to:

Role	Privacy Officer (General Manager)
Entity	Rojone Pty Ltd
Postal Address	44 Aero Road, Ingleburn, NSW, 2565
Telephone	02 98291555
Email	sales@rojone.com.au
Website	www.rojone.com.au

This Policy is reviewed at least every two (2) years, and whenever there is a material change to Rojone's business, applicable law, or Defence security obligations.