RHEINMETALL	Data Privacy Policy		
		Issued:	16/11/2026

1.0 Purpose

This Policy explains how we collect, use, disclose, store, and protect personal information, and how individuals can access or correct their information or make a privacy complaint.

2.0 Scope

This Policy applies to Rheinmetall Defence Australia Pty Ltd ('RDA') and its related bodies corporate such as Rheinmetall MAN Military Vehicles Australia Pty Ltd ('RMMVA') and Logistics Solutions Australasia Pty Ltd ('LSAust') operating in Australia and New Zealand (in this Policy it is referred to as 'the Companies', 'we' or 'our').

Rheinmetall Defence Australia Pty Ltd and wholly owned Rheinmetall entities in Australia ("RDA", "we," "us," "our") are committed to protecting the privacy of individuals and ensuring the secure handling of personal information. We operate in Australia and New Zealand and comply with applicable privacy laws in each jurisdiction, including:

- The Privacy Act 1988 (*Cth*) and Australian Privacy Principles (APPs); and
- The Privacy Act 2020 (*NZ*) and Information Privacy Principles (IPPs) in New Zealand

This Policy applies to all personal information collected and held by Rheinmetall Defence Australia Pty Ltd ('RDA') and its related bodies corporate such as Rheinmetall MAN Military Vehicles Australia Pty Ltd ('RMMVA') and Logistics Solutions Australasia Pty Ltd ('LSAust'), including that of employees, contractors, suppliers, business partners, and other individuals we engage in the course of our business operations in both Australia and New Zealand.

We are a business-to-business (B2B) manufacturer and do not deal directly with consumers.

3.0 Definitions

AI	Artificial Intelligence
APPs	Australian Privacy Principles
CCTV	Closed-Circuit Television
Corporate Environment	The Rheinmetall Defence Australia & New Zealand's Network which incorporates hardware and software necessary to support business objectives within Australia and abroad.
IPPs	Information Privacy Principles
LSAust	Logistics Solutions Australasia
Personal Information	Information, or an opinion, whether true or not, and whether recorded in material form or not, that could identify an individual. Personal information will vary,

	depending on whether a person can be identified or is reasonably identifiable in the circumstance, which may include, an individual's name, signature, address, phone number or date of birth, sensitive information, credit information, employee record information, photographs, and location information from a mobile device.
PIA	Privacy Impact Assessments
Privacy Act *(Cth)*	Australian Privacy Act 1988 *(Cth)*
Privacy Act *(NZ)*	Privacy Act 2020 *(NZ)*
RDA	Rheinmetall Defence Australia
RMMVA	Rheinmetall MAN Military Vehicles Australia
Sensitive Information	As a subset of personal information, sensitive information requires a higher level of protection which includes information, or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information, genetic information; and biometric information.

4.0 Roles and Responsibilities

Data Privacy Officer	The Data Privacy Officer is responsible for ensuring compliance with privacy legislation by: • Overseeing the protection of Personal and Personal Sensitive information; • Liaising with the Office of the Australian Information Commissioner (OAIC); and • Providing advice on privacy obligations to ensure the organisation's collection, use, disclosure and protection of Personal information comply with legislative requirements.
Compliance Officer	Ensures this Policy complies with Rheinmetall Group Policy.
Employees, Contractors and Third Parties	All Employees, Contractors and Third Parties are responsible for compliance with this Policy, and any supporting policies, standards, and procedures.

5.0 What Personal Information we collect

We collect Personal Information that is necessary for our business functions and to fulfill our legal obligations. The types of personal information we collect include:

- Name;
- Contact details (e.g. address, email, phone number);
- Personal details (e.g. date of birth, gender);
- Employment details (e.g. cover letter, resume and working history, qualifications, tax data, emergency contacts, and medical/health information (where required for health and safety));
- Financial information (e.g. bank account details for payroll, superannuation fund details);
- Identification documents (e.g. passport, driver's license);
- Supplier and business partner contacts, bank details for payments;
- Closed-Circuit Television (CCTV) footage, visitor logs, vehicle registration; and
- Other relevant information required for employment purposes.

We do not generally collect your Sensitive Information (e.g., political opinions, sexual orientation, etc) with the exception of criminal records (which we will generally only collect with your prior consent), and information regarding any disability or pre-existing health condition requiring accessibility assistance (which we will generally only collect where you provide it to us voluntarily, or otherwise with your prior consent).

The Privacy Act contains certain exemptions in relation to certain acts undertaken in relation to employee records and related bodies corporate. Where appropriate we make use of relevant exemptions in the Act.

5.1 Methods of Collection

We collect Personal Information directly from you through various means, including online forms, face-to-face meetings, phone calls, emails, contracts, and security systems such as, (e.g., CCTV or visitor sign-in systems).

We may also collect information from third parties, such as your employer or contracting organisations, a service provider, a veteran’s community or from a publicly available record.

We take reasonable steps to ensure the personal information we collect is accurate and up to date.

6.0 Purpose of Collection

6.1 Primary Purpose

The purposes for which we collect your Personal Information include to:

- Manage employment relationships, including but not limited to payroll processing, benefits administration and performance evaluations;
- Implement our voluntary share plan for eligible employees;
- Consider and process employment applications;

- Communicate with you and respond to your inquiries, feedback or complaints;
- Comply with legal and regulatory requirements;
- Conduct criminal record and security checks;
- Improve our services and products;
- Managing vendor, contractor, and business partner relationships;
- Financial management, including payments and invoicing;
- Security and risk management (e.g. site access control); and
- Internal reporting, auditing, and record keeping.

6.2 Secondary Purposes

We may also use or disclose personal information for secondary purposes closely related to the primary purpose set out in this Privacy Policy, or otherwise with your prior consent.

7.0 Use, Disclosure and Automatic Processing of Personal Information

7.1 Use of Personal Information

We use your Personal Information only for the purposes set out in this Privacy Policy or as otherwise permitted by law, including to:

- Administer payroll, benefits, performance evaluations, and other similar uses related to your employment with us;
- Assess your eligibility to participate, and if eligible, to administer and facilitate your participation in our voluntary share plan;
- Assess and administer your employment application;
- Communicate with you and respond to inquiries, feedback or complaints; and
- Comply with our legal and regulatory requirements.

7.2 Disclosure of Personal Information

We may disclose your Personal Information to:

- Our employees and related bodies corporate;
- Third parties such as service providers located outside of Australia (as set out at section 7.3 below), payroll processors, and contractors who assist us in our business operations;
- Regulatory bodies, government agencies and law enforcement agencies in Australia or New Zealand;
- Related companies within Rheinmetall Group; and
- Professional advisors, such as lawyers and accountants, where necessary for them to perform their services any other third parties as required or authorised by law.

We do not sell or rent Personal Information to third parties.

7.3 Artificial Intelligence (AI) and Automated Processing

We may utilise approved enterprise technologies, including Artificial Intelligence (AI) tools, to support business operations and improve efficiency.

We have undertaken a review of our current business processes and information handling activities to assess whether any processing activities constitute automated decision-making for the purposes of the Australian Privacy Principles, including APP 1.7-1.9.

Following this review, we have not identified any decision-making processes in which a computer program makes, or is substantially and directly responsible for making, a decision that could reasonably be expected to significantly affect an individual's rights or interests without meaningful human involvement.

Accordingly, we do not currently engage in automated decision-making activities that trigger the transparency obligations under APP 1.7-1.9.

We will periodically review business processes, technologies and systems to assess whether future activities involve automated decision-making requiring additional transparency disclosures under applicable privacy legislation.

7.4 Cross-Border Disclosure

Although we primarily operate in Australia and New Zealand, if we do transfer personal information outside these countries (e.g., for cloud services, global vendors or members of the Rheinmetall Group), we will:

- Take reasonable steps to ensure the recipient protects it in accordance with Australian and New Zealand privacy laws; and
- Obtain consent where required, or ensure contractual safeguards are in place.

7.5 Privacy Impact Assessments

We apply a Privacy by Design approach and may conduct Privacy Impact Assessments (PIAs) for new projects, systems, technologies, or business activities that involve personal information and may create privacy risks. PIAs help us identify, assess, and manage privacy risks and ensure appropriate safeguards are implemented to protect personal information.

7.6 Storage and Security of Personal Information

We generally hold personal information in our electronic databases but also store personal information in hard copy form and in various third-party databases and platforms.

7.7 Storage Measures

We take reasonable steps to protect your personal information from misuse, interference, loss, unauthorised access, modification, or disclosure. These steps include:

- Secure physical storage systems (e.g. locked cabinets, limited access storage facilities);
- Electronic storage systems secured with access controls and encryption (including anti-virus and firewalls); and
- Regular security audits and risk assessments.

7.8 Retention and Destruction

Personal information is retained by us for as long as is necessary to enable us to fulfill the purposes set out in this Privacy Policy or as otherwise required by law. We may also use personal information to meet internal and external audit requirements or information security purposes.

When we no longer require your personal information, that information is securely destroyed or de-identified in accordance with our information retention procedures. Job and Veterans Engagement applicant data will be stored for an additional six months after the application process has finished. If an individual provides consent to store their data for future opportunities, we will store that data for an additional 24 months.

8.0 Access and Correction

8.1 Access Rights

To request access to your personal information which we hold, please contact our Privacy Officer using the contact details provided at section 9.0 (Contact Us) below (or, if you are an employee, please contact the Human Resources Department).

We will respond to your request within a reasonable timeframe, usually within 30 days. Where we hold information that you are entitled to access, we will endeavour to provide you with a range of suitable access options (e.g. email or post). A fee may be charged to cover our reasonable costs associated with retrieving and providing access to your personal information.

8.2 Correction Rights

If you believe that any personal information, we hold about you is incorrect, incomplete, or outdated, you may request that we correct your personal information by contacting our Privacy Officer using the contact details provided at section 9.0 (Contact Us) below (or, if you are an employee, by contacting the Human Resources Department). We will review your request and consider whether it is reasonable under the circumstances.

If we consider your request is reasonable, we will take reasonable steps to correct the information to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held. If we consider your request is not reasonable and refuse your request, we will provide you with a written notice including the reasons for the refusal and attach a notice to our record of the relevant personal information noting that you have informed us you believe the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

9.0 Complaints

9.1 Lodging a Complaint

If you think we have breached your privacy rights or you have any concerns or complaints about the way we have handled your personal information, please contact our Privacy Officer using the contact details provided at section 9.0 (Contact Us) below. For all employees, the HR Department remains available as an alternative point of contact. Please include your name, email address and/or telephone number and clearly describe your complaint.

We take all complaints seriously and will investigate and respond to your complaint promptly (and in any event, within 30 days). We will advise whether we agree with your

complaint or not. If we do not agree, we will provide you with reasons for our decision. If we do agree, we will advise what (if any) action we consider appropriate to take in response to your complaint.

9.2 Further Recourse

After providing us with a reasonable time to respond, if you are still unsatisfied with our handling of your complaint you may contact:

- In Australia:

  Office of the Australian Information Commissioner (OAIC)

  Website: www.oaic.gov.au | Phone: 1300 363 992

- In New Zealand:

  Office of the Privacy Commissioner (NZ OPC)

  Website: www.privacy.org.nz | Phone: 0800 803 909.

10.0 Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or industry standards. The updated Privacy Policy will be posted on our website, and we encourage you to review it periodically.

11.0 Contact Us

If you have any questions or concerns about this Privacy Policy or our privacy practices, please contact our Privacy Officer at:

- Rheinmetall Defence Australia and New Zealand

  Compliance & Privacy Officer

  Administration Building – Level 2, 111 Robert Smith Street, Redbank, QLD, 4301

  compliance.aus@rheinmetall.com.au

12.0 Third-Party Audits

We may engage independent third parties to conduct audits or assessments of our information security and privacy practices. These audits may include:

- Evaluation of compliance with applicable privacy legislation (Privacy Act 1988 (Cth) in Australia and Privacy Act 2020 in New Zealand);
- Review of our data handling, storage, and protection practices; and
- Security penetration testing or system vulnerability assessments (where appropriate).

Third-party auditors are contractually bound to maintain confidentiality and protect any personal information they access during their engagements. Findings from such audits are used to improve our data protection measures and internal controls.

13.0 Data Breach Response

We take data security seriously and have established processes to manage any actual or suspected breaches involving personal information.

In the event of a data breach, we will:

1. Identify and contain the breach to prevent further loss or damage
2. Assess the nature and extent of the breach, including the types of personal information involved and the potential harm to individuals
3. Notify affected individuals and the appropriate regulatory authority:
    a. In Australia, we will notify the Office of the Australian Information Commissioner and affected individuals where required under the Notifiable Data Breaches (NDB) scheme.
    b. In New Zealand, we will notify the Office of the Privacy Commissioner if the breach poses a risk of serious harm, in line with the Privacy Act 2020.
4. Review and respond, including steps to prevent recurrence and enhance security controls.

We are committed to transparency and accountability in responding to privacy incidents and will act promptly to mitigate any risks to individuals.

14.0 Attachments

N/A