

1. Introduction

The privacy and security of the personal information of our staff, customers and suppliers is important to us. We aim to carefully and respectfully manage your personal information that is fundamental to our business. All entities of Ramcar Australia and New Zealand (the Company) in Australia and New Zealand and our parent companies in the Philippines are committed to protecting your privacy and we are bound by the Privacy Act 1988 (Cth) ('Privacy Act') and must protect your personal information according to that Act and other applicable laws.

2. Purpose

The Privacy Act requires entities bound by the Australian Privacy Principles to have a privacy policy. This privacy policy outlines the personal information handling practices of Ramcar Australia and New Zealand and explains:

- who we are;
- how we collect personal information; and
- how we handle, share and use personal information

This policy also sets out the specific legal obligations of the Company when collecting and handling your personal information as outlined in the Privacy Act and in particular in the Australian Privacy Principles found in that Act.

Scope

This Policy applies to all Workplace Participants of entities associated with Ramcar in Australia and New Zealand (the Company).

3. Exclusions

There are no exclusions under this Policy.

4. Policy Owner

The owner of this Policy is the Regional Director.

5. Responsibility

- Directors
- Operational Management Team (OMT)
- Privacy Officer
- All Staff
- All Directors and staff of our Parent companies (Manila, Philippines)

- Customers, Contractors, Distributors and Agents of Ramcar Entities
- External Consultants: HR, Finance and Legal (but not limited to)
- Suppliers and third-party providers (but not limited to)

6. Definitions¹

Privacy: Privacy is a fundamental human right that underpins freedom of association, thought and expression, as well as freedom from discrimination. But it's hard to define. Different countries offer different views, as do individuals.

Generally speaking, privacy includes the right:

- to be free from interference and intrusion
- to associate freely with whom you want
- to be able to control who can see or use information about you

And there are different ways to look at privacy, such as:

- physical privacy (for instance, being frisked at airport security or giving a bodily sample for medical reasons)
- surveillance (where your identity can't be proved, or information isn't recorded)
- information privacy (how your personal information is handled)

Information privacy is about promoting the protection of information that says who we are, what we do and what we believe.

Personal Information: includes any information or opinion, about an identified individual or an individual who can be reasonably identified from that information. The information or opinion will still be personal information whether it is true or not and regardless of whether we have kept a record of it.

7. Interpretation

This Policy is to be interpreted in a "common sense" manner, that is, using comprehensive and practical judgement based on simple observation of the situation or facts and not being subject to an overly technical analysis.

If you are unsure, then please refer to the Privacy Act for further information/reference.

¹ Ref: Australian Government: Office of the Australian Information Commissioner

8. Process

Ramcar Australia and New Zealand will collect, hold and disclose personal information to conduct functions or activities of our business operations and will undertake all/any of these activities within the terms as set out in the Privacy Act.

The process below outlines our handling practices, your rights and how to lodge a complaint with us.

8.1 What kinds of personal information we collect and store

At all times we try to only collect the information we need for the particular function or activity we are carrying out. The main way we collect personal information about you is when you give it to us. For example, we collect personal information such as:

Employees:

When you join and/or when you are employed by the Company, the personal information we collect, and store can include:

- Your full legal name
- Date of Birth (DOB)
- Home Address
- Personal email address
- Personal mobile and landline telephone numbers
- Employee, referee and next of kin or emergency contact details
- Applications for employment and supporting documents
- Certified copies of academic qualifications
- Employment contracts, and other records relating to terms and conditions of employment
- Identification, such as Proof of Australian Citizenship or valid Visa's/Right to Work in Australia, Driver's License, Passport, Birth Certificate, Medicare Card and other forms of identification used to identify you – otherwise known as a 100-point ID check
- Details of financial and other personal interests supplied by employees and their immediate family members for the purpose of managing perceived or potential conflicts of interest
- Records relating to salary, employment benefits and leave
- Medical certificates or health related information supplied by an employee or their medical practitioner
- Taxation details, Superannuation details and Banking information necessary to pay salary and wages
- Police reference checks, or other required checks where applicable
- Information relating to employees' training and development
- Information about an employee's performance

Customers, Suppliers and the General Public:

It is normal practice when conducting business with us, you may call us, email us directly or through our website or you may complete a credit application in order to purchase, supply or return goods. Any of these interactions mentioned may capture the following information:

- Full name, address and contacts details of a customer or member of the public
- Full company name including address, telephone number and ACN (Australia Company Number), ABN (Australian Business Number) or NZBN (New Zealand Business Number)
- Director's details, such as full name, DOB, home address and other contact details such as a personal email address and mobile telephone number
- Financial information about the company including auditor and credit reports

8.2 How we collect personal information and where it is stored

- Information collected is usually given to us by you. Sometimes this can be provided to us by a third party. Information can either be given to us in hard copy or sent to us electronically.
- We may also collect information from you when, as examples: we conduct a reference check or complete a National Criminal History Check for employment; or we undertake a credit history report through a third party for a new customer
- We store information both in a hard copy file in our office and also file information electronically on our network drives.
- All hard copy files are kept for seven (7) years and are then destroyed by an external secure destruction organisation.

8.3 Why we need to collect personal information

We collect personal in order to:

- Identify you and conduct appropriate checks
- Administer and manage our products and services and systems, including the management and administration of any claims
- Assess and investigate any product or warranty claims made by our customers
- Assess and investigate any claims made by an employee
- Seek recovery from you due to any claim we may have against you
- Manage, train and develop our employees and representatives
- Manage complaints and disputes, and report to dispute resolution bodies
- Get a better understanding of you, your needs, your behaviours and how you interact with us, so we can engage in product and service research, development and business strategy including managing the delivery of our services and products via the ways we communicate with you.

8.4 What happens if you don't give us your personal information?

If we ask for your personal information and you do not give it to us, we may not be able to:

- Employ you

- Assess, investigate, manage or assist in a product or warranty claim
- Provide our employees and our customers with any or all entitlements under our policies
- Provide services or products to your company
- Accept products from your company

8.5 How we use and may disclose personal information

In the course of any reference check, investigation or claim we may collect and use personal information (including sensitive information) about you either directly or indirectly from publicly available sources or from third parties to enable us to contact stakeholders who may be interested in or participating in our operations.

We use social networking services such as Twitter, Facebook and YouTube to communicate with the public about our products and services. When you communicate with us using these services we may collect your personal information, but we only use it to help us to communicate with you and the public. The social networking service will also handle your personal information for its own purposes. These services have their own privacy policies. You can access the privacy policies for Twitter, Facebook and YouTube (a Google company) on their websites.

Employees:

Sometimes we may need to collect sensitive information about you, for example, regarding your employment or prospective employment, to handle a complaint or a claim. This might include information about your performance, employment history, health, criminal history, etc.

Customers and Suppliers:

We will collect information that you provide to us when applying for credit, signing up to email and mailing lists and registering for our events, the purchase or sale of product, or when submitting feedback to our organization either verbally, in writing or via our websites.

8.6 How you can access your personal information, or ask for a correction or make a complaint if you think your information has been mishandled

You have the right to access and correct your personal information held by us. For more information about our Privacy Policy, your personal information; how we handle your information; access your personal information; or make a complaint if you think your information has been mishandled.

- If you wish to complain to us about how we have handled your personal information you should complain in writing. If you need help lodging a complaint, you can contact us.
- If we receive a complaint from you about how we have handled your personal information we will determine what (if any) action, we should take to resolve the complaint.
- If we decide that a complaint should be investigated further, the complaint will usually be handled by a more senior officer than the officer whose actions you are complaining about.
- We will advise you promptly that we have received your complaint and then respond to the complaint within 30 days.

- If you are not satisfied with our response, you may ask for a review by a more senior officer within our organisation or you can complain to the Commonwealth Ombudsman.

Please contact our Privacy Officers, as per contact details below:

| For all HR and Employee information: | For all Customer and Supplier information: |
|---|--|
| <p>Linda Scully (Head of Human Resources) <u>Privacy Officer – HR & IR</u> Ramcar Australia and New Zealand 1A Reconciliation Rise PEMULWUY NSW 2145 (PO Box 65, SMITHFIELD WEST NSW 2164) Telephone: (02) 9840 2800 Email: linda.scully@ramcar.com.au</p> | <p>Jun Lambino (Supply Chain & IT Manager) <u>Privacy Officer – Commercial</u> Ramcar Australia and New Zealand 1A Reconciliation Rise PEMULWUY NSW 2145 (PO Box 65, SMITHFIELD WEST NSW 2164) Telephone: (02) 9840 2800 Email: jun.lambino@ramcar.com.au</p> |

8.7 If we are likely to disclose your information outside Australia and, if practical, which countries they are likely to disclose the information to

We may need to provide your personal information to – or get personal information about you from – persons or organisations located overseas, for the same purposes as in ‘Why do we collect personal information?’

Usually this includes our headquarters based in Manila, Philippines who provide outsourcing services to the Australian and New Zealand operations, and whom we report to organisationally. We will always disclose and collect your personal information in accordance with privacy laws.

Web traffic information is disclosed to Google Analytics when you visit our websites. Google stores information across multiple countries.

When you communicate with us through a social network service such as Facebook or Twitter, the social network provider and its partners may collect and hold your personal information overseas.

8.8 Quality of personal information

To ensure that the personal information we collect is accurate, up-to-date and complete we:

- Record information in a consistent format
- Where necessary, confirm the accuracy of information we collect from a third party or a public source
- Promptly add updated or new personal information to existing records
- Regularly audit our contact lists to check their accuracy.

We also review the quality of personal information before we use or disclose it.

8.9 Storage and security of personal information

Under the Privacy Act (Australian Privacy Principles 12 and 13) you have the right to ask for access to personal information that we hold about you, and ask that we correct that personal information. You can ask for access or correction by contacting us and we must respond within 30 days. If you ask, we

must give you access to your personal information, and take reasonable steps to correct it if we consider it is incorrect, unless there is a law that allows or requires us not to.

We will ask you to verify your identity before we give you access to your information or correct it, and we will try to make the process as simple as possible. If we refuse to give you access to, or correct, your personal information, we must notify you in writing setting out the reasons.

If we make a correction and we have disclosed the incorrect information to others, you can ask us to tell them about the correction. We must do so unless there is a valid reason not to.

If we refuse to correct your personal information, you can ask us to associate with it (for example, attach or link) a statement that you believe the information is incorrect and why.

9. Consequences of Breaching Policy

An Employee found to be in breach of this Policy may be subject to disciplinary action up to and including, termination of employment.

A Workplace Participant, who is not an Employee of the Company, found to be in breach of this Policy will be dealt with under the relevant contract for service which may result in termination of that contract.

10. Relationship to Employment Contract

This Policy does not and will not form a part of an Employee's current or prospective employment contract, however, it is a term and condition of employment that an Employee complies with the Policy.

11. Other Obligations

This Policy operates in addition to any other obligations that exist:

- Under relevant legislation, Company policies, procedures, codes, practices, etc.; or
- In the Employee's employment contract.

12. Document Control and Amendments Summary

This Policy will be updated when information handling practices change, together with any requirements under the Privacy Act 1998.

The Company reserves the right at any time in the future to amend, vary or replace this Policy at its sole and absolute discretion.