Freightways

www.freightways.co.nz

PRIVACY POLICY - AUSTRALIA

APPROVED NOVEMBER 2023

PRIVACY POLICY - AUSTRALIA

This policy applies to all directors, employees and contractors of Freightways Group Limited and its various Business Units (**Freightways** or **we**), as well as any third parties who process Personal Information on behalf of Freightways or its Business Units (collectively, **Freightways Users**) as further specified below:

- all majority or wholly-owned Australian Freightways entities;
- any majority or wholly-owned non-Australian Freightways entity or Freightways User that carries on business in Australia; and
- any Freightways User who is an Australian citizen or whose continued presence in Australia is not subject to a legal time limitation.

INTRODUCTION AND PURPOSE

Freightways considers the protection of privacy to be of utmost importance and this Privacy Policy (**Policy**) is an essential part of ensuring Freightways and its Business Units promote an individual's confidence that their Personal Information is protected and will be treated properly. Managing Personal Information is important to Freightways in building trust and confidence with individuals while also maintaining compliance with the requirements of the Privacy Act.

The purpose of this policy is to provide a privacy framework for use in Australia, including how Freightways will collect, store, use, disclose and dispose of Personal Information in accordance with the Privacy Act.

SCOPE

Freightways complies with the Privacy Act and any other privacy and data protection laws where applicable, including where Freightways is bound by foreign laws governing these matters.

This policy covers all Personal Information regardless of whether it relates to:

- Customers
- Employees
- Contractors
- Members of the public
- Any other individual.

RELATED DOCUMENTS

The following documents are related to this policy:

- Privacy Breach Policy
- Privacy Impact Assessment
- Information Management Retention Policy and Disposal Schedule
- Privacy Act Access and Correction Request Process
- Privacy Complaints Process
- Third Party Assessment Process.

DEFINITIONS

'Business Unit' refers to each of the various majority or wholly-owned Australian operating companies of Freightways from time to time. As of November 2023, this includes:

Allied Express Transport Pty Ltd	LitSupport Pty Ltd
Med-X Pty Ltd	Shred-X Pty Ltd
The Information Management Group Pty Ltd	

This also includes Freightways Express Limited, to the extent it has an "Australian link" under the Privacy Act.

'Freightways', **'us'** and **'we'** have the meaning given to those terms in the first paragraph of this Policy.

'Freightways Users' has the meaning given to those terms in the first paragraph of this Policy.

'Personal Information' is any information which tells us something about or relating to a specific individual. The information does not need to name the individual, as long as they are identifiable in other ways, like through their home address. This may include information obtained from the use of CCTV.

'Privacy Act' refers to the Privacy Act 1988.

'Privacy Breach' is:

- an event involving unauthorised or accidental access to, or disclosure of, Personal Information; or
- an action that prevents Freightways or any of our Business Units from accessing Personal Information on either a temporary or permanent basis,

whether or not the above event or action is ongoing or was caused by, or attributable in any way to, any of our Business Units or person inside of any of our Business Units.

'**Privacy Facilitator'** is the main point of contact for a Business Unit for all privacy related matters within that Business Unit and is responsible for liaising with Freightways' Privacy Officer where escalations are required.

'**Privacy Officer'** means the Freightways' employee who is responsible for all privacy related matters in Australia across Freightways on behalf of the leadership team, monitoring compliance, acting as the contact for the Office of the Australian Information Commissioner for breach notifications, complaints and other enquiries and to ensure Freightways complies with the provisions of the Privacy Act.

'**Sensitive Information**' means any of the following:

- Personal Information that is 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, or criminal record;
- health information about an individual;
- genetic information about an individual that is not otherwise health information;
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

OVERARCHING PRINCIPLES

This section describes the broad principles under which Freightways will collect, store, allow access and correction to, use, and disclose Personal Information. The descriptions in this policy are consistent with the equivalent principles in the Privacy Act but are in summary form and may omit some of the nuance contained in the Privacy Act – if you have any questions on these principles and how they relate to the Privacy Act, please contact the Privacy Officer.

1. COLLECTING PERSONAL INFORMATION

We will only collect the minimum Personal Information necessary for our lawful business purposes. We will not collect Personal Information where it is not necessary for those purposes or where we are not permitted to do so by law.

We must give individuals the option of not identifying themselves, or to use a pseudonym, when they are dealing with us. The exception to this is if we are otherwise required by law to deal with individuals who have identified themselves, or if it is impractical for us to deal with the individual anonymously or via a pseudonym.

We will endeavour to collect Personal Information:

- Directly from the individual it is about, unless direct collection is not reasonable or practicable
- In a way that is lawful and fair in the circumstances
- In a way that ensures the information is accurate, up-to-date, complete, relevant and not misleading.

We must inform individuals about what information we are collecting, why we collect it and key details about how we will treat it (in the form of a "Privacy Notice") prior to collection or, if that is not practicable, as soon as practicable after the collection. The Privacy Notice will include the consequence for not providing the Personal Information and information about the individual's rights to access and correct Personal Information.

2. SENSITIVE INFORMATION

We must not collect Sensitive Information about an individual unless the individual consents and the information is reasonably necessary for our lawful business purposes, except in the following circumstances.

We may collect Sensitive Information without that individual's consent if any of the following circumstances apply:

- We are required by law or a court / tribunal order to do so.
- We reasonably believe that this information is necessary to lessen or prevent a serious threat to the life, health or safety of any person (and it is not reasonable or practicable to obtain that individual's consent).
- We have a reasonable suspicion that unlawful activity or serious misconduct relating to our business has been engaged in, and we reasonably believe that the Sensitive Information is required for us to take action.
- We reasonably believe that this information is reasonably necessary to assist in locating a reported missing person.
- The information is reasonably necessary to establish, exercise or defend a legal claim.
- The information is reasonably necessary for confidential alternative dispute resolution.

3. UNSOLICITED PERSONAL INFORMATION

This section 3 applies if we receive Personal Information, and where we did not ask for that Personal Information.

Within a reasonable period after receiving that Personal Information, the Freightways User who receives that Personal Information must determine whether we could have collected that Personal Information under section 1 if we had asked the individual to whom that Personal Information relates.

- If we could have, then we can use that Personal Information provided we comply with the rest of this policy.
- However, if we could not have, then we must destroy that information as soon as reasonably practicable consistently in accordance with our ***Information Management Retention Policy and Disposal Schedule***. Bear in mind our statutory obligations to retain particular types of information.

4. STORAGE AND RETENTION OF PERSONAL INFORMATION

Freightways Users must take all reasonable steps to protect Personal Information from:

- Loss
- Unauthorised access, use, modification or disclosure
- Other misuse or interference.

We will not store Personal Information for longer than is necessary for a lawful business purpose and will dispose of it or de-identify it when it is no longer needed (bearing in mind our statutory obligations to retain particular types of information). Information should be maintained consistently in accordance with our ***Information Management Retention Policy and Disposal Schedule***.

5. ACCESS TO PERSONAL INFORMATION

Individuals have the right to request access to their own Personal Information. A request can come from a customer, an employee, or any other individual. Each request must be made by either the individual concerned or their representative. They do not need to cite the Privacy Act for it to be an appropriate request. Any request for access to Personal Information must be dealt with in accordance with the ***Privacy Act Access and Correction Request Process*** and must be notified to the Privacy Officer. The Privacy Officer will guide the request and advise on appropriate withholding grounds if they apply.

As a general principle, unless there are valid reasons why we would not disclose that information (as prescribed by the Privacy Act), we will provide access to Personal Information we hold about any individual if they request that information.

All employee Personal Information requests should also be notified to the Privacy Facilitator for your brand. An employee who wishes to access their own Personal Information should make the request of their manager or Privacy Facilitator.

All requests for access must be responded to within a reasonable period.

6. CORRECTION OF PERSONAL INFORMATION

Individuals also have the right to request correction of Personal Information about themselves. These requests can be of simple facts (for example, an address) or more complex issues (such as a file note saying a customer was aggressive). In any instance we need to consider the request to correct the information and take appropriate action.

All correction requests must be managed in accordance with the ***Privacy Act Access and Correction Request Process***. Requests must be responded to within a reasonable period.

If we do not agree that the information is incorrect, we do not need to correct it – but we do need to give the individual written reasons for refusing the correction. However, when requesting a correction of their Personal Information, or at any later time, an individual can provide us with a statement of the correction sought and request that the statement be attached to the information if the correction sought is not granted. A request of this kind must be responded to within a reasonable period. Where we are asked to attach a statement of correction, we must take reasonable steps to ensure that the statement of correction is attached to the information in a manner that the statement is apparent to users of the information. We must not charge the individual for requesting, or making, such corrections.

7. USE AND DISCLOSURE OF PERSONAL INFORMATION

We will not use or disclose Personal Information unless we reasonably believe that the information is accurate, up-to-date, complete, relevant and not misleading.

We will only use Personal Information for our lawful business purposes (including as set out in the Privacy Notice or as otherwise permitted under the Privacy Act). Primarily this will be where we are using Personal Information for the reason it was initially collected.

We will not use an individual's Personal Information for training or for system testing purposes.

We will not use or disclose Personal Information for direct marketing, unless:

- the information was directly collected from the individual and they reasonably expected information to be used for direct marketing;
- the individual gave consent; or
- it is impracticable to obtain the individual's consent.

We will not send commercial electronic messages (i.e. marketing messages) which the recipient has not consented to receiving. Commercial electronic messages must include an unsubscribe facility.

Before we disclose Personal Information overseas, we need to take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles in the Privacy Act (with some exceptions, such as informed consent from the individual). We will not disclose Personal Information (including to another Business Unit) unless we have a reasonable basis for believing doing so is lawful. This will usually be where the disclosure is for the purpose the information was collected or because it is consented to by the individual. Other exceptions apply and if you are uncertain if there is any lawful basis for disclosure you must discuss this with your Business Unit Privacy Facilitator or the Privacy Officer.

We will not disclose Personal Information overseas unless it is protected by safeguards comparable to those provided under the Privacy Act in Australia (for example, because the overseas jurisdiction has laws equivalent to the Privacy Act, or because of contractual requirements on the overseas person). For guidance on any overseas disclosure of Personal Information you should consult with the Privacy Officer.

Before we disclose Personal Information overseas, we need to take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles in the Privacy Act (with some exceptions, such as informed consent from the individual).

PRIVACY BREACHES

We have clear, consistent processes for reporting, managing and escalating privacy incidents. For any suspected Privacy Breach, you must immediately follow the Privacy Breach Process and notify your Privacy Facilitator.

The Privacy Facilitator must immediately notify the Privacy Officer of each suspected Privacy Breach. The Privacy Officer will then consider whether there may have been a Privacy Breach, and whether that Privacy Breach has caused, or may cause, serious harm to one or more affected individuals.

The Privacy Officer is responsible for recording each suspected Privacy Breach in a central privacy breach log upon becoming aware of that suspected breach (or later, where more time is required to investigate or resolve a suspected breach).

THIRD PARTIES

Where we contract with a third-party to outsource the processing of Personal Information we must ensure that the Personal Information is protected by safeguards comparable to those that apply if it were managed by us. Agreements must require the contracted party to meet our privacy requirements, for example:

- Process Personal Information on our behalf only for those purposes instructed by us
- Notify us of any Privacy Breach or suspected Privacy Breach
- Maintain reasonable security safeguards
- Only retain information for a specified period (as a general rule, such specified periods should not be longer than how long we are allowed to retain that information)
- Not sub-contract the processing to a lower standard than is agreed in the contract
- Not transfer any Personal Information overseas unless it is protected by safeguards comparable to those provided under the Privacy Act in Australia.

The ***Third-Party Assessment Policy*** details how we assess and manage third parties from a privacy perspective.

COMPLAINTS

Where you become aware of a complaint about privacy or the management of Personal Information you must immediately notify your Privacy Facilitator in accordance with the ***Privacy Complaints Process.***

The Privacy Facilitator must notify the Privacy Officer.

PRIVACY IMPACT ASSESSMENT

If you are considering a new process, policy, product, service, or system that changes how we collect, use, store, disclose or dispose of Personal Information you must consider any potential privacy impacts and risks.

To initiate this, you should contact your Privacy Facilitator outlining the proposal and any anticipated risks. The Privacy Facilitator or the Privacy Officer may ask that you undertake a ***Privacy Impact Assessment***.

If a Privacy Impact Assessment is required, it must be signed off by the relevant business owner and the Privacy Officer before the process, policy or system is brought into effect.

TRAINING AND EDUCATION

We will train those employees and contractors working with Personal Information as well as ensuring that all employees undertake regular training on privacy risk areas specific to their business areas, as well as broader privacy best practices.

PROCESS REVIEW

We commit to retaining up-to-date privacy processes. Our business processes relating to the collection, access and correction, use, disclosure, storage and disposal of Personal Information will be regularly reviewed, at least annually.

ACCOUNTABILITIES AND RESPONSIBILITIES

Freightways' Board is committed to managing Personal Information by:

- Setting clear expectations regarding privacy and protection of Personal Information, and communicating them to the leadership team
- Holding the leadership team accountable for meeting those expectations
- Ensuring that effective privacy risk management is fully embedded within Freightways' overall risk management activities
- Employing high-quality monitoring and information management practices.

The Privacy Officer, on behalf of the leadership team, is accountable for:

- Promoting privacy within Freightways and encouraging Freightways to comply with the Australian Privacy Principles in the Privacy Act
- Monitoring compliance and to assist with access and correction requests
- Monitoring and advising on Privacy Impact Assessments
- Being the point of contact for the Office of the Australian Information Commissioner for Privacy Breach notifications, complaints, investigations and other enquiries
- Assisting with Privacy Breaches or any complaints raised about privacy
- Ensuring that Freightways complies with the provisions of the Privacy Act.

Each Business Unit has its own Privacy Facilitator whose role is to:

- Notify privacy incidents in accordance with the Privacy Breach Process
- Proactively assess and manage privacy risk within the Business Unit
- Ensure Business Unit employees and contractors are aware of and recognise the importance of their role in privacy
- Ensure employees and contractors are aware of and compliant with this Privacy Policy, our Policy Notice and the Privacy Act; and
- Ensure new employee induction and contractor on-boarding includes privacy training.

Freightways Users have individual responsibility to:

- Maintain best practice in relation to privacy
- Report all Privacy Breaches, suspected Privacy Breaches and near misses to their manager
- Promote privacy at work
- Comply with all applicable privacy policies and guidelines, including this Policy
- Actively participate in privacy training
- Identify privacy risks.

MONITORING AND GOVERNANCE

Our privacy policies and guidelines have been established to comply with the Privacy Act. The monitoring and oversight of privacy follows a three lines of defence model to provide assurance that privacy risks are being managed effectively under different situations:

- The first line of defence is formed by managers and employees responsible for identifying and managing risks as part of their duties and contractors obliged to identify and manage risks as part of their service provisions.
- The second line of defence is formed by privacy and internal governance policies, frameworks, tools and techniques to support privacy to be maintained.
- The third line of defence is formed by internal and external audits ensuring that the first two lines of defence are operating effectively and identifying opportunities for improvement.

NON-COMPLIANCE

Non-compliance of the terms of this Policy may result in Freightways exercising its related contractual rights, disciplinary action or dismissal.

CONTACT

Any privacy related concerns or requests for information should be initially directed to your Privacy Facilitator. A list of Privacy Facilitators can be found here.

Where required you can also contact our Privacy Officer at privacy@freightways.co.nz.

REVIEW OF POLICY

The Privacy Officer is responsible for maintaining this Policy and the Audit & Risk Committee is responsible for approving this Policy every 3 years, or more frequently as circumstances require.