

Privacy Policy

Overview

National Intermodal Corporation Limited (**National Intermodal**) is committed to protecting the privacy of individuals.

As a Government Business Enterprise, National Intermodal is bound to comply with the following legal requirements, including the regulations made under these Acts:

- the Australian Privacy Principles (APPs) as set out in the *Privacy Act 1988* (Cth);
- the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth);
- the *Privacy (Australian Government Agencies – Governance) APP Code 2017*; and
- NSW privacy legislation as set out in the *Privacy and Personal Information Protection Act 1998* (NSW) as amended from time to time.

This Privacy Policy applies to all the activities of National Intermodal and its wholly owned subsidiaries and sets out National Intermodal's policy on the management of personal information.

People dealing with National Intermodal have the right to know what sort of personal information National Intermodal holds and collects, for what purposes, and how it is collected, held, used, and disclosed. Third parties or National Intermodal directors, employees and other individuals are also entitled to access to their own in

Purpose

This policy explains how National Intermodal must manage any personal information or sensitive information that is collected, used, stored, accessed, disclosed, secured, and destroyed, to comply with the requirements of the *Privacy Act 1988* (Cth) (Privacy Act), as amended, and related National Intermodal policies.

To comply with the Privacy Act, National Intermodal must adhere to the APPs (refer to Attachment A). The APPs govern the way that National Intermodal collects, uses, stores, and discloses personal information about an individual that it receives or collects from third parties or from its directors, employees and contract staff. The APPs do not apply to conduct directly related to an employment record of a current or former employee of National Intermodal.

This policy pertains only to personal and sensitive information of an individual as defined by the Privacy Act. When this policy refers to National Intermodal, it means National Intermodal and its related bodies corporate (as defined in the *Corporations Act 2001* (Cth)).

Policy

What information does National Intermodal collect?

Personal information is information or an opinion that identifies an individual or from which an identity can be reasonably ascertained whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not.

Generally, the types of personal information National Intermodal collects include name, contact details, identification information such as a date of birth, postcode, telephone numbers, email address, organisation, title, information in forms submitted to National Intermodal and your preferences regarding interactions with National Intermodal payment details and enquiry/complaint details.

The other types of personal information that National Intermodal collects depend on the nature of the dealings with National Intermodal. For example, National Intermodal may also collect and hold information about:

- **Job applicants** – information about qualifications, experience, character and screening checks (including health, reference, background, directorship, financial probity, identity, eligibility to work, vocational suitability and criminal record checks);
- **Employees/personnel** – in addition to the information about job applicants, records of phone, internet and email usage and where undertaken, records of optical surveillance and closed circuit television monitoring for security purposes, information relating to current or former employment or engagement including information about training, disciplining, resignation, termination, terms and conditions, emergency contact details, performance, conduct, payroll matters, union or professional/trade association membership, recreation, drug/alcohol tests, leave and taxation, banking or superannuation affairs.

Sensitive information is any personal information about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, philosophical beliefs, membership of political, professional or trade associations or trade unions, sexual preferences or practices, biometric templates or information used for automated biometric verification or identification, criminal record, or health. National Intermodal does not generally collect, use or disclose sensitive information about an individual but if National Intermodal does, it will be done so in accordance with law for example, where National Intermodal has received consent to do so, or the collection is required by law.

How is information collected?

National Intermodal may collect personal information if it is necessary for business purposes or to provide information and updates to individuals, at their request. If you have signed up for email updates on the delivery of the National Intermodal terminal, National Intermodal will also send you email updates. You can opt out of receiving updates at any time by using the 'unsubscribe' link in the updates.

Personal information may be collected verbally, in writing, by telephone, by email and through National Intermodal's website, including by monitoring and recording communications and interactions. For purposes including security, dispute resolution and training, National Intermodal may operate video and audio surveillance devices in its premises.

National Intermodal endeavours to collect personal information directly from the individual except where it is not reasonably practical to do so. In some cases, National Intermodal collects personal information from third parties including public sources, information service providers and third parties providing services to National Intermodal. Individuals may use a pseudonym when dealing with National Intermodal so as not to be identified fully to us, noting that National Intermodal may be unable to provide certain services without an individual's correct identity.

Where personal information is provided to National Intermodal by a third party, the individual to whom the information relates must provide consent for the personal information to be collected and stored by National Intermodal in accordance with this Privacy Policy.

National Intermodal may also collect personal information (including sensitive information) from or about individuals when legally required or authorised to do so. National Intermodal will hold personal information from or about individuals electronically and in paper form.

In general, National Intermodal's website can be visited without revealing any personal information. The server address, domain name, date and time of visit and the pages visited may be recorded.

How is information used?

Personal information may be stored in National Intermodal's systems (and those of National Intermodal's IT service provider) and may be used for a number of purposes connected with National Intermodal's business, depending on the circumstances in which it was collected. This includes but is not limited to National Intermodal using the information:

- to verify identity;
- to manage National Intermodal's relationship with the person;
- to maintain and update National Intermodal's records;
- to protect 's lawful interests;
- in connection with suspected fraud, misconduct and unlawful activity under specific Australian legislation (including the *Crimes Act 1914* (Cth), *Customs Act 1901* (Cth), the Rail Safety National Law);
- in connection with acquisitions or potential acquisitions of its business;
- in connection with job applicants, to assess applications and consider or make contact about other positions;
- in connection with employees, for purposes relating to employment or engagement including terms of engagement, training, disciplining, payroll, superannuation, health and safety, administration, insurance (including Workcover) and staff management;
- in connection with an email message sent, to respond to the email;
- to gather demographic information about National Intermodal's website visitor trends; and
- any other purpose that would reasonably be expected.
- National Intermodal may not be able to provide services without using personal
- information

National Intermodal may not be able to provide services without using personal information.

How do we protect personal information?

National Intermodal is committed to safeguarding all personal information that is provided to it.

National Intermodal holds all personal information securely and restricts access to a limited number of employees who require access to perform their duties or fulfil National Intermodal's functions. Most personal information held by National Intermodal is stored electronically on databases, shared drives, and in emails, or physically on hard copy files.

A range of reasonable precautions are taken to protect the security of data supplied from misuse, loss, unauthorised access, modification, or disclosure. No internet, transmission or technology is ever completely secure or error-free. In particular, emails sent to or from the National Intermodal website may not be secure. Internally, strict controls and procedures are in place to ensure that the privacy and security of personal information provided to National Intermodal is protected.

We train our staff in how to keep personal information safe and secure. We use secure systems and buildings to hold your information. We only keep your information for as long as we need it.

Here are some examples of the things we do to protect personal information.

Staff training	We train our staff in how to keep personal information safe and secure.
System security	<p>We have firewalls, intrusion detection and virus scanning tools to help prevent viruses, malware and unauthorised people accessing our systems.</p> <p>When we send electronic data to other organisations, we take steps to make keep personal information safe such as using secure networks or encryption.</p>
Service providers	When we use service providers that handle or store data, we require them to take steps to keep personal information safe and use it appropriately.
Building security	We use a mix of secure floor access and other controls to protect our office.
Destroying or de-identifying data when no longer required	We aim to keep personal information only for as long as we need for our business or to comply with the law. When we no longer need information, we take reasonable steps to destroy or de-identify it.

Sharing information with other organisations

National Intermodal may share personal information with people and organisations that help National Intermodal with its business, such as professional advisors, IT support, and corporate and administrative services. National Intermodal only does this where it is necessary for the services to be able to be provided to us. When National Intermodal does this, it takes steps to ensure that its service providers are required to protect your personal information.

National Intermodal may share personal information with:

- its wholly owned subsidiaries, the Commonwealth of Australia including National Intermodal's shareholders (Minister for Finance and Minister for Infrastructure and Regional Development);
- representatives of National Intermodal or third parties to whom personal information has been provided;
- contractors and service providers which assist National Intermodal with, among other things, archival, auditing, accounting, legal, business consulting, banking, payment, delivery, data processing, data analysis, recruitment providers, external communications, community and stakeholder management, research, investigation, website and technology services;
- regulatory bodies for the purposes of seeking any relevant regulatory approvals;
- National Intermodal's insurers;
- the Australian Securities and Investments Commission and other government agencies, as required by law;
- anyone authorised by those to whom the personal information relates;
- solicitors and other parties where National Intermodal is subpoenaed to provide the information; and
- IT service providers in the following countries: USA, South Africa, Ireland and various countries within South East Asia.

National Intermodal will only disclose personal information for other purposes with consent, if the disclosure is required or authorised by law, or otherwise in accordance with the Privacy Act. National Intermodal will generally only disclose personal information to an overseas entity with agreement, or if we are required or authorised by law to do so. National Intermodal expect such parties to comply with Australia privacy law.

Direct marketing

National Intermodal wants to communicate only if individuals who opt-in want to hear from us. If an individual prefers not to receive community and stakeholder engagement information, please contact National Intermodal.

Is the information we hold accurate?

Reasonable steps are taken to ensure that all personal information is accurate, complete, and up to date whenever National Intermodal receives or uses it.

Notification should be provided to National Intermodal of a change to personal information or if the information held is incorrect or incomplete.

Storage and Security

National Intermodal takes reasonable steps to protect the security of the personal information we hold, including by:

- regularly assessing risks relating to misuse, interference, loss and unauthorised access, modification or disclosure of information;
- maintaining audit trails of access, modification, and deletion of electronic records of information; and
- undertaking regular privacy and data security audits.

National Intermodal will hold your information for as long as is required by our business operations and relevant laws, including under the *Archives Act 1983*. When we are no longer required to hold your personal information, we will destroy or de-identify it.

Loss of personal information

Despite our every effort to protect your personal information, there remains the possibility that a breach of our security could occur. In the event of loss of personal information National Intermodal will:

- Seek to rapidly identify and secure the breach to prevent any further breaches;
- Engage the appropriate authorities where criminal activity is suspected;
- Assess the nature and severity of the breach including the type of personal information involved and the risk of harm to affected individuals;
- Notify the affected individuals directly if appropriate and where possible;
- If appropriate, put a notice on our website advising of the breach; and
- use reasonable efforts to contact you promptly and to notify the Australian Privacy Commissioner (at the Office of the Australian Information Commissioner, an independent statutory authority that administers NSW's legislation dealing with privacy and access to government information) if we become aware that a third party has accessed or used your personal information without authorisation, otherwise known as an eligible data breach, likely to result in serious harm and where National Intermodal has been unable to prevent the likely risk of serious harm with remedial action.

Review of Privacy Policy

The Privacy Policy may be reviewed and revised from time to time to take account of new laws and changes to National Intermodal's operations and practices. National Intermodal reserves the right to modify or amend the Privacy Policy at any time. National Intermodal may notify changes to the Privacy Policy by publishing an updated version on our website.

How can you access and correct personal information?

National Intermodal will provide access to correct or update any personal information upon request, subject to certain legal exceptions. National Intermodal may ask the requestor to verify his or her identity and to specify the information required. To obtain access to personal information held by National Intermodal, please write to:

Company Secretary
National Intermodal Corporation Limited
Suite 3, Level 33
1 O'Connell Street
Sydney NSW 2000

Email: companysecretary@nationalintermodal.com.au

Phone: 02 8265 5600

Privacy Officer and Privacy Champion

National Intermodal has appointed the Company Secretary as the 'Privacy Officer' and 'Privacy Champion' as required by the *Privacy (Australian Government Agencies – Governance) APP Code 2017*.

The Privacy Officer is the primary point of contact for privacy matters.

Additional Information

Additional information about privacy is available at:

- The Office of the Australian Information Commissioner: http://www.oaic.gov.au/privacy-portal/about_privacy.html
- Summary of the APPs: <http://www.oaic.gov.au/privacy/privacy-act/australian-privacy-principles>
- [About the Notifiable Data Breaches scheme: https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/](https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/)
- [Reporting a data breach: https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach](https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach)

Alternatively, you may wish to discuss privacy further with the Company Secretary.

Document Status

Version	Prepared By	Reviewed By	Date Reviewed	Endorsed	Approved
1.0	A. Lowe	A. Lonsdale	September 2013		
2.0	A. Lowe	I. Hunt	February 2014		
3.0	S. McMahon	J. Webster	August 2015	Audit & Risk Committee, meeting held 8 May 2015	Board Meeting held 26 June 2015
4.0	J. Webster	I. Hunt	November 2017	Audit & Risk Committee meeting held on 7 December 2017	Board meeting held on 13 December 2017
5.0	R. Khoury Gebrail	J. Webster	April 2020	Audit & Risk Committee 28 April 2020	Board meeting 28 April 2020
6.0	K Gill	J. Webster	July 2021	Audit & Risk Committee 29 July 2021	Board meeting 29 July 2021

Attachment A – Australian Privacy Principles

Australian Privacy Principles — a summary for APP entities

from 12 March 2014


 Australian Government
 Office of the
 Australian Information Commissioner

APP 1 — Open and transparent management of personal information
Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information
Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information
Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information
Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information
Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

www.oaic.gov.au

For private sector organisations,
Australian Government
and Norfolk Island agencies
covered by the *Privacy Act 1988*