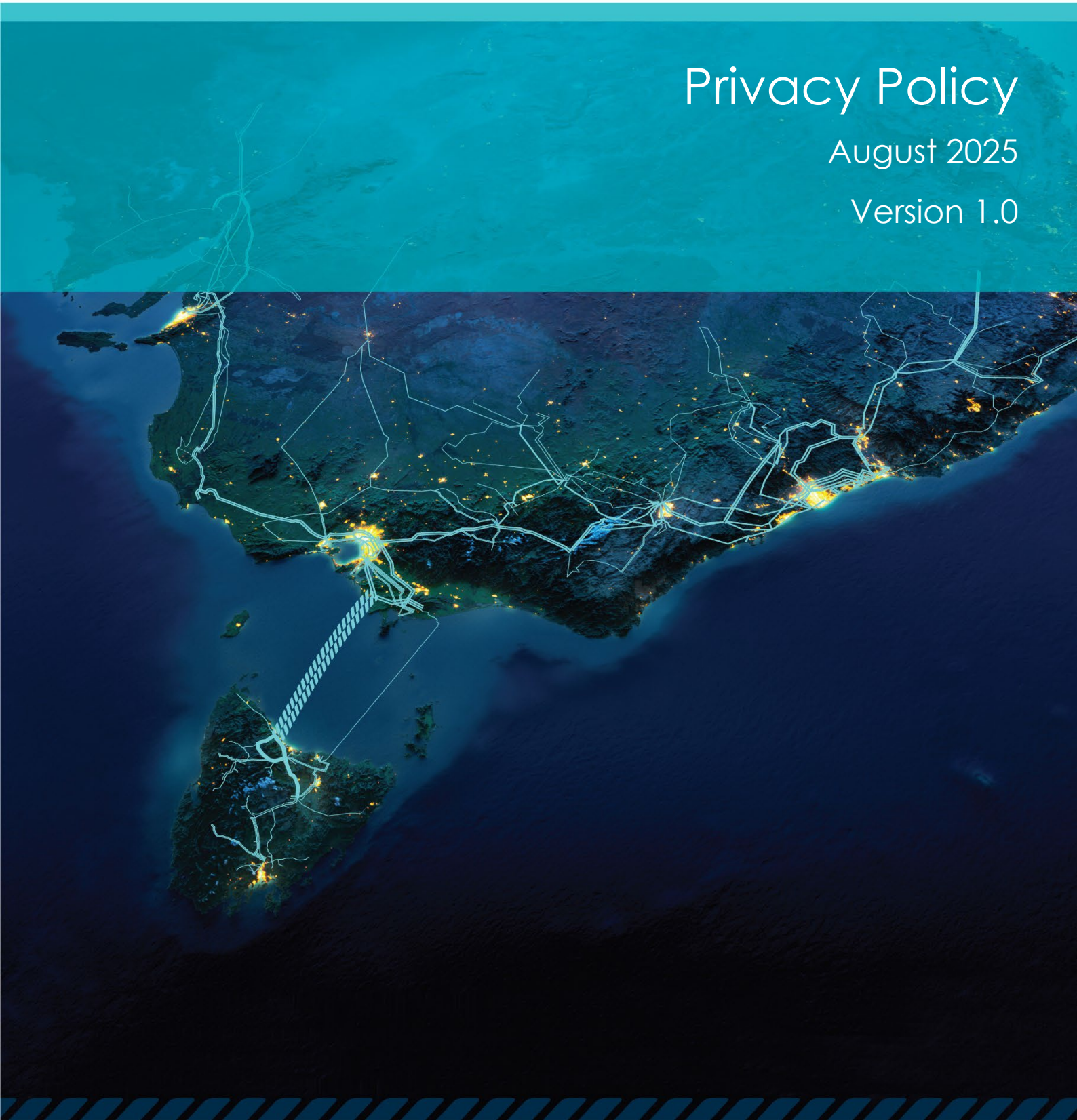




Privacy Policy

August 2025

Version 1.0



Contents

| | | |
|----------|--|-----------|
| 1 | Introduction..... | 3 |
| 1.1 | Overview | 3 |
| 1.2 | Purpose of this Privacy Policy | 3 |
| 2 | Who does this Privacy Policy apply to? | 3 |
| 3 | The kinds of personal information we collect and hold | 3 |
| 3.1 | What is personal information and sensitive information? | 3 |
| 3.2 | The personal information we collect from you | 4 |
| 3.3 | Sensitive information | 5 |
| 4 | How we collect your personal information..... | 5 |
| 4.1 | Collecting personal information from you | 5 |
| 4.2 | Collecting personal information from other sources..... | 6 |
| 4.3 | Notifying you when we collect your personal information..... | 6 |
| 4.4 | Use of tracking tools | 6 |
| 4.5 | If you do not provide your personal information..... | 7 |
| 5 | Why we collect and use your personal information | 7 |
| 5.1 | How we use or disclose personal information | 7 |
| 5.2 | Other uses | 8 |
| 5.3 | Disclosing personal information to third parties..... | 8 |
| 5.4 | Disclosing personal information overseas | 9 |
| 6 | Marketing..... | 9 |
| 6.1 | Direct marketing..... | 9 |
| 6.2 | Targeted advertising..... | 10 |
| 7 | How we protect your personal information | 10 |
| 7.1 | How your personal information is stored..... | 10 |
| 7.2 | What happens when we no longer need your personal information..... | 11 |

| | | |
|------|--|----|
| 8 | Notifiable Data Breaches | 11 |
| 9 | How you can access and correct your personal information..... | 11 |
| 9.1 | How you can access your personal information | 11 |
| 9.2 | How you can request a correction | 11 |
| 9.3 | If we refuse your request for access or correction | 12 |
| 10 | Anonymity | 12 |
| 11 | Complaints about how we handle your personal information | 12 |
| 11.1 | How you can make a complaint..... | 12 |
| 11.2 | If your complaint is not resolved..... | 12 |
| 12 | Administration of this Policy..... | 13 |

1 Introduction

1.1 Overview

The privacy of your personal information is a priority for us at Marinus Link Pty Ltd (ABN 47 630 194 562) (**MLPL, we, our or us**). We respect your right to privacy under the *Privacy Act 1988* (Cth) (**Privacy Act**) and any applicable State laws which may apply to our activities and operations from time to time and are committed to collecting and managing your personal information lawfully and transparently.

1.2 Purpose of this Privacy Policy

This Privacy Policy explains how we manage your personal information, the types of personal information we collect and the reasons we collect it, how we generally use and disclose your personal information and how we store and protect it. This Privacy Policy also explains how you can access and correct the personal information that we hold about you and how you can make a complaint if you have concerns about how MLPL has dealt with your personal information.

2 Who does this Privacy Policy apply to?

This policy applies to all of the people whose personal information we collect, including but not limited to MLPL employees, contractors, service providers, stakeholders, sponsors and business partners, landowners (i.e. persons with interests in land or property that may be affected by our operations), job applicants, users of MLPL's websites or social media pages and any other individual that interacts with us.

We may change this Privacy Policy at any time by publishing an updated version on our website with all changes effective from the date of posting, unless otherwise stated.

We encourage you to review and check our website regularly for any updates to this Privacy Policy.

3 The kinds of personal information we collect and hold

3.1 What is personal information and sensitive information?

In this policy:

- **“Personal information”** means any information about an identified or identifiable person. This includes where you can be identified, directly or indirectly, including by reference to an identifier (for example, a name or email address, or an online identifier such as a unique device identification number).
- **“Sensitive information”** means personal information defined as sensitive in the Privacy Act such as information regarding your racial or ethnic origin, religious affiliation, health information, criminal record, or membership of a trade association or union.

3.2 The personal information we collect from you

The types of personal information we collect about you may include:

- **Contact and identifying information**, such as your name and surname, postal address, email address, phone number, preferred language, employee identification numbers, licence or passport numbers, emergency contact information, social media handles or profiles, or other similar identifiers.
- **Demographic information** such as your date of birth, gender, age or ethnicity or Indigenous status (where necessary to ensure we meet our diversity and inclusion commitments or our legal obligations).
- **Financial and payment information** such as bank account, credit card or other payment details, creditworthiness checks, financial probity information, transaction history or tax-related information.
- **Land ownership or occupation details** such as any personal information collected in connection with potential property transactions or other dealings through verifying real property details such as volume and folio numbers, property IDs, maps and imagery, land usage information, access points and routes, subdivisions and plans, and information relating to traditional owners.
- **Internet or other electronic network activity and data** such as your internet protocol address, browser type, language, internet service provider, referral page, operating system, time and date stamp, the cookies that are installed on your device or other tracking data, web beacons or log files, your interaction with advertisements, websites or social media content or search terms that referred you to our website.
- **Geolocation data** such as location information while using our websites or location data gathered in connection with your interactions with MLPL, providing services to MLPL, or your usage of MLPL’s devices or equipment.
- **Opinions/sentiment information** about your views and values or personal information gathered through complaint resolution.

- **Health information** such as health fund information, and health information as it relates to employment or collected for workplace, health and safety purposes such as fatigue management, incident investigations or in connection with drug and alcohol testing.
- **Photographs, audio recordings and video footage, or biometric data** such as imagery containing faces, identifying features (about you or your vehicle) or voices, or other biometric data for the purposes of identity verification (such as fingerprints), workplace surveillance or security purposes (such as via CCTV). Photographs, audio recordings and video footage may also be used for promotional or quality assurance purposes.
- **Recruitment or employment related information** such as superannuation information, tax information, citizenship or residency status, proof of right to work in Australia, emergency contact information, eligibility to work or any personal information incidental to the employment relationship.
- **Qualifications, accreditations or authorisations** such as university accreditations, training accreditations, education, job specific qualifications or skills, information regarding previous employment or directorship, police checks, working with vulnerable people checks, visa checks, criminal record checks, Australian Security Intelligence Organisation (ASIO) clearances for workers accessing critical infrastructure.
- **Any other personal information** you voluntarily provide to us.

3.3 Sensitive information

Unless required by law, we will only collect sensitive information with your consent.

4 How we collect your personal information

4.1 Collecting personal information from you

We may collect your personal information directly from you in person, over the internet, via email, in writing, through telephone conversations or through your interactions with MLPL's systems or operations, including:

- when you procure our services or provide us with products or services;
- when you interact with us as part of our commercial or operational activities;
- when you request information from us or provide information to us;
- when you participate in our community, stakeholder engagement or sponsorship activities;

- in connection with your employment, or other relationship with us or with one or more of our stakeholders;
- when you apply to work with us (whether as an employee, contractor or service provider);
- when you access any of our physical sites or online services, including through our mobile apps, website, our social media content or online application forms.

4.2 Collecting personal information from other sources

We may also collect your personal information from publicly available sources or from third parties as permitted by law. For example, via address validation software, marketing companies, service providers, authorised representatives appointed by you, our related entities, regulatory or government agencies, recruitment agencies, current or former employers, credit reporting bodies, internet searches or any other organisation or person you ask us to collect your personal information from.

4.3 Notifying you when we collect your personal information

If we collect your personal information from third parties in circumstances where you may not be aware that we have collected your personal information, and that information can be used to identify you, we will take reasonable steps to notify you of the collection and the circumstances that surround the collection.

4.4 Use of tracking tools

We may use cookies, web beacons, log files or other similar tracking tools on our website to collect information about how our website is being used.

- **Cookies** are text files placed into your computer's browser to store your preferences. These cookies collect information on how you and other visitors use our website.
- **Web beacons** are small pieces of code placed on a web page to monitor visitors' behaviour and collect data about the visitors viewing our website.
- **Log files** track actions occurring on the website and collect data including your IP address, browser type, Internet service provider, referring/exit pages and date/time stamps.

Most browsers are initially set to accept cookies, web beacons or other tracking tools. If you prefer, you can set your browser to refuse these by selecting the appropriate settings or blocking, deleting or disabling them if your browser or device permits.

4.5 If you do not provide your personal information

If you do not provide us with your personal information when requested, this may limit the interactions we are able to have with you. For example, we may not be able to:

- do business with you such as engaging your services (or the services of an organisation you have an association with);
- provide the service or information you requested;
- handle enquiries or complaints in connection with our activities; or
- process your job application.

5 Why we collect and use your personal information

5.1 How we use or disclose personal information

We use or disclose personal information for a variety of purposes to effectively conduct our business including:

- verifying your identity and personal information;
- providing services or information to you or someone else;
- facilitating our internal business operations (including managing employees or contractors or for workplace health and safety, emergency or compliance purposes);
- analysing our offerings and stakeholder needs with a view to continuous improvement in our business activities, or optimising our operations, physical sites, engagement activities with strategic stakeholders, webpages and social media content;
- to communicate with you, including to provide you with information about MLPL, our operations and activities and to respond to your questions or complaints;
- facilitating community and stakeholder engagement activities;

- to market our business, our activities or the Marinus Link project to you, including via the internet (for example, via social media or online platforms), by phone, email or direct mail, subject to providing you with an opt out ability as required by law;
- developing, operating, maintaining and upgrading our assets and infrastructure, including works which may occur on your property or which may affect your property;
- forming and administering the contractual arrangement in place between us (or another organisation you have an association with);
- managing safety and security risks including restricting and monitoring access and use of our sites (for example, via CCTV) or our information technology assets (for example, through monitoring electronic communications);
- to comply with any applicable laws, regulations or codes of practice, including but not limited to, in respect of our reporting obligations under all such requirements;
- to respond to law enforcement requests and as required by applicable law, court order, governmental regulations, or other lawful processes;
- as necessary or appropriate to prevent or investigate any actual or suspected fraud, unlawful activity or misconduct or protect the rights, property, security, and safety of us, our employees, our contractors, our consumers, our information systems and the public.

5.2 Other uses

We may also collect and process your personal information for any other purposes for which you have provided your consent or if there is another lawful basis for doing so.

5.3 Disclosing personal information to third parties

To help us carry out our business functions, we may disclose personal information about you to third parties, including:

- our suppliers and service providers, including those we have engaged to support the Marinus Link project;
- a financial institution;
- our advisers, consultants and contractors;
- prospective purchasers of all or part of our business or assets;

- identity, background, right to work, credit or fraud-checking agencies and service providers who assist us with our business;
- Government, regulatory or public sector bodies (as required or authorised by law);
- third parties for the purpose of confirming matters associated with safety or compliance (including, in relation to your training, authorisations and competencies);
- people you have authorised to interact with us on your behalf (such as recruitment agencies or your professional advisors);
- law enforcement agencies (as required or authorised by law); and
- any other person where you have given your consent.

We will take reasonable steps to ensure that these third parties are bound by confidentiality and privacy obligations in relation to your personal and confidential information.

We will not sell, gift, rent or trade your personal information to anyone.

5.4 Disclosing personal information overseas

We may store personal information with, or disclose personal information to, third party service providers located overseas.

Where we disclose personal information to a third party which is located overseas or which will hold personal information overseas, we will take reasonable steps to ensure that the overseas recipient of such personal information handles it in accordance with the standards required under the Privacy Act and ensure that the recipient is subject to binding contractual obligations.

6 Marketing

6.1 Direct marketing

We may use your personal information to provide you with information about us, the Marinus Link project or related matters which may interest you. If you do not wish to receive marketing material from us, you may:

- contact the Privacy Officer; or
- opt-out of receiving further marketing material via any opt-out mechanism contained in our marketing correspondence.

6.2 Targeted advertising

We may use your personal information to provide you with targeted advertisements, or for the purposes of online behavioural based marketing, to provide you with information about us or the Marinus Link project. You can find more information about how targeted advertising works from the Office of the Australian Information Commissioner. If you do not wish to receive targeted advertising on the following platforms, you can opt out by using the opt out features of the individual platforms, which as of the date of this policy include:

- [Facebook](#);
- [Google](#);
- [Pinterest](#);
- [LinkedIn](#);
- [Meta](#);
- [Amazon](#); and
- [Microsoft](#).

7 How we protect your personal information

7.1 How your personal information is stored

We store your personal information in paper and electronic form.

The security of your personal information is important to us. We safeguard your personal information and protect it from misuse, unauthorised access, disclosure or interference by maintaining physical security measures (by restricting access to systems or buildings to authorised persons), electronic security systems (such as firewalls, data encryption, antivirus protections and other measures) and backup and recovery systems to deal with major business interruptions.

We impose confidentiality obligations on our employees, consultants and contractors, as well as providing them with training and requiring them to comply with strict privacy and security policies and procedures in accordance with industry standards.

We periodically review our information security practices and safeguards and update as required.

7.2 What happens when we no longer need your personal information

Unless the law requires otherwise, we will take reasonable steps to destroy or permanently de-identify personal information if it is no longer required.

8 Notifiable Data Breaches

If we become aware of a suspected personal information data breach, we will conduct an appropriate assessment to determine if there is a likely risk of serious harm to any individual associated with the data breach. Where we believe there is a likely risk of serious harm, we will notify the Office of the Australian Information Commissioner and any affected individuals in accordance with our obligations under the law.

9 How you can access and correct your personal information

9.1 How you can access your personal information

You may request access to the personal information we hold about you by contacting our Privacy Officer.

We will acknowledge your request for access within 14 days of its receipt and give you access within 30 days in the manner you request if it is reasonable and practicable to do so, unless we have a lawful reason for refusing. For example, we may need to refuse to grant you access if providing this access may disclose personal information about another person.

We may need to verify your identity before we give you access to your personal information. Depending on the nature of the request, we may charge you a small fee to access that information.

9.2 How you can request a correction

You may ask us to correct any personal information about you which you think is inaccurate, incomplete, out of date or misleading. We will respond to a correction request within a reasonable time.

If we correct your personal information that we have previously disclosed to another entity, and you ask us to tell the other entity about the correction, we will take reasonable steps to tell the other entity about the correction, unless it is impractical or unlawful to do so.

9.3 If we refuse your request for access or correction

If we refuse to allow you access to your personal information or to correct that information, then we will provide you with the reasons for our decision as required by the Privacy Act. We will also inform you of mechanisms available to complain about the refusal.

10 Anonymity

You have the option to remain anonymous, or to use a pseudonym when dealing with us where it is lawful and practical to do so. However, without your personal information we may not be able to interact with you as you require (for example, we may not be able to appropriately respond to your request or complaint).

11 Complaints about how we handle your personal information

11.1 How you can make a complaint

If you have any complaints about our privacy practices or would like further information, please contact our Privacy Officer:

Privacy Officer

Telephone: 1300 765 275

Mail: GPO Box 721, Hobart, TAS 7001

Email: Privacyofficer@marinuslink.com.au

Complaints and enquiries about the treatment of personal information (including a possible breach of privacy) by us must be made in writing (a letter or email), addressed to the Privacy Officer. We will treat complaints confidentially. We will respond within a reasonable time after receipt of the complaint (usually 30 days).

11.2 If your complaint is not resolved

If you are not satisfied with the outcome of the Privacy Officer's investigation or we have not replied to you within a reasonable time, then you can raise your concern with the Office of the Australian Information Commissioner in Australia. Complaints can be made in the following ways:

Office of the Australian Information Commissioner

Telephone: 1300 363 992

Email: enquiries@oaic.com.au

Mail: Office of the Australian Information Commissioner

GPO Box 5218, Sydney, NSW 2001, Australia

Online: www.oaic.gov.au/privacy/making-a-privacy-complaint

12 Administration of this Policy

This Privacy Policy is administered by Governance and Compliance and will be reviewed and approved every two years or updated where applicable.

A handwritten signature in black ink that reads "Stephanie McGregor".

Stephanie McGregor

19 August 2025

Chief Executive Officer

Marinus Link Pty Ltd