Ethos Health – Privacy Policy

About this Privacy Policy

This is the Privacy Policy for Ethos Health Pty Ltd ABN 91 137 759 310 (Ethos Health, us, we, our).
Ethos Health is committed to protecting your privacy in accordance with the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs), and Australian state health records legislation.

Our Role: Data Controller vs. Data Processor

Data Controller: Ethos Health acts as a Data Controller in respect of Personal Information collected directly through our website, direct customer interactions, marketing activities, and administrative operations.

Data Processor: Where Ethos Health provides Software-as-a-Service (SaaS) or Platform-as-a-Service (PaaS) applications, or mobile applications to our corporate clients, enterprise partners, or program sponsors—for health, wellbeing, preventative care, or workplace health and safety purposes—that organization is the primary Data Controller. Ethos Health processes and hosts that information on their behalf in accordance with our contractual agreements with them.

This Privacy Policy explains what Personal Information we collect, how we handle and protect it, and the rights available to you.

This Privacy Policy was last reviewed on ***16th October 2026***. We may update this policy periodically, and updated versions will be published on our website. Where required by law, we will notify you of material changes.

What Personal Information Do We Collect?

General Personal Information

We collect general identification and contact details, including:

- Full name, email address, postal address, and telephone number;
- Date of birth, age, and gender; and
- Employment details, job title, and employer/contractor name.

Sensitive & Health Information

Due to the nature of our SaaS/PaaS platforms and workplace health and safety services, we may collect **Sensitive Information** (specifically health information). This may include:

- Medical assessments, injury reports, and health monitoring data;
- Physical health, movement, or fitness-for-work measurements; and
- Workplace incident and safety management entries.

We only collect Sensitive Information where it is reasonably necessary for one of our primary functions or activities, and where you have provided **explicit consent**, or where the collection is required or authorized by law (such as under applicable occupational health and safety legislation).

How We Collect and Store Your Personal Information

How We Collect Information

We collect Personal Information through various channels, including:

- Direct submissions via our website, user registration forms, and SaaS/PaaS platforms;
- Interactions and data entry through our mobile applications;
- Communications with you, including emails, customer support requests, and phone calls; and
- Automated website analytics and cookies (see Section 7).

Where permitted and practical, you may interact with us anonymously or using a pseudonym. However, if you choose not to provide required Personal Information or health data, we may be unable to provide you with access to our SaaS/PaaS platform, health services, or customer support.

How We Store and Retain Information

We store Personal Information across secure digital systems, hard copy files, and website databases. Some systems may be hosted by vetted third-party service providers.
We retain Personal Information only for as long as necessary to fulfill the purposes for which it was collected, or as required by Australian law. **Please note:** Medical and workplace health records are subject to statutory retention periods under Australian federal and state legislation (often requiring retention for a minimum of 7 years, or longer for specific workplace health exposures).
When Personal Information is no longer required, it is destroyed or permanently de-identified using secure methods.

How We Use Your Personal Information

We collect, hold, use, and disclose Personal Information for the following primary purposes:

- Providing and maintaining our SaaS/PaaS platforms for workplace health and safety management;
- Delivering workplace health monitoring and reporting services;
- Supplying identified or aggregated safety reports to your employer or contracting business (where they have engaged our services for your workplace);
- Responding to inquiries and providing customer support;
- Sending system notifications, updates, and operational communications; and
- Direct marketing (where you have opted in or as otherwise permitted by law).
- We also use Personal Information for internal operations, including:
- System maintenance, auditing, and compliance checks;
- Security monitoring, fraud prevention, and vulnerability assessments; and
- Product improvement, feature development, and usage trend analysis.

De-identified Information

We may de-identify and aggregate data using standard anonymization processes so that individuals cannot reasonably be re-identified. We may use this de-identified, statistical data for research, product improvement, or publication purposes.

Data Sovereignty, Security & Overseas Transfers

Primary Data Residency (Sydney, Australia)

All primary databases, software applications, and customer data associated with our PaaS and SaaS platforms are hosted in secure data centres located in **Sydney, Australia**. We prioritize keeping core personal and health information onshore to satisfy strict data sovereignty requirements.

ISO 27001 Security Framework

Our PaaS and SaaS platform operations and data management processes form part of our **ISO 27001 certified Information Security Management System (ISMS)**. This ensures that your personal and health information is protected by internationally recognized security controls, rigorous threat monitoring, and regular independent auditing.

Third-Party Service Providers

In limited operational circumstances, specific supporting tools—such as transactional email delivery services, customer support portals, or VoIP platforms—may utilize third-party infrastructure hosted outside Australia (primarily in the **United States** or the **European Union**).
Where third-party service providers process data on our behalf outside Australia, we enforce appropriate safeguards through our ISO 27001 vendor management protocols. This includes formal data protection agreements that comply with Australian Privacy Principle 8.

Social Media and External Links

Our website may contain links to third-party social media platforms, blogs, or external websites. Information you submit on third-party platforms is governed by the privacy policies of those specific providers. We are not responsible for the privacy practices or content of third-party platforms.

Cookies and Tracking Technologies

We use cookies and similar tracking technologies to operate and improve your experience on our website and SaaS/PaaS platforms.

How We Use Cookies

Essential Cookies: Necessary for platform operation, sign-in authentication, and secure session management.

Analytics Cookies: To track site performance, traffic sources, and user engagement.
You can manage or disable cookies through your browser settings. Disabling essential cookies may impact platform functionality or prevent full access to our software tools.

Accessing and Correcting Your Personal Information

Under the Australian Privacy Principles (APPs 12 and 13), you have the right to request access to the Personal Information we hold about you and to request that we correct any details that are inaccurate, out-of-date, incomplete, irrelevant, or misleading.

Making a Request: To request access or correction, contact our Privacy Officer using the details in Section We will respond to your request within a reasonable period (usually within 30 days).

Costs: We do not charge a fee for making an access or correction request. We may charge a reasonable administrative fee for retrieving and providing copies of your information if the request is complex or resource intensive.

Exceptions: In certain circumstances permitted by law (for example, where providing access would pose a serious threat to life or health, or would unreasonably impact the privacy of others), we may refuse access. If we refuse, we will provide you with written reasons.

Opting Out of Marketing: You may opt out of receiving direct marketing communications at any time by using the "unsubscribe" link in any marketing email or by contacting us directly.

Complaints Procedure

If you believe Ethos Health has breached the Australian Privacy Principles or mishandled your personal or health information, please contact us using the details below.
We take all privacy concerns seriously. We will acknowledge receipt of your complaint promptly and will use our best efforts to investigate and respond within **5 business days**.
If you are not satisfied with our response or how your complaint was handled, you may lodge a formal complaint with the **Office of the Australian Information Commissioner (OAIC)**:

Website: www.oaic.gov.au
Telephone: 1300 363 992
Post: GPO Box 5218, Sydney NSW 2001

Contact Us

If you have questions, wish to exercise your rights, or want to make a privacy complaint, please contact our Privacy Team:

Email: enquiries@ethoshealth.com.au
Web Form: https://ethoshealth.com.au/contact
Postal Address: Ethos Health Pty Ltd, Level 1, 21 Annie St, Wickham, NSW 2293, Australia