Privacy Policy

TrustWorks 360 (**TW360**) is a privacy, information security, and trust solutions provider based in Sydney, Australia. In this policy, “TW360”, “we”, “us”, “our”, “ours” refers to TrustWorks 360 Pty Ltd, ACN 140 022 373

Our services are to match our clients with curated technical and business process management solutions offered by our partners, and to assist with solution implementation and provide ongoing client support.

We acknowledge the value that our partners and clients and, in turn, their customers and employees, place on strong privacy practice and ensuring the confidentiality integrity, and availability of personal information and related critical services.

TW360 is an Australian company. As such, we apply the privacy principles of the *Australian Privacy Act 1988* (Cth) (**Privacy Act**) in our collection and handling of personal information – that is, information that identifies a person or could reasonably lead to them being identified. We also seek to exceed the requirements of other law that protects personal information such as the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth).

This Privacy Policy provides details about our personal information handling practices to support our transparency obligations under the Privacy Act, as well as other data protection laws that may apply where we collect, and store personal information of people located outside of Australia.

This Policy Privacy applies only to TW360. The privacy practices of our partners are set out in their own privacy policies accessible via their website link on the TrustWorks360 website.

Personal information collected and used

We don’t collect much personal information, but when we do, we use it to provide services to you and to help us to carry out our business.

How we collect, store, use and disclose this information depends on our relationship with you – where you are a:

- Website visitor
- Partner or prospective partner
- Client or prospective client, or a
- Person contacting us to submit a query or request.

In these relationships, we either:

- Collect personal information directly from you and are fully responsible for our control of the information, or
- Obtain personal information from our clients when we manage it for them and on their behalf (i.e., our management of the information is dictated by the terms of a service contract (**Client-provided data**)).

We collect and deal with personal information as follows:

Collected from	What is collected	Why we collect and manage it
Website visitors *When you visit or interact with our website*	• Your server and IP address • The name of the top-level domain (for example, .gov, .com, .edu, .au) • The type of browser used • The date and time you accessed our website • The pages accessed and documents downloaded • The specific referring website which directed you to our website	To understand how you interact with our website (**Analytics data**) To conduct analytics (at an aggregate level) to improve our website, services, features or other offerings Better understand website visitors' needs, interests and suitability for various products and services Recommend specific products and services that may be of benefit Respond to issues, questions and queries
Partners and prospective partners *When you are the representative for a partner privacy, information security or trust solution provider, or when you are exploring the possibility of partnering with us*	• Name • Contact details • Business name • Position title and work responsibilities • Nature of services provided or to be provided • Account details (if this involves client log-ins) • Invoicing, banking or credit facility details **(Payment data)**	To manage the current or prospective business relationship, including to: • Contact you directly for a business purpose • Respond to your queries • Process transactions associated with our partnership • Provide clients with ongoing service delivery and support

Collected from	What is collected	Why we collect and manage it
Clients and prospective clients *When you are the contact person for a client (e.g., an organisation, company, corporation, government department or agency) or when you are exploring becoming a client*	• Name • Contact details • Business name • Position title and work responsibilities • Nature of services sought or provided • Account details (if this involves client log-ins) • Invoicing, banking or credit facility details (**Payment data**)	To manage the business relationship and administer delivery of services, including to: • Contact you directly for a business purpose • Respond to your queries • Process transactions associated with our services • Provide you with ongoing service delivery and support
Customer, contractor or employee of a client *When this information is contained in data we manage for our clients (***Client-provided data***)*	• The personal information will be dictated by the service contract with our client	Delivery of contracted services to our client, potentially including: • Establish the identity of our clients' customers, contractors and employees • Perform necessary identity and security verifications • Provide ongoing service delivery • Respond to issues, questions and queries • Protect people (e.g., our client's customers) from information security incidents • Co-operate with legal authorities as necessary to comply with applicable laws
People contacting us to submit a privacy or security query, complaint or rights request	• Name • Contact details • Nature of the contact made • Details relating to the contact made	Fulfilment of these administrative functions

Analytics data - *more information*

For analytics, we use cookies, web beacons and clickstreaming.

Cookies – Cookies are identifiers that can be sent from our website via your browser to your device's data store. You can elect not to accept cookies by changing the designated settings on your web browser; however, disabling cookies may prevent you from using

certain functions and features of our website. Information collected from the use of cookies is used to improve our online services.

Web beacons – Web beacons are small, graphic images that enables us to monitor user activity at an aggregate level. A web beacon is a very small pixel which is invisible to the user. The information collected through web beacons is not of a personal nature.

Clickstreaming – Clickstreaming enables us to analyse the paths that visitors take as they access our website and navigate its pages, and potentially, link to other sites.

Payment data – *more information*

We collect and manage payment information as part of the provision of our services. Payments are generally made when a client receives our invoice. however, online payments via our secure payment gateway can also be made.

TW360 uses secure payment provider, Stripe, to manage online payments in accordance with strict security and privacy protocols.

Client-provided data – *more information*

Client-provided data, including any personal information therein, is owned and controlled by our clients. We manage this information in accordance with the contractual requirements set by our clients (which includes our observance of information security controls, cyber incident reporting and data breach management/ reporting requirements).

Third party access to personal information

We do not sell personal information to third parties or otherwise provide it to them for their benefit.

In deploying our partner solutions, or in the fulfilment or delivery our services otherwise, we may (based on contractual arrangements) share personal information with TW360 partners, affiliates, subsidiaries, contractors and agents.

We may also be required or authorised to provide personal information to third parties (such as law enforcement or regulatory authorities) under a domestic or international law.

Our internal functions and activities

We handle personal information in the following primary ways as part of our internal functions and activities:

Work tools – Microsoft 365

We use Microsoft 365 to conduct our work, which includes handling documents and correspondence that contain personal information. We only use the following products and services: Exchange, OneDrive, SharePoint, Teams, Planner and Office

We have set up reasonable security safeguards including multi-factor authentication (MFA), role-based access controls, and promptly applying patches to applications and devices.

Our Microsoft 365 data is stored in Australia. Microsoft's Trust Center is located here.

Work tools – Hubspot

We use Hubspot as a Customer Relationship Management and Support ticketing system. This includes maintaining contact information and tracking of support and other client related activities. The Hubspot trust centre is located here

Work tools – Sales Flow

We use Sales Flow to engage with clients and prospects via Linked In. This includes messaging and providing content. The Sales Flow Privacy Policy is located here

Consent

Most of our handling of personal information is directed by our clients. However, where we control what happens to the personal information, we will not use or disclose it except as set out in this Privacy Policy unless you have consented, or we are required or authorised by law to do so.

Security, storage and retention

Security and storage

We implement physical, procedural and technical security with respect to our offices and information storage facilities to safeguard against loss, misuse, unauthorised access, disclosure, or modification of personal information. This also applies to our destruction of personal information.

A core value for us is respecting the confidentiality of the personal information we hold and manage. Only authorised personnel trained in privacy and information security have access to personal information.

Depending on the nature of our relationship with you, personal information may be stored or processed in jurisdictions where TW360 partners, affiliates, subsidiaries or agents maintain facilities. While predominantly, personal information (including back-ups) is stored in Australia, other jurisdictions may include: the US, Israel and the EU.

We encourage you to review our partner websites, solutions and privacy policies; however, we do not ensure the protection of any personal information that you provide to a website that may be referenced or linked by us. You are advised to undertake your own diligence before clicking on these links.

If you are concerned that TW360 may have been subject to a cyber incident or data breach, please notify us via the **Contact** information supplied below.

Retention

We retain personal information only if it is needed for efficient and effective solution delivery, fulfilment of our services otherwise, or TW360 administration (e.g., employee management and management rights requests) and for a reasonable time thereafter.

We securely destroy personal information when it is no longer needed – subject to any legislative or contractual requirements.

Data quality

We take reasonable steps to ensure that the personal information we use is accurate, complete and up-to-date. If you advise us that your information – including your contact details – have changed, we will promptly update the information.

Where your personal information is contained in client-provided data, we will pass on requests relating to your personal information to the relevant client.

Your rights

We support your ability to seek access to and correction of your own personal information (per the Privacy Act), and to ask us to act in relation to other information and privacy rights, including:

Your right	What is this?
Right to access	The right to request access to your personal information held by us
Right to correct	The right to seek correction of your personal information where you consider it is incorrect, incomplete, misleading or out-of-date
Right to erasure	The right to request us to delete all personal information we hold about you
Right to object	The right to object at any time to certain type of processing of your personal information
Right to data portability	The right to receive the personal information holds about you in an accessible format
Right to restrict processing	In certain circumstances, you have the right to restrict how we deal with your personal information.

Rights request or privacy complaint

You can contact us to make a **rights request** – that is, to request access to your personal information held by us, request a correction or amendment of your personal information and to ask us to act in relation to your other rights as noted above.

You also have a right to make a **privacy complaint** about our dealings with your personal information.

If you submit a rights request or make a privacy complaint, we may require you to verify your identity before we can proceed. We will collect and use your name, contact

information and details regarding your request or complaint to communicate with you and address your request or complaint.

We will not, however, deal with third parties seeking your information unless we have your express permission, or we are required by law to do so.

If you submit a rights request to us and the personal information is controlled by our client because of our contract with them, we will – with your permission – pass on the rights request to that client.

Contact

We are committed to treating your personal information with respect and consideration. Please contact us by email at contact@trustworks360.com if you:

- have any questions or concerns regarding this Privacy Policy
- believe the privacy of your personal information has not been respected and wish to make a privacy complaint
- wish to tell us about a potential security incident or data breach involving personal information held by us, or
- would like to make a rights request.

We will promptly acknowledge your contact and will respond to your specific query within thirty (30) business days (and sooner where this is required by law).

If you have made a **privacy complaint** to us and you are not happy with how we have responded, you can seek assistance from the Office of the Australian Information Commissioner (**OAIC**). The OAIC's process is available here.

Updates

We may update this Privacy Policy as necessary and appropriate, with the updated version being promptly posted on our website. We recommend that you revisit this Privacy Policy on a regular basis.

Last updated 22nd July 2024.