This policy explains how our organisation collects and manages the personal data of natural persons, including retained data.

DEFINITIONS

Personal data means any information that is related to you that reveals your identity. It does not apply to personal data that has been rendered anonymous so that you are no longer identifiable. Nor does it apply to the processing of personal data which concerns legal (non-natural) persons.

Our organisation means Tap into Safety Pty Ltd and includes any parent, subsidiaries and affiliates.

Our clients mean legal persons (e.g. companies) who purchase and use our products and services.

WHAT WE DO

We are an Australian-based technology company, providing developed software products and services to domestic and international customers (**our clients**). Personal data may be disclosed to overseas recipients (our clients based outside of Australia), who are entitled to disclosure. We develop specialised health and safety software applications to address problems and critical risks relating to unique work environments. Our safety training software is used on mobile devices and the web for increased accessibility.

We may give our staff and third-party business partners, access to your personal data for the purpose of delivering our software products to our clients in Australia or overseas. We will require them (and our clients) to comply with this Policy.

COLLECTION OF INFORMATION

WHAT WE COLLECT

We collect and process personal data in connection with our commercial activities with our clients, which are legal persons, and only by lawful and fair means. We estimate that around 50 percent of the personal data we collect is de-identified.

NOTE: Data protection does not apply to the processing of personal data rendered anonymous.

Our clients' workers create their own account on our system and complete online assessments in their own time. When you create your own online account on our system, you provide us with personal data (e.g. your name, birthdate, email address). We may also receive your personal data from our clients, which use our software and which you work for, and who will notify you of this.

NOTE: We do **NOT** collect, process or use the personal data of children.

Although we may collect analytic data to measure traffic and usage trends for our software applications, may use cookies to improve and develop our products and services; may obtain log file information from our servers; may employ clear gifs (web beacons) to track online usage patterns for more accurate reporting and software improvement; may use and remotely store identifiers (provided by your devices, tools and protocols, such as internet protocol addresses and cookie identifiers) to assess browsing and use of our software, we DO NOT use that information to identify you.

WHY WE COLLECT

When you log onto our system to use our *Hazard Insight* software as part of your mandatory workplace safety training, we collect personal data so that we can track and accurately gauge how you can identify and control hazards within the workplace. Results are tracked in real time via our comprehensive reporting platform. We then report your monitored behaviour to our client and your name is identified with the data.

Your use of our *All of Me* software is VOLUNTARY and an account can only be created by YOU! The only personal data we receive is what you give us when you set up your account and you are able to select your own filters, including using a pseudonym, if you do not wish to identify yourself. Data is collected to identify and address early indicators of stress anxiety and depression. Results are de-identified. The purpose is to improve mental health in the workplace. The data is **not** personal data because it cannot be linked back to you.

NOTE: We do **NOT** sell or lease or transfer your data to anyone else.

MANAGING PERSONAL DATA

Our commitment

Legal Compliance

To do our best to comply with our obligations under Australian and EU Privacy Laws, including Australian Privacy Principles (known as **APP**) and with EU General Data

Protection Regulation (known as **GDPR**), and to seek similar assurances from our clients;

Business Methods

- To adopt suitable business methods to help us demonstrate our compliance to the APP's and the GDPR, including open and transparent information handling practices in our day to day operations;

Rules

- To implement data protection rules across our organisation and across persons within our control, such as staff and third-party business partners;

Safeguards

- To do our best to apply appropriate safeguards to protect your personal data. This includes:
    - having in place a suitable code of conduct; and
    - securing your personal data in a manner that, amongst other things, prevents discriminatory effects on you or that results in measures having such an effect.

NOTE: We use the best of **Microsoft**'s cloud storage services to keep reports secure and safe. We will inform you without delay in the event of any harmful data breach.

Transparency of purpose

- To ensure that the specific purposes for which we process personal data are:
    - Explicit and legitimate; and
    - Determined together with our clients; and
    - Clearly consented to by you, at the time of the collection of personal data.

NOTE:

It is a legitimate interest to process personal data for purposes compatible with those for which the personal data was initially collected; or to the extent strictly necessary to ensure network and information security; for example, to prevent unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communications systems. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

Where you have given consent, processing of personal data shall be allowed, irrespective of compatibility of the purposes, as long as it is not incompatible with a legal, professional, or other binding obligation of secrecy.

Processing of data shall be considered lawful where it is necessary in the context of a contract with our clients, or the intention to enter into a contract, or if carried out in accordance with a legal obligation.

Secure and confidential processing

- To ensure that personal data is processed in a way that provides appropriate security and confidentiality. This includes preventing unauthorised access to, or use of, personal data and the equipment used for the processing.

Reduce risk of error

- To implement suitable technical measures to ensure that any factors causing errors or risks of errors, and which result in inaccuracies in personal data, are fixed or minimised.

Review, Rectification and Erasure

- To take all reasonable steps to ensure that personal data is accurate, up-to-date and complete, and that inaccurate personal data is corrected or deleted;

- To take all reasonable steps to erase personal data no longer needed for any purpose for which it may be used or disclosed

YOUR RIGHTS

Summary

Informed Consent

- Your consent is required before a business can use your personal data. Your consent should be affirmative, freely given, specific, informed and unambiguous.

You will be asked to affirm your consent when you create your own account to access our system.

- You have the right to be informed of the existence of the processing operation in relation to your personal data and its purposes, including the existence of any profiling and the consequences of the profiling. This information should be given to you at the time the information is collected from you.

- Where personal data is collected from you, you have the right to be informed whether you are obliged to provide the personal data, and of the consequences if you do not provide such data.

Data Protection

- You have the right to general protection of personal data.

- You have the right to be informed without delay (i.e. within 72 hours) in the event of harmful data breach.

Data Access

- You have the right, upon request, to access, free of charge, personal data held or processed.

- You have the right to object to or seek correction of personal data by electronic means and without undue delay (i.e. within one month). You have the right to be given reasons for any refusal to comply with your request.

- You have the right to be informed of any new purposes for processing your data.

- You have the right to be informed whether automated decisions are made about you based on your personal data and be given an opportunity to contest it.

To request Access email info@tapintosafety.com.au

Data Transfer

We do not transfer personal data. We only use personal data in conjunction with the services we provide to our clients for whom you are likely to be working. If our clients no longer use our system, or if you request erasure of personal data from our system, in either of these cases we will erase your personal data from our system.

Data Erasure

- You have the right, upon request, to require personal data to be erased, even if previously you gave your affirmed consent (e.g. by ticking a consent box, or by verbal or written means) for us to process it.

To request deletion of personal data that is not already de-identified email info@tapintosafety.com.au

COMPLAINT HANDLING

We will deal promptly (within 30 days) with any complaints about a likely breach of this Policy, including a likely breach of the APP's or GDPR and you will receive an initial response within 72 hours.

To lodge a complaint email info@tapintosafety.com.au