



Privacy Policy

Purpose

To ensure Techvisa complies with the requirements under the *Privacy Act 1988* (Cth) and *Privacy Amendment (Private Sector) Act 2000* (Cth) (National Privacy Principles). For a summary of the National Privacy Principles go to the Australian Privacy Commissioners website (<http://www.Privacy.gov.au>).

Scope

This policy outlines information relating to Techvisa, its employees and clients. This policy relates to personal information which Techvisa collects, uses or discloses and includes information held in conventional, electronic and digital format.

This policy and the Privacy Act does not cover the collection, retention nor disclosure of employee records. Employee records are kept in accordance with ss 535 and 536 of the *Fair Work Act 2009* (Cth) and regulations 3.31 to 3.46.

Policy

1. Access to our Privacy Policy

The Privacy Policy of Techvisa is publicly available www.techvisa.com.au This policy will also be made available on request in digital or hardcopy.

2. Privacy Officer

Where an individual or client requests access to their record, requests must be made in writing and sent to the Privacy Officer. The Privacy Officer is the contact point for any internal or external queries or requests for access across Australia.

Attention: Privacy Officer
Sam Bricknell – sam@techvisa.com.au



3. Consent

When you provide personal information to Techvisa you consent to the use of your personal information according to the purpose it was provided and in accordance with this Policy.

If Techvisa obtains personal information about you from a third party, we will request consent to use your personal information. Once consent is given your personal information will be used, disclosed and treated according to this Policy.

4. Collection of Personal Information

Personal information will only be collected via lawful and fair means. Techvisa's usual practice is to collect personal information directly from you. Collection may occur when you fill in and submit one of our forms, provide information to us through our websites or electronically via our telecommunications or email systems.

We also collect personal information that has been provided to us through an external third party, or a publicly available source. Techvisa will take reasonable steps where practicable to inform you that we have collected personal information from a third party.

Personal information is information from which the identity of a person can be reasonably ascertained and includes everyday information such as name, address, telephone number, e-mail address or date of birth. The type of personal information we collect and use will depend on various factors such as the type of service you request or we require and the applicable legal and regulatory obligations. This may include, but is not limited to, collection and use of the following kinds of information:

Contact information that allows us to communicate with you (e.g. e-mail, social media contact details, address, telephone number, comments made on our websites, Facebook, Twitter or on email)

Identity information that allows us to identify you (e.g. name, date of birth, occupation, government issued identification, photo identification)

Professional information that helps us to understand more about your employment history including qualifications, talents, skills and abilities (e.g. references, resume, qualification documents)



Web Searches information that allows us to assess your suitability for a position (e.g. background checking via Google, regulatory and immigration).

Other individuals information we request, or that you provide, about an individual other than yourself (previous employer and referees)

Sensitive information is defined in the Privacy Act and includes information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs, membership of a trade union or other professional body, criminal record or health information.

Examples of sensitive information we collect include but is not limited to:

- **Criminal record checks;**
- **Health information;**

5. Use of personal information

We collect your personal information for the primary purpose of providing our services to you and direct marketing.

We may also use your personal information for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use or disclosure. This includes disclosure for use:

- to obtain quotes from health insurance providers;
- to make enquiries with VEVO;
- for BVB;

If your personal information is used for the purpose of direct marketing and you do not wish to continue receiving our communications, you may unsubscribe from our mailing/marketing lists at any time by contacting our Privacy Officer and requesting not to receive direct marketing communications. Your marketing preference will be updated on our systems.

6. Disclosure

Disclosure refers to the situation where Techvisa releases information to others outside the company. It does not include giving individuals information about themselves.



Disclosure can be made with an individual's permission. Written permission must be obtained to disclose sensitive information.

We may disclose personal information in the following circumstances:

- Publishing information through the internet so it can be accessed by another entity;
- Sending documents containing personal information to another person other than the individual;
- Revealing information in the course of a conversation.

7. Data Quality and Correction

Techvisa takes reasonable steps to ensure that the personal information it collects is accurate, up to date and complete.

In circumstances where your personal information has changed, or you find the information to be inaccurate please contact the Privacy Officer for correction. The Privacy Officer will take reasonable steps to update and correct the information in accordance with applicable privacy law. Techvisa may also contact you from time to time to check the information is correct.

If we have disclosed personal information about you that is inaccurate you can ask us to notify third parties to whom we made the disclosure. Reasonable steps will be taken to notify the third party unless it is impracticable or unlawful to do so.

If we do not agree the information should be changed and refuse to correct your personal information you may make a complaint.

8. Access

Subject to some exceptions, you may gain access to the personal information we hold.

An important exception is where evaluative material is obtained confidentially during reference checks. We will refuse access if it would breach confidentiality or if it would interfere with the privacy of others.

If you wish to obtain access to your personal information you should contact our Privacy Officer. You will need to verify your identity. If we refuse access to personal information or to give access in the manner requested, you may make a complaint.



9. Data Security and Storage

Techvisa takes reasonable steps to protect the personal information we hold from loss, unauthorized access and misuse. Your information is stored on our database and cloud storage. This database is operated on a server that allows disclosure only as required for the performance of our services. The database has restricted user access.

We take a range of measures to protect your personal information. These measures include

- Staff training
- Document control for sensitive information
- Confidentiality procedures
- Password protection and encryption
- Policies on laptop, mobile phone and portable storage device security

10. Retention and Disposal

We only retain your personal information until it is no longer required, or you withdraw your consent or as required by law. You can withdraw your consent at any time by contacting the Privacy Officer.

Unless we have a legal obligation to retain the data, it will be deleted. If we are unable to dispose of the data then it will undergo a de-identification processes. Sensitive data is purged after three years as required by law.

Note: Employee records are exempt from disposal requirements in Australia.

11. Data Breaches

In the event that personal information has been lost or subjected to unauthorised access, we will take all necessary steps to immediately contain and rectify the data breach and prevent reoccurrence.

Where the data breach is likely to result in serious harm, we will take reasonable steps to notify you and provide you with relevant information in relation to the breach. As soon as practicable, we will also contact and prepare a statement for the Information Commissioner detailing the breach and the steps taken. A review of the incident will be completed, and action taken to prevent future breaches.



12. Privacy Complaints

You may make a complaint about our handling of your personal information if you believe that we have interfered with your privacy. Complaints should be made to the Privacy Officer in writing.

When we receive your complaint, we will take steps to confirm the authenticity of the complaint and the contact details of the complainant. Upon confirmation, we:

- will write to you to acknowledge receipt and to confirm that we are handling your complaint;
- may ask for clarification of certain aspects of the complaint and for further details;
- will consider the complaint and may make further enquiries;
- will require a reasonable time to respond (usually 30 days);
- will suggest possible solutions if the complaint can be resolved through access or correction;
- will suggest a solution, on a confidential and without prejudice basis, if we believe that your complaint may be capable of some other solution.

If the complaint cannot be resolved, we will suggest that you take your complaint to a recognised external dispute resolution provider such as the Office of the Australian Information Commissioner.