

peoplefusion privacy policy

1. Introduction

peoplefusion values your privacy and is committed to ensuring the confidentiality of your personal information. We manage personal information in accordance with the *Privacy Act 1988* and *Australian Privacy Principles*. This condensed policy applies to information collected by peoplefusion Pty Ltd.

We reserve the right, at our discretion, to modify, add to or remove portions of this Privacy Policy at any time. You should review this Privacy Policy periodically so that you are updated on any changes. We welcome your comments and feedback.

We only collect information that is reasonably necessary for the proper performance of our activities or functions.

We do not collect personal information just because we think it could be useful at some future stage if we have no present need for it.

We may decline to collect unsolicited personal information from or about you and take steps to purge it from our systems.

By following the links in this document, you will be able to find out how we manage your personal information as an APP Entity under the Australian Privacy Principles (APPs).

You will also be able to find out about the information flows associated with that information.

If you have any questions please [contact us](#).

1.1. APP Entity

peoplefusion Pty Ltd manages personal information, as an APP Entity, under the Australian Privacy Principles (APPs).

Because we are a contracted service provider to a range of Commonwealth, State and Territory government agencies, it sometimes becomes necessary for us to collect and manage personal information as an Agency under different privacy arrangements.

If you wish to know whether this applies to you, please contact us.

1.2. Information Flow

When we collect your personal information:

- we check that it is reasonably necessary for our functions or activities as a recruitment firm providing on-hire and permanent recruitment solutions to our clients.
- we check that it is current, complete and accurate. This will sometimes mean that we have to cross check the information that we collect from you with third parties.
- we record and hold your information in our Information Record System. Some information may be disclosed to overseas recipients.

- we retrieve your information when we need to use or disclose it for our functions and activities. At that time, we take reasonable steps to check that it is current, complete, accurate and relevant. This will sometimes mean that we have to cross check the information that we collect from you with third parties once again - especially if some time has passed since we last checked.
- subject to some exceptions, we permit you to access your personal information in accordance with APP:12 of the (APPs) and the remainder of this Privacy Policy.
- we correct or attach associated statements to your personal information in accordance with APP:13 of the (APPs).
- we may destroy or de-identify your personal information when it is no longer needed for any purpose for which it may be used or disclosed provided that it is lawful for us to do so. We do not destroy or de-identify information that is contained in a Commonwealth Record.

2. Kinds of information that we collect and hold

Personal information that we collect and hold is information that is reasonably necessary for the proper performance of our functions and activities as a recruitment firm and is likely to differ depending on whether you are:

- a Candidate
- a Client
- a Referee

2.1. For Candidates

The type of information that we typically collect and hold about Candidates is information that is necessary to assess amenability to work offers and work availability; suitability for placements; or to manage the performance in work obtained through us and includes:

- Full name
- Address
- Phone number
- Email address
- Employment history
- Referee details
- Opinions of others about your work performance, work experience and qualifications
- Aptitude test results and pre-employment medical results
- Financial details, such as banking, superannuation and Tax File Number

2.2. For Clients

The type of information that we typically collect and hold about Clients is information that is necessary to help us manage the presentation and delivery of our services and includes:

- Entity and trading names, ABN
- Addresses
- Switchboard phone and fax numbers
- Full names, phone numbers, email addresses and position title of client contacts
- Basic information on the company which may include annual turnover, number of employees, organisational structure, culture

2.3. For Referees

The type of information that we typically collect and hold about Referees is information that is necessary to help to make determinations about the suitability of one of our Candidates for particular jobs or particular types of work and includes:

- Full name
- Phone number
- Email address
- Current or previous employer and your position title
- Your opinions about Candidates work performance, work experience and qualifications

3. Purposes

The purposes for which we collect, hold, use and disclose your personal information are likely to differ depending on whether you are:

- a Candidate
- a Client
- a Referee

The following sections are also relevant to our use and disclosure of your personal information:

- Our Policy on Direct Marketing
- Overseas Disclosures

3.1. For Candidates

Information that we collect, hold, use and disclose about Candidates is typically used for:

- work placement operations
- recruitment functions
- statistical purposes and statutory compliance requirements

3.2. For Clients

Personal information that we collect, hold, use and disclose about Clients is typically used for:

- client and business relationship management
- recruitment functions
- marketing services to you
- statistical purposes and statutory compliance requirements

3.3. For Referees

Personal information that we collect, hold, use and disclose about Referees is typically used for:

- to confirm identity and authority to provide references
- candidate suitability assessment
- recruitment functions

3.4. Our Policy on Direct Marketing

Your personal information may be used for marketing purposes directly. Your information may be provided to a third party for the purposes of marketing our products and services.

We will:

- provide an option for individuals receiving marketing communication from us to opt out of receiving such communication
- comply with anti-spam legislation providing all recipients with inferred consent, clear and accurate information and an option to unsubscribe from marketing communications.

4. How your personal information is collected

The means by which we will generally collect your personal information are likely to differ depending on whether you are:

- a Candidate
- a Client
- a Referee

We sometimes collect information from third parties and publicly available sources when it is necessary for a specific purpose such as checking information that you have given us or where you have consented or would reasonably expect us to collect your personal information in this way.

Sometimes the technology that is used to support communications between us will provide personal information to us - see the section in this policy on Electronic Transactions.

You have no obligation to provide any information requested by us, however if you choose to withhold personal information from us it will likely prevent us from being able to provide you with the services that you have requested.

See also the section on Photos & Images.

4.1. For Candidates

Personal information will be collected from you directly when you fill out and submit one of our application forms or any other information in connection with your application to us for work.

Personal information is also collected when:

- you apply for an advertised role on a third party website, e.g. Seek

We may also collect personal information about you from a range of publicly available sources including newspapers, journals, directories, the Internet and social media sites. When we collect personal information about you from publicly available sources for inclusion in our records we will manage the information in accordance with the [APPs](#) and our Privacy Policy.

4.2. For Clients

Personal information about you may be collected:

- when you provide it to us for business or business related social purposes;

We may also collect personal information about you from a range of publicly available sources including newspapers, journals, directories, the Internet and social media sites. When we collect personal information about you from publicly available sources for inclusion in our records we will manage the information in accordance with the APPs and our Privacy Policy.

4.3. For Referees

Personal information about you may be collected when you provide it to us:

- in the course of our checking candidate references with you and when we are checking information that we obtain from you about candidates;

We may also collect personal information about you from a range of publicly available sources including newspapers, journals, directories, the Internet and social media sites. When we collect personal information about you from publicly available sources for inclusion in our records we will manage the information in accordance with the APPs and our Privacy Policy.

4.4. Photos & Images

We may take photographs during peoplefusion sponsored or organised events. peoplefusion representatives will oblige, when requested not to take your photograph, during these events. In the case your photograph is taken, we may use the images for our social media pages and other marketing activities.

4.4.1 For Candidates

As part of our candidate registration process we will request that you supply us with an original photographic proof of identification document (ID). We will take a photocopy or other image of that ID document and will store and use that copy in accordance with our Privacy Policy.

At any time during the consultation and application process we may request you to participate in an online video interview. The interview will be conducted via a third party contracted service provider (CSP, refer to clause 6.1 below), accessed by logging on to that CSP's website. The completed video will be viewed by us online, but will not be stored by peoplefusion. The video may be stored by the CSP, which will be outside of the direction or control of peoplefusion. You should consider any terms governing the CSP's provision of services to you, including their website, before logging on to and completing the interview via the CSP's website.

4.5. Electronic Transactions

Sometimes, we collect personal information that individuals choose to give us via online forms or by email, for example when individuals:

- ask to be on an email list such as a job notification list;
- register as a site user to access facilities on our site such as a job notification board;
- make a written online enquiry or email us through our website;
- submit a resume by email or through our website;

It is important that you understand that there are risks associated with use of the Internet and you should take all appropriate steps to protect your personal information. It might help you to look at the OAIC's resource on [Internet Communications and other Technologies](#)

You can contact us by land line telephone or post if you have concerns about making contact via the Internet.

4.5.1. Social Media

We may use social networks to collect personal information about you where publicly available or available to us through the Privacy Policy of these third party social networks. You are responsible for your own security and personal information for third party social networks and should consult those third party privacy policies to find out how they collect, use and manage your personal information.

4.5.2. Internet and Web

We may use publicly available internet sources to collect information. We will use reasonable endeavours to keep the data we collect from internet sources accurate and up to date, and may confirm this information with you as appropriate.

4.5.3. Email Transactions

We will record your email address if you transmit to us electronically either in an email message or via a web page form. It will only be used for the purpose in which you provide it and will not be disclosed to any third party without your consent.

5. How your personal information is held

Personal information is held in our Information Record System until it is no longer needed for any purpose for which it may be used or disclosed at which time it will be de-identified or destroyed provided that it is lawful for us to do so. Personal information is held in paper archives, by electronic or computer data base and remotely in cloud based storage systems.

We strive to ensure the security, integrity and privacy of personal information collected and held by us, and we review and update our security measures in light of current technologies. Unfortunately we cannot guarantee that our data storage measures are totally secure.

We take a range of measures to protect your personal information from:

- misuse, interference and loss; and
- unauthorised access, modification or disclosure.

5.1. Our Information Record System

Our Information Record System is stored on a secure server system.

- personal information is stored in electronic format on a secure server system
- our IT provider may have an electronic backup of these files stored off site
- where our portable electronic devices have access to our Information Record System, this access is secure

5.2. Data security of personal information

We have taken reasonable steps to protect the personal information we hold from misuse and loss and from unauthorised access, modification or disclosure. Staff are required to sign a confidentiality clause as a part of their contracts of employment. They are also required to adhere to and comply with our Privacy Policy. There are a range of physical and electronic procedures to ensure that privacy is safeguarded. However, the internet is not secure and we cannot guarantee the security of any information sent to us via the internet. Sometimes breaches of personal information occur, which can range from non-threatening to serious. When a data breach is considered serious it is likely to cause harm to the individual that the personal information is about. This is called an eligible data breach. If a circumstance arises that is considered an eligible data breach, we will notify the individual and the Office of the Australia Information Commissioner. In this notification we will make recommendations to the individual on the steps they should take in order to protect themselves in relation to the breach of information.

6. Disclosures

We may disclose your personal information for any of the purposes for which it is primarily held or for a lawful related purpose.

We may disclose your personal information where we are under a legal duty to do so.

Disclosure will usually be:

- internally and to our related entities
- to our Clients
- to Referees for suitability and screening purposes.

6.1. Related Purpose Disclosures

We outsource a number of services to contracted service suppliers (CSPs) from time to time. Our CSPs may see some of your personal information. Typically our CSPs would include:

- Software solutions providers;
- I.T. contractors and database designers and Internet service suppliers;
- Legal and other professional advisors;
- Insurance brokers, loss assessors and underwriters;
- Superannuation fund managers;
- Background checking and screening agents;

We take reasonable steps to ensure that terms of service with our CSPs recognise that we are bound by obligations to protect the privacy of your personal information and that they will not do anything that would cause us to breach those obligations, however we will not be held responsible for any misuse of your personal information by our CSPs.

6.2. Cross-Border Disclosures

While it is unlikely, some of your personal information may be disclosed to overseas recipients. We cannot guarantee that any recipient of your personal information will protect it to the standard to which it ought to be protected. The costs and difficulties of enforcement of privacy rights in foreign jurisdictions and the impracticability of attempting to enforce such rights in some jurisdictions will mean that in some instances, we will need to seek your consent to disclosure.

As part of provision of our services to you we may store your personal information using online or cloud software. The personal information that you provide to us may be transferred to the servers of our software providers as a function of transmission across the internet. By providing your personal information you are consenting to that personal information being transferred to and stored on the servers as set out in this Privacy Policy.

However, as the third parties who host our servers do not control, and are not permitted to access or use your personal information (except for the limited purpose of storing the information), we do not “disclose” personal information to those server hosts, whether or not they are located overseas. We will use reasonable endeavours to ensure that our server hosts do not have access to, and use the necessary level of protection to safeguard, your personal information and otherwise comply with the APPs. If you do not want your personal information to be transferred to a server in the manner set out in this paragraph or to any other international locations, you should not provide us with your personal information or use our services.

7. IP Addresses

If information is gathered by our website or online database, our web servers may gather your IP address to assist with the diagnosis of problems or support issues with our services. This information is gathered in aggregate only and cannot be traced to an individual user.

Our website may contain links to third parties’ websites, including sites maintained by related entities. Those other websites are not subject to this Privacy Policy and are not governed, managed or controlled by us. You should familiarise yourself and ensure you are comfortable with any particular privacy policies governing the use of those websites prior to such use.

8. Cookies and Applets

We may use cookies to provide you with a better experience when using our website/portal. These cookies allow us to increase your security by storing your session ID and are a way of monitoring single user access. This aggregate, non-personal information is collated and provided to us to assist in analysing the usage of the site.

9. Access & Correction

Subject to some exceptions set out in privacy law, you can gain access to your personal information that we hold.

Important exceptions include:

- evaluative opinion material obtained confidentially in the course of our performing reference checks; and access that would impact on the privacy rights of other people. In many cases evaluative material contained in references that we obtain will be collected under obligations of

confidentiality that the person who gave us that information is entitled to expect will be observed. We do refuse access if it would breach confidentiality.

For more information about access to your information see our Access Policy.

For more information about applying to correct your information see our Correction Policy.

9.1. Access Policy

If you wish to obtain access to your personal information you should contact our Privacy Officer. You will need to be in a position to verify your identity.

- We will respond to all requests for access to your personal information with a response with 5 business days
- In the event we refuse to provide access because of subclause 12.3 in APPs, you should follow the Complaints Procedure to prompt the Privacy Officer to initiate an investigation.

9.2. Correction Policy

If you find that personal information that we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, you can ask us to correct it by contacting us.

We will take such steps as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

If we have disclosed personal information about you that is inaccurate, out of date, incomplete, irrelevant or misleading, you can ask us to notify the third parties to whom we made the disclosure and we will take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

- We will respond to all written requests to correct your personal information in a timely manner. We will make such corrections within 5 business days of our response.
- In the event we refuse to correct information, you should follow the Complaints Procedure to prompt the Privacy Officer to initiate an investigation.

10. Complaints

You have a right to complain about our handling of your personal information if you believe that we have interfered with your privacy.

For more information see our Complaints Procedure

10.1. Complaints procedure

If you are making a complaint about our handling of your personal information, it should first be made to us in writing.

You can make complaints about our handling of your personal information to our Privacy Officer, whose contact details are:

The Privacy Officer

Phone: 02 4929 1666

Email: reception@peoplefusion.com.au.

You can also make complaints to the [Office of the Australian Information Commissioner](#)

Complaints may also be made to [RCSA](#), the industry association of which we are a member.

RCSA administers a Code of Conduct for the professional and ethical conduct of its members.

The RCSA Code is supported by rules for the resolution of disputes involving members.

NOTE: The Association Code and Dispute Resolution Rules do NOT constitute a recognised external dispute resolution scheme for the purposes of the APPs; but are primarily designed to regulate the good conduct of the Associations members.

When we receive your complaint:

- We will take steps to confirm the authenticity of the complaint and the contact details provided to us to ensure that we are responding to you or to a person whom you have authorised to receive information about your complaint;
- Upon confirmation we will write to you to acknowledge receipt and to confirm that we are handling your complaint in accordance with our policy.
- We may ask for clarification of certain aspects of the complaint and for further detail;
- We will consider the complaint and may make inquiries of people who can assist us to established what has happened and why;
- We will require a reasonable time (usually 30 days) to respond;
- If the complaint can be resolved by procedures for access and correction we will suggest these to you as possible solutions;
- If we believe that your complaint may be capable of some other solution we will suggest that solution to you, on a confidential and without prejudice basis in our response;

If the complaint cannot be resolved by means that we propose in our response, we will suggest that you take your complaint to any recognised external dispute resolution scheme to which we belong or to the [Office of the Australian Information Commissioner](#).