



Equifax HR Solutions

Privacy Policy

Equifax HR Solutions is committed to protecting your privacy. This Privacy Policy explains how we collect and use your personal data and which rights and options you have in this respect. If you would like to learn more about your use of our information services or the information that we collect and provide, please refer to our **Terms of Supply** and the relevant **Statement of Work** or **Service Terms** (where available) for those services. Please also refer to our **Cookie Policy** which explains the use of cookies and other web tracking devices through our website.

Who is responsible for your personal information?

Equifax Australasia Workforce Solutions Pty Limited ABN 86 080 799 720, which trades under the business names of **Equifax HR Solutions** and (for one of its services) **fit2work**, is responsible for your personal information. It is a member of the Equifax Group of companies, comprising Equifax, Inc (NYSE: EFX), as the ultimate parent company headquartered in Atlanta, Georgia, and its related body corporates, subsidiaries and affiliates.

How do we deliver our services?

Our information services include verification, scoring and background reporting services, HR platform systems for workforce management across the employment cycle, and a range of other workforce data management services. Our information services are categorised, and more particularly described in and governed by, the **Statements of Work** or **Service Terms** for our product areas, being:

- *fit2work*;
- Equifax HR Platform (formerly *eRecruit*);
- *eCredential*; and
- Equifax Verification Exchange®

The details of how we collect and use your personal data and the rights and options you have in respect of each product area is explained further in the **Collection Statement** for that product area. This Privacy Policy is to be read in conjunction with each relevant Collection Statement covering your use of our information services.

We collect, use, disclose and hold personal information in accordance with both Australian and New Zealand privacy laws. Those laws include the *Australian Privacy Principles* and Part IIIC of the *Privacy Act 1988* (Cth), the *New Zealand Information Privacy Principles* in the *Privacy Act 2020* (NZ) and the *Credit Reporting Privacy Code 2020* (NZ).



What personal information do we collect?

The personal information we collect will vary depending on which of our information services you use and is described in more detail in the **Collection Statement** for that product area. By way of overview, that personal information may include:

- contact information, such as your name, sex, job title, residential address, business address, telephone number, mobile phone number, fax number and email address;
- background information, such as past residential addresses (for up to the last 5 years), employment and academic history, former names and aliases and marital relationship;
- government identifiers, including passport and driver's licence numbers, and visa information;
- information collected from publicly available resources, integrity data bases and credit agencies;
- sensitive information, such as membership of a professional or trade association or union, health personal data, and details of any police or criminal record you may have;
- employee records, including variations to your employment, terminations, leave requests, performance management assessments, and payroll/HRIS systems data;
- résumés, recruitment records, identity documents and reference checks;
- payment data, such as data necessary for processing payments and fraud prevention, and related billing information;
- dispute information, where you dispute the accuracy of any report we obtain;
- your password for an Equifax website or other password protected platforms or services, where you use one in conjunction with our services;
- other search specific data, such as information about relevant litigation or other legal proceedings against you or a third party related to you, regulatory sanctions or insolvency records;
- other personal data regarding your preferences where it is relevant to the services that we provide; and/or
- details of your contact with our offices or representatives.

Unless you operate an account with us, we outsource payment collection arrangements to third-party suppliers, who may collect payment information (including credit/debit card numbers and security code numbers) under the terms of their own privacy policy. We do not collect that information.

How do we collect your personal information?

We may collect personal information about you in various circumstances, including:

- when you or an organisation (usually an employer or prospective employer, or a service provider you have approached) seek to use any of our on-line or manual information services;
- when you or your organisation browse, make an enquiry or otherwise interact on our website;
- when you attend a seminar or another Equifax event or sign up to receive personal data from us, including training; or
- when you or your organisation offer to provide or provide services to us.



In many circumstances, particularly in background checking or for HR platform services, we collect personal information about you from a third-party source. For example, we may collect personal information from your employer organisation, other organisations with whom you have dealings, government agencies, a credit reporting agency, an information or service provider, or from publicly available records.

Are you required to provide personal information?

As a general principle, you will provide us with your personal information entirely voluntarily; however, there may potentially be detrimental effects for you in the event you choose not to consent or to provide some data, depending on the information service being used and the requirements of any organisation requesting you to use our services. For example, there are circumstances in which we cannot act or completely provide our information services without certain categories of personal information, because this data is required to carry out a legally required compliance screening or a background check required by an employer. In these cases, it will unfortunately not be possible for us to provide you with what is requested without the relevant personal information and we will notify you and the relevant organisation accordingly.

For what purposes will we use or disclose your personal data?

Our use and disclosure of the personal information we collect will vary depending on which of our information services you use and is described in more detail in the **Collection Statement** for that product area. We may also use your personal information for the following general purposes:

- managing and administering your or your organisation's business relationship with Equifax, including processing payments, accounting, auditing, billing and collection, and support services;
- compliance with our legal obligations (such as record keeping obligations), compliance screening or recording obligations (e.g. under antitrust laws, export laws, trade sanction and embargo laws, for anti-money laundering, financial and credit check and fraud and crime prevention and detection purposes), which may include automated checks of your contact data or other information you provide about your identity against applicable sanctioned-party lists and contacting you to confirm your identity in case of a potential match or recording interaction with you which may be relevant for compliance purposes;
- to analyse and improve our services and communications to you;
- protecting the security of and managing access to our premises, IT and communication systems, online platforms, websites and other systems, preventing and detecting security threats, fraud or other criminal or malicious activities;
- for insurance purposes;
- for monitoring and assessing compliance with our policies and standards;
- to identify persons authorised to trade on behalf of our clients, customers, suppliers and/or service providers;
- to comply with our legal and regulatory obligations and requests anywhere in the world, including reporting to and/or being audited by national and international regulatory bodies, and law enforcement agencies;



- to comply with court orders and exercises and/or defend our legal rights; and
- or any purpose related and/or ancillary to any of the above or any other purpose for which your personal information was provided to us.

With whom will we share your personal data?

How we share the personal information we collect will vary depending on which of our information services you use and is described in more detail in the **Collection Statement** for that product area. We may also share your personal data in the following circumstances:

- between Equifax entities and other service providers where required for providing the information services requested and for administrative, billing and other business purposes – as further detailed below;
- with companies providing services for money laundering checks, credit risk reduction and other fraud and crime prevention purposes and companies providing similar services, including financial institutions, credit reference agencies and regulatory bodies with whom such personal data is shared;
- with any third party to whom we assign or novate any of our rights or obligations; and
- with courts, law enforcement authorities, regulators, legal practitioners or other parties where it is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim, or for the purposes of a confidential alternative dispute resolution process.

We are part of a global group and may retain service providers within or outside of the Equifax group, domestically or abroad, to process personal information for a permitted purpose on our behalf and in accordance with our instructions only. In any event, we will retain control over and will remain fully responsible for your personal information and will use appropriate safeguards as required by applicable law to ensure the integrity and security of your personal information when engaging such service providers.

Otherwise, we will only disclose your personal information as described in this Privacy Policy or when you direct us or give us permission (including by way of acknowledging a **Collection Statement**), when we are required by applicable law or regulations or judicial or official request to do so, or as required to investigate actual or suspected fraudulent or criminal activities.

We may also use aggregated personal information and statistics for monitoring website usage to help us develop our website and our services.

Personal information about other people which you provide to us

If you provide personal information to us about someone else (such as one of your employees, a prospective employee, officers, or someone with whom you have business dealings) you must ensure that you are entitled to disclose that personal information to us and that, without our taking any further steps, we may collect, use and disclose that personal data as described in this Privacy Policy. In particular, you must ensure the individual concerned is aware of the various matters detailed in this Privacy Policy and any applicable Collection Statement, as those matters relate to that individual,



including our identity, how to contact us, our purposes of collection, our personal information disclosure practices (including disclosure to overseas recipients), the individual's right to obtain access to the personal information and make complaints about the handling of the personal information, and the consequences if the personal information is not provided (such as our inability to provide services).

Keeping personal information about you secure

We will take appropriate technical and organisational measures to keep your personal information confidential and secure in accordance with our internal procedures covering the storage, disclosure of and access to personal information. Personal information may be kept on our personal information technology systems, those of our contractors or Affiliates, or in paper files.

Transferring your personal information abroad

Where we are likely to disclose your personal information to overseas recipients, it may be described in more detail in the **Collection Statement** for that product area. When doing so we will comply with applicable data protection requirements and take appropriate safeguards to ensure the security and integrity of your personal data. Any disclosure of your personal information to an overseas recipient will be for the purposes of providing the information services requested (including administrative, billing, business purposes, and any purpose stated in the Collection Statement for that product area). We are also likely to disclose your personal information to overseas recipients in cases where your background or a specific search requested relates to a foreign activity or presence. In any case, the overseas recipients are likely to be in those relevant jurisdictions in which the foreign activity or presence relates to, or in a jurisdiction such as, but not limited to, the USA, India, Malaysia or Costa Rica, where we have agents or service providers.

Where we do disclose personal information offshore, many of the overseas entities are related to us. The countries in which the entities are located include, but are not limited to, the USA, Chile, the Philippines, India, Costa Rica and Ireland. A list of the countries in which Equifax group entities are located can be found on our parent's website at <https://www.equifax.com/about-equifax/company-profile/>.

Data storage architecture employed by cloud service providers to us also means that personal information contained in some communications with us, or in certain types of documents, may be held in the EU or sharded in multiple overseas locations.

We may also, in some circumstances, disclose personal information to our customers in locations overseas, in connection with the provision of our services to those customers.

As part of a global group providing services to customers and in dealing with our customer relationships, we may also disclose or provide access to personal information (other than credit information) of an organisation's employees, contractors or other service providers as made known to us by an organisation, to overseas entities. This occurs, for example, where we have engaged with overseas entities to provide services (including technology, operations, billing, administrative and customer support services) to us, and they need to access that personal information held by us to provide those services. By dealing with us, an organisation or other business entity acknowledges that these service arrangements may result in personal information provided by it or collected about such persons being disclosed to or used by an overseas recipient and that:



- (a) the overseas recipient may not be required to protect that personal information in a way that provides comparable safeguards to those under the Privacy Law;
- (b) the overseas recipient may be subject to a foreign law that could compel the disclosure of your personal information to a third party, such as an overseas authority (for example, under legislation to intercept cyber traffic or obstruct terrorism), and the individual may not be able to seek any redress in that overseas jurisdiction; and
- (c) we will not be accountable under the Privacy Law, and an individual will not be able to seek redress under the Privacy Law, if the overseas recipient handles their personal information in breach of the Privacy Law.

By dealing with us, the organisation or other business entity – on behalf of those individuals – consents to any such disclosure, accepts that APP 8 (in Australia) will not apply in respect of any such personal information and warrants that it has satisfied itself that our overseas disclosure of personal information is compatible with and satisfies any privacy policy or other privacy statement or requirement that it operates under.

Updating personal information about you

If any of the personal information that you have provided to us changes, for example if you change your email address or if you wish to cancel any request you have made of us, or if you become aware we have any inaccurate personal information about you, please let us know by sending an email to: support@fit2work.com.au (**fit2work**), support.au.ve@equifax.com (**Verification Exchange**) or (where relevant) to the contact address specified in the **Statement of Work** or **Service Terms** for those particular services. We will not be responsible for any losses arising from any inaccurate, inauthentic, deficient or incomplete personal information that you provide to us.

For how long do we retain your personal information?

In most instances we provide our information services as agent for your employer or other customer entity under a limited agency solely for purposes of delivering those services, in which case (subject to legal or other constraints binding us) any retention period may be determined by the privacy or other policies of that entity. Generally, your personal information will be deleted or deidentified when it is no longer reasonably required for a permitted purpose or you withdraw your consent (where applicable) and we are not legally required or otherwise permitted to continue storing such data. In particular, we will retain your personal information (under a 'Legal Hold') where required for Equifax to assert or defend against legal claims until the end of the relevant retention period or until the claims in question have been settled.

Unsolicited Personal Information

Where we have received unsolicited personal information about you (information that we did not request), we will destroy or de-identify that information within a reasonable time, but only if it is lawful and reasonable to do so.



Your rights

Subject to certain legal conditions, you have the right to request a copy of the personal information about you which we hold, to have any inaccurate personal information corrected (where that is within our power or control) and to object to or restrict our using your personal information. You may also make a complaint if you have a concern about our handling of your personal information.

If you wish to do any of the above, please send an email to support@fit2work.com.au (**fit2work**), support.au.ve@equifax.com (**Verification Exchange**) or (where relevant) to the contact address specified in the **Statement of Work** or **Service Terms** for those particular services or email our Equifax complaints team at customercomplaintsAU@equifax.com. We may request that you prove your identity by providing us with a copy of a valid means of identification to allow us to comply with our security obligations and to prevent unauthorised disclosure of data. We reserve the right to charge you a reasonable administrative fee for any manifestly unfounded or excessive requests concerning your access to your data, and for any additional copies of the personal information you request from us.

We will consider any requests or complaints which we receive and provide you with a response in a timely manner. If you are not satisfied with our response, you may take your complaint to a relevant privacy regulator. The contact details for the Australian bodies is set out below:

Australian Financial Complaints Authority (AFCA)

GPO Box 3
Melbourne VIC 3001
p: 1800 931 678
<http://www.afca.org.au>

Office of the Australian Information Commissioner (OAIC)

GPO Box 5218
Sydney NSW 2001
p: 1300 363 992
<http://www.oaic.gov.au>

In New Zealand, you should contact:

The Office of the Privacy Commissioner (OPC)

PO Box 10 094,
The Terrace,
Wellington 6143
p: 0800 803 909
f: (04) 474 7595
<https://www.privacy.org.nz>



Updates to this Privacy Policy

This Privacy Policy was previously updated in January 2022. We reserve the right to update and change this Privacy Policy from time to time to reflect any changes to the way in which we process your personal information or changing legal requirements. In case of any such changes, we will post the changed Privacy Policy on our website or publish it otherwise. The changes will take effect as soon as they are posted on this website.

How to get in touch with us

We welcome your views about our website and our Privacy Policy. If you would like to contact us with any queries or comments, please send an email to the Equifax address mentioned above under “**Your rights**” or send a letter to our Privacy Officer at:

Equifax Privacy Officer
Locked Bag 965
North Sydney, NSW 2059

or phone us on 1300 575 575.