Privacy Policy

Effective date: 7 July 2026

Read about how Link Financial Services Pty Ltd trading as Focus Partners Australia | Link Financial (**FPALF**) collects, protects, uses and shares your personal information.

Purpose of this policy

We take client privacy, confidentiality and data security very seriously and have thereby developed a firm wide Privacy Policy ("this Policy") which applies to all of our employees, in every capacity.

This Policy sets out our commitment in respect of personal and credit information we hold about you and how that information is used. It aims to ensure that we comply with the Privacy Act (Cth) 1998 ("Privacy Act"), the Australian Privacy Principles ("APPs") and all other relevant legislation which collectively outlines the rights and responsibilities of private sector organisations in the collection, holding, use, correction, disclosure and transfer of personal and credit information.

This Policy outlines how we handle your personal and credit information. However, we may provide additional details on our management practices when we collect your information, at the start of our engagement or periodically throughout our ongoing service relationship.

We may change this Policy by publishing changes to it on our website. Please check our website regularly to ensure that you are aware of any changes to this Policy.

What information do we collect?

Personal information is information about you that is reasonably identifiable (i.e. name, email address, contact details).

Credit information is personal information that is collected in connection with a credit application. This includes identification information, default information or repayment history information.

In this Policy we use the term personal information to refer to both personal information and credit information.

The information we may collect (and hold) about you includes:

- name, address, email address, date of birth, phone number(s);
- tax file number;
- information about dependents or family members;
- bank account details or credit or debit card details;
- Medicare number, pension card number;
- accounting and financial information;
- occupation, employment history and details;
- family commitments and social security eligibility;
- financial needs and objectives;
- assets and liabilities (current and future), income, expenses;
- superannuation and insurance details;
- risk profile details;
- details of your interactions with us;
- internet protocol address;
- identity information such as driver's licence and passport numbers;
- any other relevant information that you give to us for the purpose of providing you with our products or services.

The collection of sensitive information is restricted by the Privacy Act. This includes information about your religion, racial or ethnic origin, political opinions, criminal record and sexual orientation. It also includes health information and biometric information.

Typically, we collect this information only when it is required to deliver a specific product or service, and you have given your consent for its collection. For instance, we may gather health information from you to process an insurance policy application.

How do we collect your personal information?

We primarily collect personal information directly from you. For example, we gather information when you apply for or use a product or service, when you communicate with us in person or over the phone.

Additionally, we collect information electronically, such as when you visit our website or send us electronic messages (see “Electronic collection of personal information”).

While we will always strive to collect personal information directly from you when it is reasonable and practical, there are times when we may obtain personal information about you from other individuals and organisations, sometimes without your direct involvement. For example, we may gather personal information about you from:

- related entities
- publicly available sources of information, such as public registers
- your representatives (including your legal adviser, mortgage broker, executor, administrator, guardian, trustee or attorney);
- banks, financial institutions, fund managers, superannuation funds and other financial product providers;
- your advisors;
- your employer;
- through our website;
- other organisations, who jointly with us, provide products or services to you;
- from third-parties, including credit reporting bodies (“CRB”) and other credit providers, government departments or address validation providers; and
- insurers, re-insurers and health care providers.
- suppliers and service providers in connection with providing our products and services;

We collect information when you:

- visit our website;
- submit application forms with us;
- participate in a phone call with us;
- email or otherwise correspond with us.

Laws requiring or authorising us to collect personal information

We are required or authorised to collect:

- Certain identification information about you by the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and Anti Mondy Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No.1);
- Your Tax File Number, if you choose to provide it, by the Income Tax Assessment Act 1936 (Cth); and
- Certain information in relation to your application if you have applied for insurance as required by the Insurance Contracts Act 1984 (Cth).

How do we hold personal information?

Most of the information we hold about you is stored electronically in secure data centers located in Australia and the United States ("US"), either owned by us or external service providers. Some of your information may also be stored in paper files. We implement a variety of physical and electronic security measures to safeguard the personal information we hold. For example:

- Access to information systems is controlled through identity access management;
- Employees are bound by internal information security policies and are required to keep information secure;
- All employees are required to complete training about information security; and
- We regularly monitor and review our compliance with internal policies and industry best practice.

We take reasonable steps to destroy or permanently de-identify any personal information after it can no longer be used.

Who do we disclose your personal information to, and why?

We may provide personal information about our clients to organisations outside of FPALF. Before sharing any of your personal information with another person or organisation, we take all reasonable steps to ensure that the third-party is committed to protecting your personal information to at least the same extent as we do, or that you have explicitly consented to the disclosure.

Furthermore, to protect personal information, we establish a contract with our service providers that require them to comply with the Privacy Act. These agreements ensure they

use the personal information we provide solely for the specific purposes we outline.

Generally, we disclose personal information to organisations that help us. This may include:

- Our agents, contractors and external service providers (for example technology service providers);
- Insurers, re-insurers and health care providers;
- Payment systems operators (for example merchants receiving card payments);
- Other organisations, who jointly with us, provide products or services to you;
- Financial services organisations, including banks, superannuation funds, stockbrokers, custodians, fund managers and portfolio service providers;
- Credit reporting bodies and other credit providers;
- Debt collectors
- Legal advisers or auditors
- Your representatives (including your legal adviser, accountant, mortgage broker, executor, administrator, guardian, trustee or attorney);
- IT service providers;
- External dispute resolution schemes;
- Regulatory bodies, governments agencies and law enforcement bodies in any jurisdiction; and
- Our related entities, including our parent companies and subsidiaries. Additionally, in the event of a sale, merger, or other transfer of our business or assets, your information may also be disclosed to or transferred with the buying entity.
- We may also disclose your personal information to others outside FPALF where:
- We are required or authorised by law or where we have a public duty to do so;
- You may have expressly consented to the disclosure or the consent may be reasonably inferred from the circumstances; or
- We are otherwise permitted to disclose the information under the Privacy Act.

Transborder disclosure of personal information

We may disclose your personal information to a recipient which is located outside Australia:

- As a result of using cloud software where servers are located outside Australia. This includes our service providers which are likely to be located in the US, New Zealand or other countries;
- Any financial institution which you hold an account with overseas where you have given us permission to make enquiries on your behalf;
- Organisations, staff and/or contractors operating overseas including US, China and Croatia, who assist us with our business and services we provide you.
- Our staff if they are located outside of Australia.

What if you don't provide us with your personal information?

We will offer individuals the option to remain anonymous or use a pseudonym when interacting with us, provided it is lawful and practicable to do so. A pseudonym refers to a name or other identifier that differs from the individual's actual name.

For instance, you can visit our website and make general phone inquiries without needing to identify yourself.

However, in some cases, if you choose not to provide the requested personal information, we may not be able to deliver the product or service you're seeking.

Credit related information

Why we collect credit-related personal information

We collect, hold, use and disclose credit related personal information for the purposes permitted by the Privacy Act and the Privacy (Credit Reporting) Code 2014 ("CR Code") and so as to provide our services to you including, but not limited to:

- Financial planning and strategy review services;
- Investment advice;
- Insurance and protection advice;
- Debt finance and mortgage broking;
- Retirement and estate planning; and

- Other purposes required or authorised by law.

What information we collect for credit purposes?

The credit related personal information that we may collect and hold includes:

- Your current and prior names, date of birth, address, gender and driver's licence number;
- financial information for example, your income, expenses, assets and liabilities;
- information about credit that has been provided to you;
- credit payments of $100 or more owed to another credit provider that are overdue for more than 60 days that you have been notified of (and whether you have subsequently repaid the overdue amount);
- whether you have committed a serious credit infringement;
- credit related court proceedings and personal insolvency information;
- publicly available credit related information; and
- a credit rating or score that is calculated by a CRB and that has a bearing on your credit-worthiness.

How do we use personal information collected for credit purposes?

Where you have consented to it, we will use your personal information to better inform ourselves as to your credit position and, in undertaking our services to you, we may provide personal information about you that we have collected to:

- service providers and specialist advisers to FPALF who have been contracted to provide us with support, administrative, financial, insurance, research or other services;
- insurers, credit providers, courts, tribunals and regulatory authorities as agreed or authorised by law;
- credit reporting or reference agencies or insurance investigators; and
- anyone authorised by you, or specified by you or by a contract to which you are a party.

Which credit reporting bodies do we deal with?

We may deal with the following Credit Reporting Body (CRB): Equifax

Equifax organises, assimilates and analyses data on more than 820 million consumers and more than 91 million businesses worldwide.

www.equifax.com.au

You can ask Equifax not to use the information disclosed for the purpose of pre- screening of direct marketing by a credit provider

What if you are a victim of fraud?

If you think you have been a victim of fraud, you can request the above credit reporting body not to disclose credit reporting information about you.

Direct marketing

We may use your personal information to offer products and services that we believe may interest you, but we will respect your preference if you ask us not to. We may contact you about these offers through various channels, including mail, phone, email, SMS, or other electronic methods such as social media or targeted ads on our websites.

We may also share your personal information with third-party companies outside of FPALF that help us market our products and services to you.

If you have consented to receiving marketing communications from us, your consent will remain valid until you inform us otherwise. However, you can opt out at any time by:

- contacting us (details at the end of this Policy); or
- using the unsubscribe facility that we include in our electronic messages. If we have collected the personal information that we use to send you marketing communications from a third-party (for example a direct mail database provider), you can ask us to notify you of our source of information, and we will do so, unless this would be unreasonable or impracticable.

Electronic collection

We will collect information from you electronically, for instance through internet browsing, mobile or tablet applications.

Each time you visit our website, we collect information about your use of the website, which may include the following:

- the date and time of visits;
- which pages are viewed;

- how users navigate through the site and interact with pages (including fields completed in forms and applications completed);
- location information about users;
- information about the device used to visit our website; and
- IP addresses.

We use a technology called cookies when you visit our site. Cookies are small pieces of data stored on your hard drive or in memory. They help record details about your visit, enabling the site to remember you the next time you return and provide a more personalized experience.

One of the reasons we use cookies is to enhance your security. The cookies we send to your computer cannot read your hard drive, access any information from your browser, or control your computer. They are specifically designed to prevent them from being sent to other sites or accessed by any unauthorised parties.

We won't ask you to supply personal information publicly over Facebook, Instagram, LinkedIn, X (formerly Twitter), or any other social media platform that we use. Sometimes we may invite you to send your details to us via private messaging, for example, to answer a question.

Access to and correction of personal information

At any time you can request access to the personal information we hold about you. You can also ask for corrections to be made. To do so, please contact us (details at the end of this Policy).

You can also apply to access personal information about you that a CRB holds by contacting the relevant CRB using the contact information set out above.

There is no fee for requesting that your personal information is corrected or for us to make corrections. In processing your request for access to your personal information, a reasonable cost may be charged. This charge covers such things as locating the information and supplying it to you.

There are some circumstances in which we are not required to give you access to your personal information.

If we deny your request to access or correct your personal information, we will provide you with a notice explaining our reasons, unless it would be unreasonable to do so.

If we refuse your request to correct your personal information, you also have the right to ask that a statement be added to your record indicating that you disagree with its accuracy.

In the event that we deny your request to access or correct your personal information, we will inform you of the process for lodging a complaint about the refusal.

General

Data Quality and Security

FPALF is committed to keeping your personal information secure and confidential. All reasonable precautions will be taken to protect personal information from loss, misuse, unauthorised access or alteration. We take reasonable steps to:

- make sure that the personal information that we collect, use and disclose is accurate, up to date and complete and (in the case of use and disclosure) relevant;
- protect the personal information that we hold from misuse, interference and loss and from unauthorised access, modification or disclosure; and
- destroy or permanently de-identify personal information that is no longer needed for any purpose that is permitted by the APPs.

You can help us keep your information up to date by letting us know about any changes to your details, such as your address, email address or phone number.

You acknowledge that the security of online transactions conducted through the website cannot be fully guaranteed. To the maximum extent allowed by law, FPALF is not responsible for any misuse, loss, or unauthorised access to your personal information where the security of that information is beyond FPALF's control.

Within FPALF, access to personal information is restricted to personnel on a need to know basis. FPALF has directed its staff that personal information must be dealt with in accordance with this Policy and kept secure from unauthorised access or disclosure. We educate our staff about their duty to protect your privacy and provide training regarding this Policy.

Security

The steps we take to secure the personal information we hold include website protection measures (such as firewalls and anti-virus software), security restrictions on access to our computer systems (such as login and password protection), controlled access to our corporate premises, policies on document storage and security, personnel security

(including restricting access to personal information on our systems to staff who need that access to carry out their duties), staff training and workplace policies.

Website Security

While we strive to protect the personal information and privacy of users of our website, we cannot guarantee the security of any information that you disclose online and you disclose that information at your own risk. If you are concerned about sending your information over the internet, you can contact us by telephone or post (details at the end of this Policy).

If you are a registered user of our website and/or our client portal, you can also help to protect the privacy of your personal information by maintaining the confidentiality of your username and password and by ensuring that you log out of the website when you have finished using it. In addition, if you become aware of any security breach, please let us know as soon as possible.

IP Address

An IP (internet protocol) address is a number that is automatically assigned to your computer by your internet service provider when you log on. Your IP address is not linked to your personal information but we do preserve the right to use IP addresses to identify individuals who may threaten our site, services or clients. IP addresses may also be used to help diagnose problems with our website and to gather broad demographic information.

Third party websites

Links to third party websites that are not operated or controlled by us are provided for your convenience. We are not responsible for the privacy or security practices of those websites, which are not covered by this Policy. Third party websites should have their own privacy and security policies, which we encourage you to read before supplying any personal information to them.

Data Breaches

If there is any breach of your personal information FPALF will deal with such breach and notify you in accordance with its obligations under the Privacy Act.

Exemptions

There is an exemption in the Privacy Act regarding information relating to current or former employees. The Privacy Act does not apply to an act done or practice engaged in by FPALF in relation to:

- a current or former employment relationship between FPALF and the individual; and
- an employee record held by FPALF relating to the individual (includes personal information relating to the employment relationship and may include information such as recruitment/termination information, terms and conditions of employment, health and banking details).

This exemption does not apply to applicants who are unsuccessful in securing a role with us. In those cases, we will take all the necessary steps to ensure proper collection, use, storage, disclosure of and access to information in accordance with the Privacy Act and other applicable laws.

Resolving privacy concerns and complaints.

If you are concerned about how your personal information is being handled or if you have a complaint about a potential breach of the Privacy Act or the APPs, please first contact our Privacy Officer.

Complaints should be directed to our Privacy Compliance Officer in writing (details below).

We will acknowledge your complaint within 24 hours or 1 business day.

If we are unable to resolve your complaint at the first point of contact, we will work with you to better understand your concerns and investigate your complaint.

Under the Privacy Act you may complain to the Office of the Australian Information Commissioner about the way we handle your personal information.

The Commissioner can be contacted via website www.oaic.gov.au or:

The Commissioner
GPO Box 5218
Sydney NSW 2001
Phone: 1300 363 992
Email: enquiries@oaic.gov.au

Contact Us

Please send feedback, comments, complaints or requests for further clarification of this Policy via email to privacy@focuspa.com.au, phone (03) 9528 8688 or by post:

Privacy Officer
Level 2, 205 Balaclava Road
Caulfield North VIC 3161