Australian Unity Life Bonds Limited Privacy Policy

Privacy Commitment

We understand that your privacy is important to you and we care about protecting the privacy and security of your personal information, including any sensitive and credit-related information.

We protect the personal information of our members and customers in accordance with Australian Privacy Laws.

About this Policy and your privacy

Australian Unity Limited (AUL)[1] and its subsidiaries are subject to the same standards for handling of personal information, regardless of which services they provide. AUL businesses include wealth, financial planning, bank, general insurance, private health insurance, trustee services, retirement villages, home care services, aged care services, and disability services.

Effective 31 October 2023, Australian Unity Life Bonds Limited (AULBL) (formerly IOOF Limited ABN 21 087 649 625) will join the Australian Unity Group.

There will be a transition period, initially for twelve months,[2] during which time IOOF Service Co Pty Ltd (ABN 99 074 572 919) (IOOF), part of the Insignia Financial Group, will continue to manage the business activities for AULBL, on behalf of AUL.

This Policy will apply to AULBL's business activities during the transition period and sets out how your personal information will be managed. It explains:

- how and why we collect, use, hold and disclose your personal information
- how you can access the information we hold about you
- how you can ask us to correct your information or make a complaint about how we have managed your information; and
- the safeguards we have in place to protect the personal information we hold.

This Policy reflects the Australian Unity Group Privacy Policy. AUL offers a broad range of products and services and the personal information we collect about our members and customers depends on the type of product or service received or requested from us. Therefore, some of the content of this Policy will not be relevant to customers who transition over from the Insignia Financial Group. At the end of the transition period, we anticipate the personal information of AULBL customers will be managed in accordance with the Australian Unity Group Privacy Policy. Customers will be notified when this occurs.

Information we collect

Personal information we collect

Personal information includes any information or opinion that can identify somebody, such as name, address, date of birth, telephone numbers or driver's license number.

The personal information we collect about you depends on the type of product or service you receive or request from us. We may also collect personal information from you, or third parties, to manage your accounts and services and to better understand you, your preferences and interests.

[1] Australian Unity is "we", "us" and "Australian Unity Group".
[2] With an option to extend for a further period of up to twelve additional months.

This information may include:

- identifying and contact information, such as name, date of birth, address, telephone number, email address and social media platform username
- demographic information, such as age and gender
- financial information, such as banking, payment and contribution details
- government issued identifiers, such as Tax File, Medicare and Driver's License numbers
- transaction information, such as records of service contacts, reasons for applying for a product or service, photographs, video and call recordings of contacts
- registration to programs offered by AUL or our partners
- activity or preference information collected by our partners, such as property sales or buying habits
- website usage; and
- other personal information needed or required by law, such as the Anti-Money Laundering and Counter Terrorist Financing Act 2006 (Cth) or tax treaties.

Sensitive information we collect

Sensitive information includes information about a person's racial or ethnic origin, political opinions, political association, religious beliefs or affiliation, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record, health information and genetic information.

We will only collect sensitive information if:

- we need it to provide you with the products or services you have requested or for one of our functions or activities, and have your consent, or
- we are legally required or allowed to collect this information.

This may include:

- health information required to provide you with healthcare, aged care, or disability services or to process an insurance claim, like your medical history, medical diagnosis, medications you need, behaviour management plans or cognitive capacity
- information to deliver culturally appropriate services, such as your religious, racial, and ethnic background; including if you identify as an Aboriginal and Torres Strait Islander person, or
- information about your personal circumstances if you want to vary your repayments for a credit product because you are experiencing financial difficulties (financial hardship).

Do you have to provide your personal information?

You can remain anonymous or use a pseudonym if we do not need your personal information to provide a product or service.

You may choose not to disclose your personal information to us, but it may limit or prevent us from releasing records to you, dealing with you, managing emergencies effectively, providing you with products and services or letting you know about other products and services that might better suit your needs.

How we collect your personal information

In most cases we'll collect personal information directly from you when apply for a product or service, use our website, apps, social media, talk to us, provide feedback, visit one of our offices or register for an Australian Unity program.

There are times where we may collect information about you from other sources.

Sometimes we collect information about you from other sources including:

- someone you have authorised to act on your behalf, like your partner, a family member, agent, power of attorney or guardian
- a third party, such as your treating hospital, dentist or other health service provider, or private health insurance fund
- a person covered under your private health insurance cover
- a person such as a spouse, parent or dependent seeking financial planning services
- a nominated beneficiary, a plan guardian or a nominated student of an investment bond
- a Data Holder (under CDR rules) from which you consented for us to collect CDR data, such as a bank or any other CDR participant of the CDR – Open Banking regime
- credit reporting bodies, if we request a report about your credit history and other credit providers
- organisations that we have an arrangement with to offer or promote products or services to you
- marketing companies, if we acquire contact information to tell people about our products and services that may be of interest to them
- brokers, aggregators or parties who may introduce you to us, such as a recruitment firm or referral partner
- referees that you provide to us as a prospective employee
- publicly available records including phone directories, websites or the electoral roll
- third parties who make information available to better understand you, your preferences and interests, and
- other related entities to help us better manage our relationship with you.

Where you have given us personal information about another person, for example a person you have authorised to act on your behalf, we expect you to tell those people that you have given us their information, and to tell them about this Policy.

When we get information we didn't ask for?

Where we receive unsolicited personal information that we do not need to deliver products and services to you (for example, in correspondence that you may send to us), we will where reasonable to do so, destroy or de-identify this information. Where we retain this information, it will be subject to this Policy.

Information we collect electronically

We collect information about our customers' preferences and behaviours to help us administer and enhance:

- the performance of our system
- the content of our website, and
- the products and services we offer to you.

We also monitor web traffic to make sure the website is available during peak periods.

Whenever anyone visits our website, online member services or apps, we collect data about their visit using 'cookies' to obtain information about how our website is being used. Until you log into our website, any browsing you do on our website is anonymous.

When you log on to our one of our online services, we will ask for information to identify you. We will also use the 'cookies' for security purposes. Our website also includes calculators which may require you to enter your personal details.

You may change the settings on your browser to reject cookies, however doing so might prevent you from accessing the secured pages of our website.

Our websites contain links to other sites, which are not subject to this Policy and our procedures. Refer to these websites directly to obtain their privacy policies and practices.

We may also engage third parties, including Facebook and Google, to use cookies, web beacons and other storage technologies to collect or receive information from our website and elsewhere on the internet, to provide measurement and analytics services and target ads.

If you wish to opt out of us using your personal information to display targeted advertising on digital platforms, please call the Insignia Financial Investor Services Team on 1800 002 217. To otherwise manage the ads you see on digital platforms, please visit the platform's website (for example, Google Ad Settings https://adssettings.google.com/ or Facebook Ad Preferences https://www.facebook.com/help/568137493302217).

How we use personal information

We use your personal information to provide you with products and services (including third party products and services) you've applied for, to identify you, to manage your account and improve the service you receive. We also use this information to comply with our legal obligations.

Some specific uses include to:

- identify you
- provide and manage a product or service, including assisting you to complete online applications, answering your enquiries and complaints
- plan and deliver your personal, clinical and care services
- assess your eligibility for membership of AUL and, if eligible, place your name, address and other required personal information on AUL's member register
- provide you with information in relation to your AUL membership (if eligible) including, regulatory notices (for example, notices of meeting) or benefits that are exclusively available to AUL members
- help us develop insights and conduct data analysis to improve the delivery of products and services, enhance our customer relationships and to effectively manage risks
- understand your interests and preferences so we can tailor our products, services and marketing and tell you about other products and services that may be of interest to you

- where you opt in, to help us to develop health programs to treat a specific illness or condition or to offer services (for example, in-home rehabilitation services)
- improve the service we provide to you by identifying training and development opportunities for our employees and representatives
- protect your accounts by identifying and investigating suspected fraud, other criminal activity or misconduct
- manage our rights and obligations regarding external payment systems, including claiming and receiving funding due to us in advance or in arrears for services planned or provided to you
- interact with regulators and government departments or agencies in relation to a complaint made by you or your representative, or an incident that is reportable to a regulator under an Act or regulation, and
- meet our obligations under applicable laws, such as the Anti-Money Laundering and Counter-Terrorism Financing Act and tax treaties.

How we use your information to tell you about our products and services

We may use your personal information to tell you about products or services you request or that we think might benefit you, including via:

- email
- SMS, or other electronic notification
- social media and other digital platforms
- our website or apps
- via the CDR consumer dashboard (for the purpose of Open Banking)
- mail, or
- telephone.

We respect the rights of our customers to choose the material they want to receive and how they wish to receive it, including by electronic means. You can therefore choose to receive only the materials you want or opt-out of receiving marketing information from us by calling the Insignia Financial Investor Services Team on 1800 002 217.

Who we disclose information to and why

We may share your personal information within the Australian Unity Group, to selected third parties to assist us with providing you with products and services and to other parties you have consented to share your information with, or where we are required by law.

We may share your personal information within the Australian Unity Group. This helps us provide you with information about other products and services within the group, verify your personal information, assess your eligibility for AUL membership and offer a streamlined customer-experience across our group.

We may also provide your personal information to selected third parties outside the Australian Unity Group to assist us to provide you with products and services, deliver technology or other support for our business systems, refer us to new customers, or assist us with marketing and data analysis.

To protect your personal information, we select service providers that we expect to comply with applicable Privacy Laws and to only use the personal information we disclose to them for the specific role we ask them to perform.

We also have agreements in place which set out the terms we expect our service providers to comply with. We may ask for information to satisfy ourselves that they can comply, and are continuing to comply, with the terms of the agreement.

For example, we may disclose personal information to:

- your representatives, including your legal adviser, accountant, mortgage broker, financial adviser, executor, administrator, guardian, trustee, funeral director (for funeral bonds), attorney or family member)
- the holder of a health insurance policy (including sensitive and health information about benefits claimed under the membership unless you have requested that we not disclose this information)
- insurers and re-insurers
- authorised representatives and credit representatives who sell or arrange products and services on our behalf
- hospital and other health service providers, including to provide you with clinical services for a specific condition, such as in-home rehabilitation services; or when it is necessary to prevent or minimise harm or injury, or to allow for safe clinical handover and continuous medical management
- financial services organisations, including banks, insurers, superannuation funds, stockbrokers, custodians, fund managers and contracted service providers
- payment systems operators (for example, merchants receiving card payments)
- our contracted service providers (for example, mailing houses, technology service providers and cloud storage providers)
- other organisations who we partner with to offer or provide products or services to you, or who provide analytical or marketing services to assist us to improve the delivery of products and services, and to enhance our customer relationships
- our professional advisers such as financial advisers, legal advisers and auditors
- fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct
- debt collectors
- external dispute resolution schemes, and
- regulatory bodies, government agencies and law enforcement bodies in any jurisdiction.

We may also disclose your information to others where:

- we are required or authorised by law
- we have obtained clear and specific consent from you, we may share with Accredited Data Recipients (ADR) as agreed with you, or
- you have expressly consented to the disclosure, or the consent may be reasonably inferred from the circumstances.

Disclosing information overseas

We may disclose your personal information to service providers located overseas. When we do disclose or store information overseas, we take reasonable steps to ensure that your information is provided with the same level of protection as it is within Australia.

We may disclose your personal information to service providers located overseas — including the United States, Canada, the United Kingdom, Ireland, India, Germany, New Zealand and the

Netherlands. In some cases, our service providers may store personal information in countries that are not listed above if that is where their computer systems or IT services are located.

When we do disclose or store information overseas, we take reasonable steps to ensure that your information is provided with the same level of protection as it is within Australia. We also comply with specific security standards prescribed by the CDR rules in relation to CDR Data.

We do this by only engaging with third parties located in a country which we believe has similar privacy laws to Australia, or by ensuring the third party can provide the same level of protection consistent with our Privacy Laws. We have agreements in place which set out the terms we expect them to comply with, which include compliance with privacy and other Australian laws. Before entering the agreement, and throughout the engagement, we may ask for information to satisfy ourselves that they can comply, and continue to comply with the terms of the agreement.

Where you ask us to disclose information to an overseas recipient, we may not take the above steps in relation to the management of your information. Where that overseas recipient is an ADR, we will comply with CDR obligations in relation to that disclosure.

How we hold and protect your information

We use a range of physical, electronic, and other security measures to protect the security, confidentiality, and integrity of the personal information we hold about you.

Most of the information we hold about you is stored electronically, and some information will be stored in paper files.

We store most of the information we hold about you electronically. Some of your information is in secure data centres that are located in Australia and some with selected service providers (including cloud service providers) who may store your information outside Australia.

The security measures we use to protect your personal information include:

- information security controls, such as passwords to control access to computer systems
- privacy training for our employees so that they know how to keep your information safe and secure
- physical security, such as locks and security systems over our paper and electronic data stores and premises
- access management controls, to prevent unauthorised people accessing our systems
- firewalls and intrusion detection software security measures for our website and computer systems, and
- processes designed to identify you when you deal with us by phone, online or face to face, to ensure we only disclose your information to you, or someone properly authorised by you.

As a Data Holder in relation to CDR Data, we comply with the security controls obligations and security standards of the CDR Privacy Safeguard Guidelines.

Unfortunately, no data transmission over the internet or data storage system can be guaranteed to be 100% secure. If you have reason to believe that the security of any account you have with us has been compromised, please contact the Insignia Financial Investor Services Team immediately on 1800 002 217.

What you can do to protect your information

Keep your access details, like your username, password and PIN, confidential and don't share them or leave them somewhere that's easy for others to access or find. Don't allow others to use your credentials or use words that are easily guessed.

Where you allow others to use your credentials or where your credentials are used by others, we will assume that they are you.

Let us know immediately if you suspect that there has been an unauthorised access to your information or use of your credentials.

Keep up to date with security information at **Scamwatch** — a website run by the Australian Competition and Consumer Commission (ACCC) which provides information to consumers about scams. www.scamwatch.gov.au

De-identified information

Where we no longer need to keep your information for a business purpose and the legal retention period for keeping this information has passed, we will either destroy or de-identify this information.

This Policy will not apply to the use of de-identified information — information where identifiers that could be used to identify you have been removed — because it is not information that identifies you.

How we will handle a data breach

In the event of any loss, or unauthorised access or disclosure of your personal information that is likely to result in serious harm to you, we will investigate and notify the Office of the Australian Information Commissioner and other relevant regulatory bodies, and notify you as required under Privacy Laws.

Accessing and correcting your personal information

Any queries about access and correction to your personal information should be directed to the Insignia Financial Investor Services Team – contact details set out below.

Accessing your information

Your request should include a detailed description of the information required, including enough information so we can verify your identity and, if necessary, your right to the information (e.g., you have consent or guardianship orders) .

We will try to provide you with the information you asked for within 30 days. We will keep you updated as to the progress of your request.

What happens if we cannot provide you access to information?

In some cases, we can refuse access or only give you access to certain information, such as if this access may interfere with the privacy of other individuals or if this access may reveal commercially sensitive information.

If you've accessed one of our services anonymously or by using minimal identifiers (e.g. just a first name and postcode or contact number) we may not be able to provide you access to personal information if we can't reasonably identify you.

If we're unable to provide you with access to your information, we'll inform you of the reasons why.

Correcting your information

If you believe that the information we hold about you is inaccurate, incomplete or out-of-date, please contact the Insignia Financial Investor Services Team on 1800 002 217 with the details of your correction request.

If we disagree with the request for correction or, by law, correction is not possible (e.g. Health data), we'll write to you to let you know why.

Resolving your privacy concerns

To resolve an issue or make a complaint about how we manage your personal information, please contact Insignia Financial.

1		**Contact the Insignia Financial Investor Services Team** Contact us directly on 1800 002 217
2		**Contact the Insignia Financial Privacy Officer** If you are not satisfied with the response, please contact the Insignia Financial Privacy Officer By mail: Privacy Officer Insignia Financial Group GPO Box 264 Melbourne VIC 3001 or by email: Privacy.Officer@insigniafinancial.com.au

If you are not satisfied with the response from Insignia Financial, there are other steps you can take.

3		**Contact an external body** If you've followed these steps and you're not happy with the outcome, you can contact the relevant external body: Office of the Australian Information Commissioner GPO Box 5218, Sydney, NSW, 2001 Phone: 1300 363 992 Fax : +61 2 9284 9666 Email: enquires@oaic.gov.au Website: www.oaic.gov.au If you are an Australian Unity banking customer, you can also contact: Australian Financial Complaints Authority (AFCA) GPO Box 3, Melbourne Vic 3001 Phone: 1800 931 678 Email: info@afca.org.au Website: www.afca.org.au (you can make a complaint online)

Getting a copy of the Policy

We encourage you to review and check regularly for any updates to this Privacy Policy. We will

publish the updated version on our website and, by continuing to deal with us, you accept this Privacy Policy as it applies from time to time. If you would like a copy of this Privacy Policy sent to you, please contact the Insignia Financial Investor Services Team on 1800 002 217.

Glossary

Accredited Data Recipient ('ADR')	A participant within the CDR- Open Banking Regime, who has been accredited by the regulator to receive CDR data.
Australian Privacy Laws	The Privacy Act 1988 (Cth) (Privacy Act), Privacy (Credit Reporting) Code 2014, Consumer Data Right (CDR) Privacy Safeguard Guidelines and other applicable laws in relation to the handling of personal information.
CDR	Consumer Data Right. This is a reform that enables individual and small business consumers to efficiently and conveniently access specified data about them held by businesses (data holders), and to authorise the secure disclosure of that data to accredited data recipients or to themselves.
CDR Data	Data that has been defined by the Consumer Data Right rules under one of the following groups of data: product data (to which Privacy safeguards do not apply), customer data, account data and transaction data.
Data holder	A participant within the CDR – Open Banking Regime (usually a Banking institution) that is holding the CDR information.
Personal information	Any information or opinion that can identify somebody, such as your name, address, date of birth, telephone numbers, or driver's license number.
Sensitive information	Personal information that is given a higher level of protection under the Privacy Act. It includes information about a person's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliation, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record, health information and genetic information.

Policy Administration

Policy Name	Privacy Policy
Policy Level	Level 3 —Business Unit Policy
Approval Body	AULBL Board
Date of Approval	31 October 2023
Policy Owner	Group Executive – Governance
Policy Administrator	General Manager, Group Risk and Compliance
Related policies	Code of Conduct Information Security Framework
Supporting procedures or guidelines	Data Breach Response Plan Transitional Service Agreement dated 23 July 2023
Date of last review	N/A
Regulator (if applicable)	Office of the Australian Information Commission (OAIC)
Compliance mechanism	Compliance with this policy is monitored using: • Monitoring of Transitional Services Agreement dated 23 July 2023 • Monitoring of complaints
Classification	External use (remove this page before publishing on internet)