

Australian Unity 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

This Policy sets out how Australian Unity¹ handles your personal information. 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
- the safeguards we have in place to protect the personal information we hold; and
- information about how we manage any credit-related information (see *Appendix: Handling your Credit related information*)



We'll also provide you with more information about how we handle your information when you fill out an application, make a claim, or receive the terms and conditions of your product or service.

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.

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

¹ Australian Unity is "we", "us" and "Australian Unity Group". Refer to "*Entities covered by this policy*" to see a list of subsidiaries covered by this Policy.

- 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 Australian Unity or our partners
- activity or preference information collected by our partners, such as property sales or buying habits
- website usage
- other personal information needed or required by law, such as the Anti-Money Laundering and Counter Terrorist Financing Act 2006 (Cth) or tax treaties, and
- credit related information.



At the end of this Policy, we have included an Appendix which outlines how we manage credit-related information. This is to be read in conjunction with other information in this Policy.

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 us on 13 29 39. 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, improve the service you receive and assess your eligibility for Australian Unity Limited (AUL) membership. 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 Australian Unity Limited'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 13 29 39. If you are an AUL member you can tell us how or if you want to see specific AUL member documents such as notices of meeting, annual reports and member marketing communications, by visiting our member portal at members.australianunity.com.au. Before accessing this website, you will need to register for a member portal account at australianunity.com.au/benefits.

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 us immediately on 13 29 39.

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 13 29 39, emailing us via our website www.australianunity.com.au/contact-us, or writing to us.

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 us 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, contact us first and let us respond to your complaint.

1		Contact us Contact us directly on 13 29 39 or email us through the website www.australianunity.com.au/contact-us
2		Escalate to our complaints teams If you are not satisfied with our response, ask to speak to our Complaints Team.
3		Contact Australian Unity's Privacy Officer Group Privacy Officer Australian Unity Limited Level 15, 271 Spring Street Melbourne VIC 3000

If you are not satisfied with our response, there are other steps you can take.

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

4



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 us.

Entities covered by this Policy

Australian Unity Limited and its subsidiaries are subject to the same standards for handling of personal information, regardless of which services they provide. Australian Unity Limited businesses include our dental centres, wealth, financial planning, bank, general insurance, private health insurance, trustee services, retirement villages, home care services, aged care services, and disability services. Our subsidiaries include but are not limited to:

- Australian Unity Health Limited
- Australian Unity Bank Limited
- Lifeplan Australia Friendly Society Limited
- Australian Unity Retirement Living Services Limited
- Australian Unity Finance Limited
- Australian Unity Trustees Limited
- Australian Unity Property Limited
- Australian Unity Care Services Pty Ltd
- Australian Unity Home Care Service Pty Ltd
- Remedy Healthcare Group Pty Ltd
- Australian Unity Health Care Pty Limited
- Australian Unity Funds Management Limited
- Australian Unity Investment Real Estate Limited

The credit reporting provisions in this Policy apply to Australian Unity Bank Limited because it provides consumer credit products and services to its retail banking customers and handles credit-related information.

Appendix: Handling your credit-related information

Additional information about how Australian Unity Bank Limited collects, uses, discloses credit related information (a subset of personal information) is outlined below.

Credit-related information we collect



Credit-related information is a type of personal information that includes “credit information” and “credit eligibility information”. The glossary end of this Policy contains definitions of these terms.

When you apply for credit, give a guarantee, or have a credit product with Australian Unity Bank Limited, we collect credit-related information relevant to your application. We also collect credit information for ongoing management of your account.

Some of the information we collect is:

- the type of credit product you want, and how much you want to borrow
- financial information, such as: employment, income, expenses, savings and transaction account history
- information from a credit report from a credit reporting body
- how you have managed the repayment obligations on other credit products with us, and other financial institutions, and
- details about any bankruptcies, insolvencies, or other credit-related court proceedings.

Credit-related information we collect from others

If you apply for credit or give a guarantee or have a credit product with Australian Unity Bank Limited, we collect personal information and credit-related information about you from third parties, such as:

- any referees that you provide
- your employer
- credit providers, and
- third party service providers including credit reporting bodies.

Credit-related information we use, disclose and why

When you apply for a credit product, or act as guarantor for a person applying for a credit product, we collect information about you from credit reports provided by credit reporting bodies. We use this information, along with other credit-related information we have collected from you, to assess your application.

To obtain a credit report, we provide information to the credit reporting body:

- that identifies you
- the type of account you are applying for, and
- the amount you are applying for.

We may also provide information about the way in which you manage your account, such as:

- whether you make your repayments on time

- if you fail to make repayments
- if you default on your obligations to repay your credit contract, or
- if you commit a serious infringement, such as fraudulent behaviour or deliberately fail to make your repayments.

We may deal with the following credit reporting bodies: Equifax Pty Ltd, Illion Australia Pty Ltd and Experian Australia Credit Services Pty Ltd. These bodies are required to have a privacy policy which explains how they manage your personal information.

You can access their respective policies on their websites:

- www.equifax.com.au/privacy
- www.illion.com.au/privacy-policy
- www.experian.com.au/privacy-policy.

Home loan customers

If you require mortgage insurance, we share your personal and credit-related information with our mortgage insurer Genworth Financial Mortgage Insurer Insurance Pty Ltd.

You can access their privacy policy on their website:

- www.genworth.com/online-privacy-policy.html.

Refusal of credit applications

We may refuse an application for consumer credit made by you or with other applicants.

Our refusal may be based on credit eligibility information from a credit reporting body about you, another applicant or another person proposed as guarantor. If this occurs, we'll give you written notice that the application has been refused based on that information. We'll tell you the name and contact details of the relevant credit reporting body and other relevant information.

Have you been a victim of fraud?

Credit reporting bodies collect credit information about individuals which they provide as credit reports to credit providers (for example, Australian Unity Bank Limited), and others in the credit industry to help with managing credit risk, collecting debts and other activities.

You can also ask a credit reporting body through contact details on their website, not to use or disclose your personal information if you believe on reasonable grounds that you have been, or are likely to be, a victim of fraud, including identity fraud.

Correction of credit-related information

If you believe incorrect information was provided to us by a credit reporting body, or information we have provided to a credit reporting body is incorrect, we'll contact the credit reporting body and other credit providers to investigate the accuracy of your information.

This can take up to 30 days. If we need longer, we will let you know why. We will also tell you when we correct the information.

If we do not agree that the information is incorrect, we will write to you to tell you why and what you can do if you are not satisfied with our response.

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.
Credit eligibility information	Information that has been obtained from a credit reporting body, or that has been derived from that information, that is about an individual's credit worthiness.
Credit information	<p>Personal information that includes the following:</p> <ul style="list-style-type: none"> • information about an individual, like their name and address, that we may use to identify that individual • information about an individual's current or terminated consumer credit accounts and an individual's repayment history • the type and amount of credit applied for in any previous consumer or commercial credit applications to any credit provider, where that credit provider has requested information • information about an individual from a credit reporting body • information about consumer credit payments overdue for at least 60 days and for which collection action has started • advice that payments that were previously notified to a credit reporting body as overdue are no longer overdue • information about new credit arrangements an individual may have made with a credit provider, in relation to consumer credit currently or previously held, to deal with any defaults or serious credit infringements by that individual • information about court judgments which relate to credit that an individual has obtained or applied for • information about an individual on the National Personal Insolvency Index • publicly available information about an individual's credit worthiness, and • an opinion of a credit provider that an individual has committed a serious infringement of credit provided by that credit provider. <p>We may not hold all of these kinds of information about a particular individual. If we hold any of these kinds of information, it is protected as "credit information" under this Privacy Policy.</p>
Credit-related information	Means Credit information, Credit eligibility information and related information.
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.