Shartru Wealth Management Privacy Policy Statement

Protecting our clients' privacy is very important to us. The Privacy Act requires that we handle your personal information in accordance with a set of national principles, known as the Australian Privacy Principles (APPs), which regulate the collection, use, correction, disclosure and transfer of personal information about individuals by organisations like us in the private sector. This Policy explains our policies and practices with respect to the collection, use and management of your personal information and our approach to the APPs.

Roles, Responsibilities and Policy Governance

The Shartru Board is ultimately responsible for overseeing this Policy. The CEO and/or Privacy Officer is responsible for updating this Policy and for managing the business impacts of privacy laws within Shartru.

This Policy is reviewed and updated annually by the CEO and/or Privacy Officer, unless required earlier. The most current version of the Policy can be obtained from our website at www.shartruwealth.com.au. Questions about this policy should be directed to the CEO and/or Privacy Officer.

Further Information and Feedback

You can contact our CEO and/or Privacy Officer by:

Phone: 1300 478 424
Mail: PO Box 565 Belmont NSW 2280
Email: compliance@shartru.com.au

Members of our Group

The Shartru Group includes:

- Shartru Wealth Management ABN 46 158 536 871 (Holds an Australian Financial Services Licence 422409 and provides financial planning advice to retail and wholesale clients)
- Shartru Capital Group Pty Ltd ABN 87 160 155 322 (Investment and Advisory Firm)
- Shartru Investment Management Pty Ltd ABN 46 604 880 006 (Investment Manager for the Shartru Managed Discretionary Account Service)
- Shartru Agency Pty Ltd ABN 45 622 327 897
  (Real Estate services)
- It also includes our Corporate Authorised Representatives and Authorised Representatives.

Members of the group that have collected personal information are permitted by the Privacy Act to

disclose personal information to other members of the group. We only share information where this is relevant to the purpose. The list of Authorised Representatives changes from time to time and details of our current authorised entities and representatives are available at www.asic.gov.au.

General Obligations

What information do we collect?

We will collect and hold your personal information for the purposes of:

- providing advice, products and services to you
- managing and administering your products and services
- verifying your identity
- letting you know about our other products and services.

The type of information collected from you includes information that is necessary to operate your account or for us to provide advice to you. We may ask you to provide personal information such as your:

- contact details including name and e-mail address, residential and/or postal address and phone number
- personal details including date of birth, financial goals and standing plus medical history
- estate planning details
- occupation and employment arrangements
- residency status and tax file number (TFN).

This information is primarily collected from forms you have completed, or through ongoing communications with you or persons you authorise to communicate with us on your behalf such as your adviser.

We will inform you of any legal requirements for us to ask for information about you and the consequences of not giving us that requested information. For example, in addition to the personal information we will obtain from you, whenever you acquire a new product or service from us, we may require documents evidencing your identity. Such evidence may include a certified copy of your driver's licence, passport or birth certificate.

We will only solicit personal information about you where you have knowingly provided that information to us, we believe you have authorised a third party to provide that information to us, or we are obligated by law to obtain such information. Third parties that we may need to collect information from include your financial adviser, product issuer, employer, accountant or solicitor. To verify your identity for Know Your Customer (KYC) purposes, we may also solicit personal information about you from reliable identity verification service providers.

There are specific circumstances in which we will ask for your consent to provide sensitive information such as:

- health information when you apply for insurance or from medical practitioners when you make a claim
- income information when you apply for insurance protection or salary continuance insurance
- details of your dependents.

What if you do not give us the information we request?

You are not obligated to give us the information that we request. However, if you do not give us the information that we ask for, or the information you give is not complete or accurate, this may:

- prevent us being able to provide you with financial services and/or advice
- prevent our services from meeting your needs or may cause you to suffer unforeseen financial consequences
- prevent or delay the processing of your applications or insurance claims
- affect your eligibility for specified insurance cover
- impact the taxation treatment of your account
- prevent us from contacting you.

For example, if you elect not to provide us with your personal information as and when requested, we may not be able to provide you with financial advice due to inability to meet requirements under the Corporations Act 2001.

Use of information

How do we use the information that we collect from you?

We use your personal information for the purpose for which it has been obtained and for related purposes. For example, we collect your personal information so that we can act on your request to:

- provide financial advice to you
- provide assistance with ancillary services such as Centrelink
- establish your investment and superannuation accounts
- set-up and administer a self-managed super fund
- implement your investment instructions
- establish and maintain insurance protection
- report the investment performance of your account
- keep you up to date on other products and services that may be of interest to you.

We will not adopt as our own any identifiers that you may provide to us such as TFNs, Medicare numbers etc. They may be held on file if you have provided consent.

Disclosure

Who do we give your information to?

For the purpose of providing services to you (or a related purpose), we may provide your information to other companies within the Shartru Group or external parties. Where personal information is disclosed, there are strict controls in place to ensure information is held, used and disclosed in accordance with the APPs.

The types of external organisations to which we may disclose your personal information include:

- your financial adviser
- organisations involved in providing, managing or administering our products or services such as paraplanning services, advice software vendors, external dispute resolution services, insurers, investment managers, product

issuers, superannuation trustees or mail houses
- medical practitioners and other relevant professionals, where you have applied for insurance cover or made a claim for disablement benefit
- your personal representative, or any other person who may be entitled to receive your death benefit, or any person contacted to assist us to process that benefit
- other Australian Financial Services Licensees or financial advisers or their agents for due diligence purposes in the event of business sales
- financial institutions that hold accounts for you
- professional advisers appointed by us such as auditors to ensure the integrity of our operations
- professional advisers appointed by you (including your accountant, solicitor, executor, administrator, trustee, guardian or attorney)
- businesses that may have referred you to us (for example your Accountant).

Like other financial services companies, there are situations where we may also disclose your personal information where it is:

- required by law (such as to the Australian Securities and Investments Commission, Australian Taxation Office or pursuant to a court order)
- authorised by law (such as where we are obliged to disclose information in the public interest or to protect our interests)
- necessary to discharge obligations (such as to foreign governments for the purposes of foreign taxation)
- required to assist in law enforcement (such as to a police force).

We may also disclose your information if you give your consent.

Will my information be disclosed overseas?

It is generally unlikely that we will disclose your personal information overseas. However, we may use third-party service providers or outsourcing services that include offshore operations to provide services to you. Depending on the circumstances, the relevant countries will vary such that it is not practicable to list them here.

Any overseas disclosure does not affect our commitment to safeguarding your personal information and we will take reasonable steps to ensure any overseas recipient complies with the APPs.

Where we may be transferring your personal information overseas, we will either seek your consent or inform you and ensure that appropriate contractual measures are in place requiring the overseas entity to protect your personal information in accordance with our obligations under Australian privacy law.

Access and correction of information

Can I access my information and what if it is incorrect?

You may request access to the personal information we hold about you. We may charge a reasonable fee to cover our costs.

There may be circumstances where we are unable to give you access to the information that you have requested. If this is the case, we will inform you and explain the reasons why.

We will take reasonable steps to ensure that the personal information we collect, hold, use or disclose is accurate, complete, up to date, relevant and not misleading.

You have a right to ask us to correct any information we hold about you if you believe it is inaccurate, incomplete, out of date, irrelevant or is misleading. If we do not agree with the corrections you have supplied and refuse to correct the personal information, we are required to give you a written notice to that effect and a statement if requested.

If you wish to access or correct your personal information, contact your adviser in the first instance. You may then contact us through our offices or by writing to the CEO and/or Privacy Officer.

Protection of the personal and sensitive information that we hold

How do we protect the security of your information?

We have security systems, practices and procedures in place to safeguard your privacy. We also train our authorised representatives and staff as to their obligations about your personal information.

We may use cloud storage or third-party servers to store the personal information we hold about you. These services are subject to regular audit and the people who handle your personal information have the training, knowledge, skills and commitment to protect it from unauthorised access, disclosure or misuse.

If you use secure sections of our websites, we will verify your identity by your username and password. Once verified, you will have access to secured content. You are responsible for maintaining the secrecy of your login details.

Our authorised representatives protect information in several ways including providing secure storage for physical records, restricting access to their office to authorised persons, and ensuring client data is regularly backed up offsite.

Risks of using the internet

There are inherent security risks in transmitting information through the internet. You should assess these potential risks when deciding whether to use our online services. If you do not wish to transmit information through electronic means, there are other ways in which you can provide this information to us.

Our websites may use cookies and/or other analytics tools which may enable us to identify you, your browser or other information about you while you are using our site. These cookies may be permanently stored or temporary session cookies. They are used for a variety of purposes, including security and personalisation of services. They are frequently used on websites and you can choose if and how a cookie will be accepted by configuring your preferences and options in your browser.

All browsers allow you to be notified when you receive a cookie and you may elect to either accept it or not. If you wish not to accept a cookie, this may impact the effectiveness of the website. Your internet service provider or other IT service provider should be able to assist you with setting your preferences.

Where you choose to communicate with us by email, we will store your email, name and address with any other contact or personal details you have provided on our databases.

Retention of your personal information

We are required by law to retain certain records of information for varying lengths of time and, in certain circumstances, permanently. Where your personal information is not required to be retained under law and is no longer required for the purpose for which it was collected, we will take reasonable steps to irrevocably destroy or de-identify it.

European Union General Data Protection Regulation (GDPR)

If you reside in a country that is a member of the European Economic Area (the EU and Norway, Lichtenstein and Iceland), in addition to the protection you receive under the Privacy Act, you are entitled to other protections provided by the GDPR, including, in certain circumstances, the right to:

- have your personal information erased
- access your personal information in an electronic and portable format
- restrict or object to the processing of your personal information.

Complaints and breaches

If you believe that we have breached the APPs by mishandling your information, you may lodge a complaint with the CEO and/or Privacy Officer.

- The CEO and/or Privacy Officer will respond to your complaint within 30 days.
- If you are not satisfied with the outcome, you may lodge a complaint with the Australian Information Commissioner (OAIC). Further information is available at www.oaic.gov.au.

If you have a complaint about a breach of the GDPR, you may contact the local regulator in your European Economic Area.

We are committed to helping you have control of your personal information and so it is our practice to take reasonable steps to notify you if we are aware that we have breached your privacy.

In accordance with the Notifiable Data Breaches Scheme, if your personal information is involved in a data breach that is likely to result in serious harm to you, we will notify you and the Australian Information Commissioner.