Shartru Wealth Privacy Policy and Collection Statement
(Privacy Policy)

Drafted by: Compliance Officer
Approved by: Compliance Manager
Version: 3
Date Approved: 08/09/2023

Shartru Wealth Management Privacy Policy and Collection Statement

Shartru Wealth Management Pty Ltd (ACN 158 536 871, AFSL 422 409) (Shartru Wealth) is bound by the Privacy Act 1988 (Privacy Act), including the Australian Privacy Principles (APPs), and recognises the importance of ensuring the confidentiality and security of your personal information.

All third parties (including clients, suppliers, sub-contractors, or agents) that have access to or use personal information collected and held by Shartru Wealth, must abide by this Privacy Policy and Collection Statement (Privacy Policy).

In this Privacy Policy:

- Disclosure of information means providing information to persons outside of Shartru Wealth;
- Personal information means information or an opinion relating to an individual, which can be used to identify that individual;
- Sensitive information is personal information that includes information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences and criminal record, and also includes health information; and
- Use of information means use of information within Shartru Wealth.

Roles, responsibilities, and policy Governance

The Shartru Wealth Board is ultimately responsible for overseeing this Policy. The Compliance Manager is responsible for updating this Policy and for managing the business impacts of privacy laws within Shartru Wealth.

This Policy is reviewed and updated annually by the Compliance Manager 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 Compliance Manager.

Further Information and Feedback

You can contact our Compliance Manager by:

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

Members of Shartru Pty Ltd ATF Shartru Unit Trust Group

The Shartru Group includes:

- Shartru Wealth Management (SWM) ABN 46 158 536 871 (Holds an Australian Financial Services Licence 422409 and provides financial planning advice to retail and wholesale clients)
- All entities identified within Shartru Pty Ltd.
- It also includes our Corporate Authorised Representatives and Authorised Representatives of Shartru Wealth.

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.

Related Policies

This policy is in conjunction with other related policies; SWM Cyber Resilience, SWM Notifiable Data Breaches, Data Breach Response Policy, SWM Privacy & Information management, SWM Outsourcing, SWM Document Retention, SWM Marketing your Advice, SWM Information & Technology, SWM Internal Dispute Resolution (Complaints) and SWM Monitoring & Supervision.

What personal information do we collect and hold?

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

- providing advice, recommendation of 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 your name, address (residential or postal), phone numbers, email addresses,
- occupation and employment arrangements;
- bank account details;
- driver's licence details;
- date of birth;
- financial information, including details of your investments, your insurance policies, estate planning strategies, taxation information, health information;
- residency status and tax file number (TFN).

How do we protect personal information?

We generally collect personal information directly from you. This information is primarily collected through 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 do not give you the option of dealing with them anonymously, or under a pseudonym. This is because it is impractical, and, in some circumstances, illegal for Shartru Wealth to deal with individuals who are not identified.

We will not collect sensitive information about you without your consent, unless an exemption in the APPs applies. These exceptions include if the collection is required or authorised by law, or necessary to take appropriate action in relation to suspected unlawful activity or serious misconduct. If the personal information we request is not provided by you, we may not be able to provide you with the benefit of our services, or meet your needs appropriately.

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.

Unsolicited Personal Information

We may receive unsolicited personal information about you. We destroy or de-identify all unsolicited personal information we receive, unless it is relevant to our purposes for collecting personal information. We may retain additional information we receive about you if it is combined with other information we are required or entitled to collect. If we do this, we will retain the information in the same way we hold your other personal information.

Who do we collect personal information about?

The personal information we may collect and hold includes (but is not limited to) personal information about:

- clients;
- potential clients;
- service providers or suppliers;
- prospective employees, employees and contractors; and
- other third parties with whom we come into contact

Use of Information

Why do we collect and hold personal information?

We may use and disclose your personal information for any of the following purposes. We may also use and disclose your personal information for secondary purposes which are related to the primary purposes set out above, or in other circumstances authorised by the Privacy Act.

Sensitive information will be used and disclosed only for the purpose for which it was provided (or a directly related secondary purpose), unless you agree otherwise, or an exemption in the Privacy Act applies. 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.

Disclosure

Who might we disclose personal 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. If we disclose your personal information to service providers that perform business activities for us, they may only use your personal information for the specific purpose for which we supply it. We will ensure that all contractual arrangements with third parties adequately address privacy issues, and we will make third parties aware of this Privacy Policy. 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;
- a related entity of Shartru Wealth;
- 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).
- Organisations involved in in a transfer of sale of all or part of our assets or business
- Organisations involved in managing payments, including payment merchants and other financial institutions such as banks.

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

Will my information be disclosed overseas?

We may disclose your personal information overseas. 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.

We will not send personal information to recipients outside of Australia unless:

- we have taken reasonable steps to ensure that the recipient does not breach the Act and the APPs,
- the recipient is subject to an information privacy scheme similar to the Privacy Act; or
- the individual has consented to the disclosure.

If you consent to your personal information being disclosed to an overseas recipient, and the recipient breaches the APPs, we will not be accountable for that breach under the Privacy Act, and you will not be able to seek redress under the Privacy Act.

Access and correction of information

Can I access my personal information?

Subject to the exceptions set out in the Privacy Act, you may gain access to the personal information that we hold about you by contacting the Shartru Wealth's Compliance Manager. 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 provide access within 30 days of the individual's request. If we refuse to provide the information, we will provide reasons for the refusal.

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. We will require identity verification and specification of what information is required. An administrative fee for search and photocopying costs may be charged for providing access.

How do we keep personal information accurate and up-to-date?

We are committed to ensuring that the personal information we collect, use and disclose is relevant, accurate, complete and up-to-date.

We encourage you to contact us to update any personal information we hold about you. If we correct information that has previously been disclosed to another entity, we will notify the other entity within a reasonable period of the correction. Where we are satisfied that the information is inaccurate, we will take reasonable steps to correct the information within 30 days, unless you agree otherwise. We do not charge you for correcting the information.

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 Compliance Manager.

Protection of the personal and sensitive information that we hold

Management of personal information

We recognise the importance of securing the personal information of our customers. We will take steps to ensure your personal information is protected from misuse, interference or loss, and unauthorised access, modification or disclosure.

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 regarding your personal information.

Your personal information is generally stored in our Client Relationship Management (CRM Systems) or cloud based software. Any paper files are stored in secure areas. In relation to information that is held on our CRM database, or the cloud, we apply the following guidelines:

- passwords are required to access the system, and passwords are routinely checked;
- data ownership is clearly defined;
- we change employees' access capabilities when they are assigned to a new position;
- employees have restricted access to certain sections of the system;
- the system automatically logs and reviews all unauthorised access attempts;
- unauthorised employees are barred from updating and editing personal information;
- data is encrypted during transmission over the network; and
- print reporting of data containing personal information is limited.

For all employees we implement the following additional security measures:

- two-factor authentication is enabled for all email accounts;
- password complexity is enforced;

- we ensure that employees only have access to personal information which is directly relevant to their duties;
- employees are not permitted to work in public spaces;
- we monitor access to personal information, and will investigate and take appropriate action if any instances of unauthorised access by employees are detected;
- employees work from home must ensure that no other member of their household uses their work device;
- employees must store devices in a safe location when not in use;
- employees may not make hard copies of documents containing personal information, nor may they email documents containing personal information to their personal email accounts; and
- employees may not disclose an individual's personal information to colleagues or third parties via personal chat groups.

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.

Direct marketing

We may only use personal information we collect from you for the purposes of direct marketing without your consent if:

- the personal information does not include sensitive information; and
- you would reasonably expect us to use or disclose the information for the purpose of direct marketing; and
- we provide a simple way of opting out of direct marketing; and
- you have not requested to opt out of receiving direct marketing from us.

If we collect personal information about you from a third party, we will only use that information for the purposes of direct marketing if you have consented (or it is impracticable to obtain your consent), and we

will provide a simple means by which you can easily request not to receive direct marketing communications from us. We will draw your attention to the fact you may make such a request in our direct marketing communications.

You have the right to request us not to use or disclose your personal information for the purposes of direct marketing, or for the purposes of facilitating direct marketing by other organisations. We must give effect to the request within a reasonable period of time. You may also request that we provide you with the source of their information. If such a request is made, we must notify you of the source of the information free of charge within a reasonable period of time.

Identifiers

We do not adopt identifiers assigned by the Government (such as drivers' licence numbers) for our own file recording purposes, unless one of the exemptions in the Privacy Act applies.

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.

Updates to this Privacy Policy

This Privacy Policy will be reviewed from time to time to take account of new laws and technology, and changes to our operations and the business environment.

Responsibility

It is the responsibility of management to inform employees and other relevant third parties about this Privacy Policy. Management must ensure that employees and other relevant third parties are advised of any changes to this Privacy Policy. All new employees are to be provided with timely and appropriate access to this Privacy Policy, and all employees are provided with training in relation to appropriate handling of personal information. Employees or other relevant third parties that do not comply with this Privacy Policy may be subject to disciplinary action.

Non-Compliance and disciplinary actions

Privacy breaches must be reported to management by employees and relevant third parties. Ignorance of this Privacy Policy will not be an acceptable excuse for non-compliance. Employees or other relevant third parties that do not comply with this Privacy Policy may be subject to disciplinary action.

Your rights

This Privacy Policy contains information about how:

- you may access the personal information we hold about you;
- you may seek the correction of your personal information;
- you may ask us to provide an alternative means of identity verification for the purposes of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)*;*
- you may complain about a breach of the Privacy Act, including the APPs; and
- we will deal with a privacy complaint.

Contractual arrangements with third parties

We ensure that all contractual arrangements with third parties adequately address privacy issues, and we make third parties aware of this Privacy Policy. Third parties will be required to implement policies in relation to the management of your personal information in accordance with *the Privacy Act*. These policies include:

- regulating the collection, use and disclosure of personal and sensitive information;
- de-identifying personal and sensitive information wherever possible;
- ensuring that personal and sensitive information is kept securely, with access to it only by authorised employees or agents of the third parties; and

- ensuring that the personal and sensitive information is only disclosed to organisations which are approved by us.

Incidents / Complaints handling/ Making a Complaint

We have an effective complaints handling process in place to manage privacy risks and issues. If you believe that we may have breached the APPs by mishandling your information, you may lodge a complaint with the Compliance Manager.

- The Compliance Manager will respond to your complaint within 30 days.

The complaints handling process involves:

- identifying (and addressing) any systemic/ongoing compliance problems;
- increasing consumer confidence in our privacy procedures; and
- helping to build and preserve our reputation and business.

You can make a complaint to us about the treatment or handling of your personal information by lodging a complaint with the Compliance Manager.

If you have any questions about this Privacy Policy, or wish to make a complaint about how we have handled your personal information, you can lodge a complaint with us by:

- in writing – PO Box 565 Belmont, NSW 2280
- phone - 1300 478 424
- emailing – compliance@shartru.com.au

If you are not satisfied with our response to your complaint, you can also refer your complaint to the Office of the Australian Information Commissioner by:

- telephoning – 1300 363 992
- writing – Director of Complaints, Office of the Australian Information Commissioner, GPO Box 5218, SYDNEY NSW 2001
- online submission – https://forms.business.gov.au/smartforms/landing.htm?formCode=APC_PC

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.