PRIVACY POLICY

Alere Private Wealth Pty Ltd abides by the Australian Privacy Principles ('APP's) established under the Privacy Act 1988 and Privacy Amendment (Enhancing Privacy Protection) Act, 2012. Detailed below, for your information, is our policy on the management of personal information.

APP1 – Open & transparent Management of Personal Information

We are committed to managing any personal information we collect from our clients in an open and transparent way.

We collect personal information from you and about you as part of our advisory role. We only collect information from you that we believe we need in order to deliver and market our services to you, manage our relationship with you, and to fulfil our legal obligations. We do this in a variety of ways, including asking you for data about you and asking others to provide data about you (e.g. a super fund you invest in).

Any personal information we hold about you will be securely stored either in hard copy or on computer hard drive, using computer software and/or data storage facilities provided by third parties over the internet (i.e. not just on our computers in our offices).

Because we store some of our business data electronically and may back some or all of this data up using so-called "cloud-based" technology there is a chance that some of your personal information may be disclosed to overseas recipients in the sense that its transmission to and storage via the cloud will mean it may be "disclosed" to the party that operates the IT infrastructure where the data is stored or backed up. We only deal with reputable cloud providers who contractually agree to protect the privacy of your personal information.

We are unable to say with complete certainty which countries all cloud storage facilities may be located in however if this is of concern to you, we are happy to investigate and to advise. In any case, we believe we take reasonable steps to ensure that the standards in Australian privacy law are complied with.

We are also happy to provide you with a copy of this Privacy Policy free of charge upon request.

If you have any call to complain about our treatment of your personal information you can contact us or the Privacy regulator directly – they are accessible here: www.oaic.gov.au.

APP 2 - Anonymity

Although the Privacy Act makes provision for you to remain anonymous or use pseudonyms this is unlikely to occur in your dealings with Alere Private Wealth Pty Ltd as we have obligations under the Corporations Act and the Anti-Money Laundering and Counter-Terrorism Financing Act to know and identify our clients before we provide advice to them or transact on their behalf. You do not have to provide personal information to us. But note that we may not be able to provide our services if you do not provide information we need to collect.

APP 3 – Collection of Solicited Personal Information

As an Australian Financial Services Licence holder, we are subject to certain legislative and regulatory requirements which necessitate us obtaining and holding detailed information which personally identifies you and/or contains information or an opinion about you ("personal information").

In addition, our ability to provide you with a comprehensive financial planning and advice service is dependent on us obtaining certain personal information about you, including:

a) employment details and employment history;
b) details of your financial needs and objectives;

c) details of your current financial circumstances, including your assets and liabilities (both actual and potential), income, expenditure, insurance cover and superannuation;
d) details of your investment preferences and aversion or tolerance to risk;
e) information about your employment history, employment circumstances, family commitments and social security eligibility;
f) tax-related information;
g) personal or sensitive information.

Failure to provide the personal information referred to above may expose you to higher risks in respect of the recommendations made to you and may affect the adequacy or appropriateness of advice we give to you.

We are required by various Acts and the rules and standards of various professional bodies to collect sufficient information to ensure appropriate advice can be given in respect of recommendations made to our clients. If you elect not to provide us with the personal information referred to above, we may elect to terminate our retainer with you if we believe we are unable to provide you with a complete service.

APP4 – Dealing with Unsolicited Personal Information

We will not collect any personal information about you except when you have knowingly provided that information to us or authorised a third party to provide that information to us.

If we determine that we have obtained unsolicited personal information from you (i.e. information we don't actually need in order to deliver our services to you) we will contact, you and return it or otherwise remove it from our records as soon as is practicable.

APP 5- Notification of the Collection of Personal Information

Generally, collection of your personal information will be affected in either face to face interviews, or over the telephone or internet. From time to time additional and/or updated personal information may be collected through one or more of those methods.

Where we collect information about you other than directly from you, we will advise you of this fact and provide any other information to you about that collection as is determined relevant in the circumstances and in line with the requirements of the APPs.

APP 6 – Use or Disclosure of Personal Information

We will not use or disclose Personal Information collected by us for any purpose other than:

a) the purposes for which it was provided or secondary related purposes (including marketing our services to you) in circumstances where you would reasonably expect such use or disclosure;
b) in the event that we propose to sell our business we may disclose your personal information to potential purchasers for the purpose of them conducting due diligence investigations. Any such disclosure will be made in confidence, and it will be a condition of that disclosure that no personal information will be used or disclosed by them. In the event that a sale of our business is effected, we may transfer your personal information to the purchaser of the business. As a client you will be advised of any such transfer; or
c) where you have consented to such disclosure; or
d) where the APPs authorise use or disclosure where required or authorised under law, in circumstances relating to public health and safety and in connection with certain operations by or on behalf of an enforcement body.

We will only disclose your personal information to third parties where required to deliver our services or meet legal obligations, including:

a) one of more of our agents or authorised representatives who will be the primary adviser you deal with;
b) Product issuers and financial institutions (e.g., banks, other credit providers or finance brokers, superannuation funds, insurers);
c) Platform providers and portfolio administration services;
d) AML/CTF service providers and product issuers for identity verification purposes;
e) Compliance consultants, auditors, accountants, and legal or professional advisers;
f) IT service providers, software platforms and other service providers used to support our business operations;
g) Regulatory bodies such as ASIC, AUSTRAC and the ATO where required by law.

We will take reasonable steps to ensure your information is handled in accordance with applicable privacy laws.

If we disclose your personal information to external contractors, we make it a condition of our agreement with each of our external contractors that they adopt and adhere to this privacy policy or equivalent standards so that you can have confidence that your information is to be maintained by any contractor to whom it is disclosed in accordance with this policy. If you have any concerns in this regard, you should contact us by any of the methods detailed below.

If we use or disclose your personal information for any purpose other than the primary purpose of its collection (or any secondary related purpose) we will advise you and seek your consent.

AAP 7 – Automated Decision-Making and Artificial Intelligence

How We Use Automated Systems and Artificial Intelligence

We may use automated systems, software tools and artificial intelligence technologies to assist us in providing financial services, managing regulatory obligations and improving our client services.

These technologies may be developed by us or provided by third-party technology providers and may include:

- client onboarding and identity verification systems;
- AML/CTF screening and fraud detection tools;
- client risk profiling and risk tolerance assessment tools;
- product and portfolio research systems;
- portfolio construction, asset allocation and rebalancing tools;
- financial modelling and strategy projection software;
- client relationship management and workflow systems;
- document review and drafting tools;
- generative artificial intelligence tools used to assist our staff in analysing information and preparing communications; and
- compliance monitoring and quality assurance systems.

Personal Information Used

These systems may use personal information including:

- identity and contact details;
- demographic information;
- financial information;
- investment objectives;
- risk profile information;
- superannuation and insurance information;
- information relating to your assets, liabilities, income and expenses;
- information collected during client interactions; and
- any other information you provide to us in connection with our services.

Decisions and Recommendations Supported by Automated Systems

Automated systems may be used to assist in:

- assessing client onboarding requirements;
- conducting identity verification and regulatory screening;
- identifying potential fraud, financial crime or cybersecurity risks;
- preparing financial projections and modelling outcomes;
- generating investment or insurance research;
- constructing or reviewing proposed portfolios;
- producing draft advice materials and client communications;
- identifying compliance issues or file review exceptions; and
- determining whether additional information may be required from you.

Human Oversight
Except where required by law or regulatory processes, we do not rely solely on automated systems to make personal financial advice decisions for clients.

Our advisers, authorised representatives and staff review and assess information generated by automated systems before making recommendations or taking action. Automated tools assist our personnel but do not replace professional judgment.

Use of Generative AI
We may use generative artificial intelligence technologies to assist with research, document preparation, drafting, summarisation and administrative functions.

Where generative AI is used:
- information may be processed by approved technology providers;
- we implement controls designed to protect confidential and personal information;
- outputs generated by AI are reviewed by appropriately authorised personnel before being relied upon; and
- AI-generated outputs are not treated as final advice without human review.

Your Rights
You may contact us to:
- request further information about our use of automated systems;
- seek access to personal information used by such systems;
- request correction of personal information; and
- raise concerns regarding decisions or recommendations that have been informed by automated processing.

APP 8 – Direct Marketing

We may use your personal information to market our services to you. Of course, if you do not wish to receive marketing communications from us you can opt out. E.g. If our marketing is via email, it will have an unsubscribe button or link.

APP 9 – Cross-Border Disclosure of Personal Information

As licensee, the only overseas recipient of your personal information we can currently imagine is the party that hosts any IT infrastructure that we back up our business data to – e.g. via the so-called “cloud”. We will seek confirmation from any such service provider that they will treat your data securely and in alignment with the APPs. We deal only with large, reputable cloud providers and will always have a legal agreement in place that covers their commitment to privacy standards If we form the view that they are not able to treat client personal information in this way we will seek an alternative service provider.

However, it is important to note that some of the authorised representatives that operate under Alere Private Wealth Pty Ltd AFSL may outsource some tasks related to their services to outsourced providers located overseas, which may involve disclosing your personal information. If this is the case, the relevant authorised representative is required to let you know in their privacy policy the types of services that they may outsource overseas and the countries they may be outsourced to. Typically, such services could be paraplanning or back-office administration related. Such outsourced providers are typically located in India or southeast Asian countries such as the Philippines or Vietnam.

As licensee, we require any overseas outsourced arrangements to be documented in a legal agreement where the provider must agree to meet privacy standards equivalent to Australia's requirements. The outsourced providers must continuously provide proof of the adequacy of their arrangements, and we (or our authorised representatives) are required to monitor these arrangements.

It is important to note that governments and other authorities in overseas countries may have legal rights to access personal information held by entities regulated in their jurisdiction that go beyond the access rights equivalent government agencies and authorities in Australia may have. If you do not want your information to be disclosed overseas, please let the financial planning practice you are dealing with know.

APP 10 – Adoption, Use or Disclosure of Identifiers

We identify our clients via identifiers created on our electronic database. We do not identify clients using numbers that have been assigned to them by:

(a) a government agency; or
(b) an agent of an agency acting in its capacity as agent; or
(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

It is not our practice to use or disclose such third-party identifiers, unless:

a. the use or disclosure is necessary for the us to fulfil our obligations to the agency; or
b. we reasonably believe that the use or disclosure is necessary to lessen or prevent:
   (i) a serious and imminent threat to an individual's life, health or safety; or
   (ii) a serious threat to public health or public safety; or
c. we have reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
d. the use or disclosure is required or authorised by or under law; or
e. we reasonably believe that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
   (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
   (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
   (iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

f. the use or disclosures by a prescribed organisation of a prescribed identifier in prescribed circumstances.

APP 11 – Quality of Personal Information

We will take reasonable steps to ensure the personal information we collect is accurate, up-to-date and complete. This may include asking you to verify and/or update information you provide to us.

APP 12 – Security of Personal Information

We will at all times seek to ensure that the personal information collected and held by us is protected from misuse, loss, unauthorised access, modification or disclosure. At all times your personal information is treated as confidential and any sensitive information is treated as highly confidential. We have comprehensive policies and procedures to help ensure that personal information is kept confidential and secure at all times. Measures include utilising multi-factor authentication where relevant, using complex passwords to protect documents, limiting access to only those personnel who 'need to know', regularly patching and updating software, physical security measures, and a lot more. Data is regularly backed up.

In the event you cease to be a client of this organisation, any personal information which we hold about you will be maintained in a secure off site storage facility for a period of 7 years in order to comply with legislative and professional requirements, following which time the information will be destroyed.

APP 13 – Access to Personal Information

You may at any time, by contacting us by any of the methods detailed below, request access to your personal information and we will (subject to the following exceptions) provide you with access to that information either by providing you with copies of the information requested, allowing you to inspect the information requested or providing you with an accurate summary of the information held. We will, prior to providing access in accordance with this policy, require you to provide evidence of your identity.

We will not provide you with access to personal information which would reveal any confidential formulae or the details of any in-house evaluative decision-making process but may instead provide you with the result of the formulae or process or an explanation of that result.

We will not provide you with access to your personal information if:

a) providing access would pose a serious threat to the life, health or safety of a person, or to public health or public safety; or
b) providing access would have an unreasonable impact on the privacy of others; or

c) the request for access is in our reasonable view frivolous or vexatious; or
d) the information related to existing or anticipated legal proceedings between us and would not be discoverable in those proceedings; or
e) providing access would reveal our intentions in relation to negotiations with you in such a way as to prejudice those negotiations; or
f) providing access would be unlawful; or
g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or
h) both of the following apply:
   (i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;
   (ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
i) providing access would be likely to prejudice certain operations by or on behalf of an enforcement body; or
j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

In the event we refuse you access to your personal information, we will provide you with an explanation for that refusal and the mechanisms available to complain about our refusal.

APP 14 – Correction of Personal Information

We will endeavor to ensure that, at all times, the personal information about you which we hold is up to date and accurate. In the event that you become aware, or believe, that any Personal Information which we hold about you is inaccurate, incomplete or outdated, you may contact us by any of the methods detailed below and provide to us evidence of the inaccuracy or incompleteness or outdatedness and we will, if we agree that the information requires correcting, take all reasonable steps to correct the information.

If we do not agree that your personal information requires correcting, we must, if you request, take reasonable steps to ensure that whenever your personal information is accessed or handled in the future, it is apparent that you are not satisfied as to the accuracy or completeness of that information.

We will endeavor to respond to any request for access within 14-30 days depending on the complexity of the information and/or the request. If your request is urgent, please indicate this clearly.

Contacting Us

If you wish to complain about any breach or potential breach of this privacy policy or the Australian Privacy Principles, you should contact us by any of the methods detailed below and request that your complaint be directed to the Privacy Officer. Your complaint will be considered within 7 days and responded to. It is our intention to use our best endeavors to resolve any complaint to your satisfaction, however, if you are unhappy with our response, you are entitled to contact the Office of the Privacy

Commissioner who may investigate your complaint further.

Contact Details

Privacy Officer: Michael Patman

Alere Private Wealth Pty Ltd

PO Box 12931, George Street

Post Office QLD 4003

Email:
info@alereprivatewealth.com.au

Telephone 07 3188 5290