Privacy Policy

Valentia Capital Pty Ltd

ABN 42 683 192 494 | AFSL 569170

Essense Wealth Solutions Pty Ltd

T/A Essense Wealth Solutions (EWS)

ABN 60 658 170 417 | CAR 1296349

1. Overview

The collection of personal information about individuals by organisations is governed by the Privacy Act 1988 (Cth) (Privacy Act), which contains a national scheme for the collection, use, correction, disclosure, transfer and security of personal information by organisations in the private sector.

The Privacy Act has recently been significantly amended by the Privacy and Other Legislation Amendment Act 2024 (Cth) (the 2024 Amending Act). The 2024 Amending Act introduces stronger enforcement powers for the Office of the Australian Information Commissioner (OAIC), expanded data breach notification obligations, a statutory tort for serious invasions of privacy, new criminal offences for doxxing, strengthened technical and organisational security requirements under Australian Privacy Principle (APP) 11, and (from 10 December 2026) new transparency requirements for automated decision-making (ADM) under APP 1.7 to APP 1.9.

Protecting our clients' privacy is very important to us. As part of our commitment to ensuring the safety of our clients' personal and confidential information, and as a mechanism to ensure our compliance with the Privacy Act and the Australian Privacy Principles (APPs), we have established and implemented this Privacy Policy (the Policy).

1.1 Purpose

The Policy explains our policies and practices with respect to the collection, holding, use, disclosure, correction and security of the personal information we collect from you, and the steps we take to comply with the APPs.

The Privacy Act requires us to handle your personal information in accordance with the APPs. Those Principles and our approach to those Principles are set out below.

1.2 Scope

The Policy applies to Valentia Capital Pty Ltd (ABN 42 683 192 494; AFSL 569170) and Essense Wealth Solutions Pty Ltd (EWS; ABN 60 658 170 417; Corporate Authorised Representative 1296349), each in relation to personal information it handles. EWS provides financial services as a corporate authorised representative of Valentia Capital. In this Policy, "we", "us" and "our" refer to the relevant entity or both entities where the context requires. Each remains responsible for its applicable privacy obligations.

2. Collection of personal information

2.1 What information do we collect?

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

- providing financial advisory services to you
- providing recommendations in relation to investment, insurance, superannuation and credit products
- investing in, managing and administering investment products and services on your behalf
- meeting our regulatory, compliance and record-keeping obligations under the Corporations Act 2001 (Cth), the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act), the Tax Agent Services Act 2009 (Cth) and other applicable laws
- letting you know about our other products and services.

The type of information we collect from you includes information that is necessary to operate your investment accounts, assess your financial circumstances or provide advice to you. We may ask you to provide personal information such as your:

- name
- email address
- residential and/or postal address
- date of birth
- contact details
- occupation and employer
- bank account and payment details
- financial details, including income, expenses, assets and liabilities
- tax file number (TFN)
- identity verification information (such as driver's licence, passport or Medicare details).

Much of this information is collected through application forms, fact-find documents, the use of our online portals and digital channels, or through ongoing communications with you. We will not collect any personal information about you except where you have knowingly provided that information to us, or where we reasonably believe you have authorised a third party to provide that information to us.

In addition to the personal information, you provide to us or that we collect from third parties, we may generate or derive further information about you through our systems and processes. This may include inferred or derived information such as risk scores, suitability ratings, affordability indicators, behavioural or transaction-pattern insights, fraud and AML risk flags, and other outputs generated by analytical, statistical or automated tools. Where this information identifies you or could reasonably identify you, we treat it as personal information and manage it in accordance with this Policy and the APPs.

2.2 Sensitive information

There are specific circumstances in which we may ask for your sensitive information, such as:

- personal health information from you when applying for insurance
- personal health information from medical practitioners when you are making an insurance claim
- income information from employers where you are applying for additional insurance protection or salary continuance cover
- details of your dependants, as defined at section 10 of the Superannuation Industry (Supervision) Act 1993 (Cth), for the purposes of paying benefits in the event of your death
- biometric information used for identity verification (for example, facial-match data) where you choose to verify your identity digitally.

We seek your consent where required before collecting sensitive information, except where collection is required or authorised by law.

2.3 Collection from third parties

We may also need to collect personal information about you from third parties. For example, we may collect information from your accountant, lawyer, employer, product issuer, insurer, credit reporting body, broker, referrer or aggregator. Where we collect personal information about you from a third party, we will take reasonable steps to make you aware of that collection as required by APP 5.

We are also required to collect certain information by law. Wherever there is a legal requirement for us to collect information about you, we will inform you of the obligation and the consequences of not providing the requested information. For example, in addition to obtaining personal information from you, whenever you acquire a new product or service from us, we will need to obtain certain documentary evidence as to your identity (such as a certified copy of your driver's licence, passport or birth certificate) in order to satisfy our customer identification obligations under the AML/CTF Act.

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

You are not required to give us the information that we request. However, if you do not provide the information we ask for, or the information you provide is incomplete or inaccurate, this may:

- prevent or limit the quality of advice we provide to you
- prevent or delay the processing of an application or claim
- affect your eligibility for specified insurance cover
- prevent us from contacting you
- impact the taxation treatment of your account
- prevent us from satisfying our obligations under the AML/CTF Act, in which case we may be required to refuse to provide, or to suspend, our services to you.

For example, we are required to ask for your TFN when you invest in a superannuation product. If you choose not to provide your TFN, you may be subject to higher tax charges on your superannuation and the fund may not be able to accept personal contributions.

3. Use of personal information

3.1 How do we use the information we collect?

We use your personal information for the primary purposes for which it was collected, and for related secondary purposes that you would reasonably expect. This includes:

- providing financial advice to you
- establishing and managing your investments and accounts
- implementing your investment instructions
- establishing and maintaining insurance protection
- processing contributions, transferring monies or paying benefits
- reporting the investment performance of your account
- conducting credit, suitability or affordability assessments
- verifying your identity and detecting and preventing fraud and financial crime
- complying with our legal, regulatory and risk-management obligations

- training our staff and improving our products, services and client experience
- keeping you up to date on other suitable products and services offered by us.

Personal information will also be used where you have consented to such use, where it is required or authorised by or under an Australian law or court/tribunal order, in circumstances relating to public health and safety, or in connection with certain operations by or on behalf of an enforcement body.

4. Disclosure of personal information

4.1 Who do we give information to?

Valentia Capital and EWS may share client information with each other as necessary for authorised financial advice, compliance supervision, administration and client servicing. EWS personnel in the Philippines may access information through authorised systems for these purposes.
We may provide your personal information to external parties. Where personal information is disclosed, we take reasonable steps so that information is held, used and disclosed in accordance with the APPs and this Policy.

Depending on the service, the types of recipients to whom we may disclose personal information include:

- any organisations involved in providing, managing or administering investment products or services, such as actuaries, custodians, external dispute resolution services, insurers, investment managers, fund administrators, platform providers or mail houses
- your employer (in relation to employer-sponsored superannuation arrangements)
- any fund (administrator or trustee) to which your benefit is to be transferred or rolled over
- medical practitioners and other relevant professionals where you have applied for insurance cover or made a claim
- your personal representative, or any other person entitled to receive your death benefit, or any person contacted to assist us to process that benefit
- any financial institution that holds an account for you
- any professional advisers appointed by Valentia Capital, including legal, accounting and compliance advisers
- credit reporting bodies, identity verification service providers and AML/CTF reporting entities
- businesses that have referred you to us (for example, your lawyer or accountant)
- third-party service providers and offshore providers (see section 7)
- regulators and government agencies, including ASIC, AUSTRAC, the Australian Taxation Office (ATO), APRA and the OAIC.

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

- required by law (such as to the ATO, AUSTRAC or under a subpoena or court order)
- authorised by law (such as where we are obliged to disclose information in the public interest or to protect our interests)
- necessary in discharging obligations (such as to foreign governments for the purposes of foreign taxation reporting, including FATCA and CRS)
- required to assist in law enforcement (such as to a police force or enforcement body).

We will also disclose your information where you have provided your consent.

4.2 Will my information be disclosed overseas?

From time to time, we may disclose your personal information to recipients located outside Australia -for example, when we use cloud-based platforms, IT support, paraplanning, marketing, document storage or contact-centre services that are hosted or operated overseas. Where this occurs, we take reasonable steps to ensure that the overseas recipient handles your personal information in a manner consistent with the APPs, including by using enforceable contractual obligations under APP 8.

You should also be aware that some of our overseas service providers (including major cloud, software-as-a-service, customer-relationship-management and AI vendors) may engage related entities, group companies or downstream sub-processors located in additional jurisdictions to support the delivery of their services. Where we engage such providers, we take reasonable steps to ensure that they impose APP-aligned obligations on their sub-processors and that personal information is protected throughout the supply chain.

5. Access to, and correction of, personal information

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

You may request access to the personal information we hold about you at any time by contacting our Privacy Officer (see section 11). We will respond to your request within a reasonable period and will provide you with access in the manner you request, where it is reasonable and practicable for us to do so.

There may be circumstances where we are unable, or are not required, to give you access to the information you have requested -for example, where giving access would have an unreasonable impact on the privacy of others, or would be unlawful. If this is the case, we will inform you in writing and explain the reasons why and explain how you can complain about the refusal.

You have a right to ask us to correct any information we hold about you if you believe it is inaccurate, out of date, incomplete, irrelevant or misleading. If we agree that the information is incorrect, we will correct it and, where required, notify any third party to whom we have disclosed the information of the correction. If we do not agree, we will provide you with reasons in writing and you may request that a statement be associated with the record noting that you disagree with the information.

Where reasonable and practicable, we do not charge a fee for access or correction requests.

6. Automated decision-making

From 10 December 2026, additional APP 1 privacy-policy transparency obligations apply to certain decisions made by computer programs, including decisions substantially and directly informed by automated processing of personal information that could significantly affect individuals. We assess our actual processes against those requirements.

6.1 What is automated decision-making?

Computer-assisted decision processes may include systems that calculate, compare, score or model information to support a person making a decision. Human involvement does not, by itself, determine whether the additional transparency obligations apply.

6.2 When do we use ADM?

We use software for research, financial modelling, product comparisons, risk profiling and preparation of financial advice. These tools support advisers, who assess outputs and make and approve recommendations. Our processes do not independently approve or implement financial advice without adviser involvement. Depending on the workflow, the software may process information such as:

6.3 What personal information is used?

Depending on the decision, the types of personal information used by our automated systems may include identity and authentication data, contact details, income and expense data, transaction history, repayment history, credit reporting information (including comprehensive credit reporting data), behavioural data and risk-model inputs and outputs.

6.4 How does this affect you?

Decisions made or substantially supported by ADM may significantly affect your rights or interests -for example, decisions to approve, decline, price or set conditions on a product or service. In relation to such decisions, we will:

- explain, in plain language and consistent with APP 1.7 to APP 1.9, how ADM is used and the kinds of personal information involved
- apply human oversight to ADM processes in accordance with our internal governance arrangements
- on request and where reasonably practicable, provide further information about how an automated decision was reached and the key factors used
- where appropriate and reasonably practicable, allow individuals to seek review of decisions involving significant automated processing
- comply with any applicable obligations under Australian law in relation to automated processing.

For the purposes of this Policy, "human oversight" may include (depending on the decision in question) periodic review of decision parameters and model performance, manual review of selected decisions, exception handling, escalation processes, and the right of authorised personnel to override or adjust automated outcomes. The form and extent of human oversight is determined by the nature, sensitivity and impact of the decision concerned.

We review relevant software-assisted workflows as part of our privacy and advice governance and update our disclosures where a process falls within applicable automated-decision transparency requirements.

7. Use of AI, third-party providers and offshore providers

7.1 Use of artificial intelligence (AI)

Valentia Capital and EWS use AI-assisted tools to support administration, document organisation, research, drafting, summarisation, data analysis, financial modelling and advice preparation. AI outputs are support material; authorised advisers assess and approve client recommendations and advice.

Personal information may be processed using approved technology and AI-assisted services for the purposes described in this Policy. Staff are expected to follow applicable confidentiality, access and information-security requirements when using these services.

We do not describe client information as being used for general-purpose AI model training unless this is confirmed for the relevant service. If a proposed use of client information for AI training is materially different from the original purpose of collection, we will assess whether consent or another lawful basis is required before proceeding.

AI in decision-making. We do not rely solely on AI for decisions that could significantly affect you (see section 6). Where AI is used to support decision-making, human oversight is applied in accordance with the governance arrangements described in section 6.4. We will comply with any applicable obligations under Australian law relating to automated processing.

If we use recording, transcription or AI meeting-note services, we will address applicable consent and recording-law requirements and handle resulting recordings and notes as client information.

We review our AI-assisted processes and will update this Policy if their use of personal information or their role in decisions materially changes.

7.2 Use of third-party service providers

We work with external service providers (for example, paraplanning, IT and cyber-security support, cloud and software-as-a-service vendors, marketing, customer support, archiving, mailing houses and identity-verification providers) to help deliver our services. We share only the personal information that is reasonably necessary for the relevant task and require providers to use it solely for the agreed purpose.

We take reasonable steps to assess and manage privacy and information-security risks arising from third-party service providers. Measures may include:

- contractual obligations regarding confidentiality, security, breach notification and APP compliance

Records generated by our providers (such as paraplanning reports) are treated as part of your client file and retained securely in accordance with section 8 and our record-retention policies.

7.3 Use of offshore providers

EWS directly employs staff based in the Philippines who may access client personal and sensitive information to provide advice administration and client services. These employees are not employees of Valentia Capital. Valentia Capital and EWS take reasonable steps to manage offshore access and applicable privacy obligations, including staff confidentiality arrangements and access controls. Other service providers may process information outside Australia, depending on their service and configuration.

If you have concerns about overseas access to your information, please contact the Privacy Officers. We will explain available options where practicable; some services may depend on particular support and technology arrangements.

8. Complaints

If you believe that we have mishandled your personal information or otherwise breached the APPs or this Policy, you may lodge a complaint with us. The complaint, addressed to the Privacy Officer, should be in writing and should set out the details of your concern. Refer to section 11 for contact details for our Privacy Officer.

From receipt of your written complaint, our Privacy Officer aims to acknowledge your complaint within 5 business days and to provide a substantive response within 30 days, in line with the Privacy Act and the timeframes that apply to financial services complaints handling.

In the event that the Privacy Officer is unable to resolve your complaint to your satisfaction, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC). You can lodge a written complaint with the OAIC by:

- submitting an online form through the OAIC website at www.oaic.gov.au

- emailing the OAIC at enquiries@oaic.gov.au
- calling the OAIC on 1300 363 992 (within Australia) or +61 2 9284 9749 (outside Australia)
- writing to the OAIC at GPO Box 5288, Sydney NSW 2001.

Where your complaint relates to the financial services we provide, you may also be entitled to lodge a complaint with the Australian Financial Complaints Authority (AFCA) at www.afca.org.au or on 1800 931 678.

9. Protection of the personal and sensitive information we hold

9.1 How do we protect the security of your information?

Valentia Capital and EWS take reasonable technical and organisational steps to protect personal information against misuse, interference, loss and unauthorised access, modification or disclosure, having regard to the nature of the information and relevant systems.

Our security and data-governance measures include, among others:

- strong, role-based access controls and multi-factor authentication for systems holding sensitive data

9.2 Data breaches

We assess suspected data breaches and respond in accordance with applicable law, including the Notifiable Data Breaches scheme where an eligible data breach occurs. Relevant incidents are escalated between EWS and Valentia Capital as appropriate.

9.3 Risks of using the internet

You should note that there are inherent security risks in transmitting information through the internet. You should assess these potential risks when deciding whether to use online services. If you do not wish to transmit information via email or through our website, you may provide information to us by other means, such as by post or by speaking to your adviser by phone.

9.4 Doxxing and serious invasions of privacy

We do not tolerate the misuse or unlawful publication of personal information by personnel or representatives.

9.5 Cookies and online tracking technologies

Our websites and online services may use cookies and similar technologies for security, authentication, performance and analytics. The technologies actually used may differ between websites.

Cookies and similar technologies may support website functionality, security, usage analytics and, where implemented, marketing. You can adjust cookie settings through your browser or applicable website controls.

Where the law requires us to do so, we will obtain your consent before using non-essential cookies or other tracking technologies, and we will provide a mechanism for you to manage your preferences. Most browsers and mobile devices also allow you to manage cookies and tracking identifiers through their settings. If you elect to disable or limit these technologies, certain features of our digital services may not function as intended.

10. General

10.1 How long do we retain your personal information?

We are required by law to retain certain records of information for varying lengths of time. The applicable retention period depends on the type of information and the context in which it was collected. By way of example, and without limitation, we are subject to record-keeping obligations under the following:

- the Corporations Act 2001 (Cth), including the financial services record-keeping obligations applying to AFSL holders (for example, the seven-year retention period for records relating to the provision of financial services under section 912G and related ASIC regulatory guidance, including RG 104 and RG 105)
- the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and the AML/CTF Rules, which generally require customer identification, transaction and AML/CTF programme records to be retained for at least seven years
- the Superannuation Industry (Supervision) Act 1993 (Cth) and the SIS Regulations, where applicable, including trustee record-keeping obligations
- the Income Tax Assessment Act 1936 (Cth), the Income Tax Assessment Act 1997 (Cth) and the Tax Administration Act 1953 (Cth), which impose record-keeping obligations relating to taxation
- the Insurance Contracts Act 1984 (Cth) and other insurance-related legislation, where relevant to claims handling and underwriting
- any applicable obligations imposed by ASIC, AUSTRAC, APRA, the ATO or other regulators.

Some records (such as those relating to financial advice, insurance claims and trustee functions) may be retained for periods of seven years or longer, and certain records may be retained permanently where the law so requires.

Where your personal information is no longer required to be retained under law and is no longer needed for the purpose for which it was collected (or a related purpose for which it may lawfully be used), we will take reasonable steps to permanently de-identify or destroy that information in a secure manner.

As part of our data-minimisation practices, we periodically review the data we hold and decommission information that is no longer required, in order to reduce regulatory, security and privacy risk.

10.2 Children's data

Our financial services and digital channels are not generally directed at children under 18. We nonetheless recognise that, even where a product or service is not intended for minors, incidental access by children can occur -for example, through shared devices, the embedding of digital financial services in social media or e-commerce environments, or the entry of personal information during onboarding. We periodically assess whether our websites, applications and other digital channels are likely to be accessed by children, and apply additional safeguards where that is the case.

Where we collect information about children, such as dependants and beneficiaries, we handle it for legitimate advice, insurance, superannuation and related purposes and apply appropriate privacy safeguards.

10.3 Review and updates to this Policy

We review this Policy regularly and will update it from time to time to reflect changes to our business, our use of technology (including AI and ADM), and applicable law. The current version of this Policy is available on our website. Where we make material changes, we will take reasonable steps to bring those changes to your attention.

11. How do I contact the Privacy Officer?

If you have any questions about this Policy or about how we manage your personal information, or if you wish to make a request for access, correction or a complaint, please contact our Privacy Officer using the details below.

Privacy Officers
Mark Dela Cruz and Mina Nguyen

Valentia Capital Pty Ltd (AFSL 569170)
Valentia Capital email: info@valentiacapital.com.au

Essense Wealth Solutions Pty Ltd (CAR 1296349)
EWS email: hello@ews.com.au
EWS telephone: 1800 845 061
Web: www.ews.com.au