Overview:

OneVue Holdings Limited and its wholly owned subsidiaries OneVue RE Services Limited ABN 94 101 103 011 AFS Licence No 223271, OneVue Services Pty Ltd ABN 71 104 037 256, OneVue Fund Services Pty Ltd ABN 18 107 333 308, Diversa Trustees Limited ABN 49 006 421 638, AFSL No 235153, (together referred to in this Policy as "us", "our", or "we") are committed to protecting the privacy of all personal (and sensitive) information we collect.

As part of this commitment and as a mechanism to ensure compliance with the Privacy Act 1988 (Cth) (Privacy Act), we have developed and implemented a Privacy Policy (the Policy).

This Policy sets out our practices with respect to the collection and management of personal and sensitive information, and has been developed with regard to the Australian Privacy Principles (APPs) (established under the Privacy Act) which provides the standards, rights and obligations for the handling, holding, accessing and correction of personal (including sensitive) information.

What is personal information?

Personal information is defined in law as information or an opinion about an identified individual or an individual who is reasonably identifiable; whether the information or opinion is true or not and whether the information or opinion is recorded in material form or not. Examples include an individual's name, address, contact number and email address.

Special provisions apply to the collection of personal information which is sensitive information. Sensitive information includes, for example, information about a person's health, membership of a professional or trade association, further discussed below.

What personal information do we collect?

We will collect and hold your personal information for the purposes of providing products and services to you, managing and administering those products and services, and informing you of our other products and services.

The financial products and services provided by us include both direct to client services and services provided through financial advisers and fund managers.

The information we collect directly from clients, financial advisers, fund managers, and other AFS Licensees, includes name and contact information (including email address), residential and or postal address, date of birth, tax file number (TFN), occupation, employer, bank account details, financial information, data required for anti-money laundering counter-terrorism financing purposes; and any other information required to administer the products and services we provide (including information required by law). Much of this information is collected through application forms, the use of our online facilities or through ongoing communications with you.

There are also specific circumstances in which we will ask for your sensitive information. We will only collect sensitive information from an individual where the individual has consented to the collection and the information is reasonably necessary for us to administer your account.

The sensitive information we may collect includes:

- details of your dependents, (as defined in Superannuation Law) for the purposes of paying benefits in the event of your death;
- personal health information when you apply for insurance;
- personal health information from medical practitioners when you are making a claim;
- income information from employers in instances where you are applying for additional insurance protection or salary continuance insurance;
- marital status; and
- membership of professional associations and trade unions.

How do we collect and hold personal information?

When we collect personal information directly from an individual, we take reasonable steps at, or before the time of collection to ensure that the individual is aware of certain key matters, such as:

- the details of the entity collecting the personal information;
- the purposes for which we are collecting the information (including for example where required by law);
- the organisations (or types of organisations) to which we would normally disclose information of that kind;
- the main consequences if all or some of the personal information is not collected;
- the fact that an individual is able to access the information and how to contact us to either access or correct their personal information;
- the fact that an individual may complain about the handling of their personal information if they believe it is has not been done in accordance with the Privacy Act, and how the entity will deal with the complaint.

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

We will collect personal information directly from an individual where it is reasonable and practicable to do so. Where we collect information from a third party such as financial advisers, fund manager, or another AFS Licensee, we will still take reasonable steps to ensure that an individual is made aware of same key matters as set out above.

You are not required to give us the information that we request, however if you choose not to provide the information we ask for, or the information you give us is not complete or accurate, this may for example, prevent or delay the processing of your application or any claim, affect your eligibility for specified insurance cover, or it may prevent us from contacting you. It may also (in certain circumstances) impact on the taxation treatment of your account.

We take reasonable steps to ensure that the personal information that we collect, use and disclose is accurate, complete and up to date, by reviewing personal information provided as part of the application process against certified documentation to make sure it meets requirements before processing. We advise clients to keep their information up to date and provide mechanisms for them to do so.

We take reasonable steps to protect the personal information and sensitive information that we hold from misuse and loss and from unauthorised access, modification or disclosure by using security procedures and the latest technology. Account information is password and security question protected and instructions are verified before they are processed.

Your personal information is stored on secured third party servers in Sydney, and within our onsite servers located in our secured server rooms in our Brisbane, Sydney, Melbourne and Albury data centres. Data from onsite servers is backed up to tape and pushed over the network to the data centre. Backups within the data centre are stored in two separate physical locations within New South Wales.

Any personal information sent to external locations is secured with encryption. We may disclose personal information to the following:

- internally to our staff and related bodies corporate;
- professional advisers nominated by clients;
- financial institutions, where necessary, to allow us to establish accounts or other banking facilities on behalf of clients or investors;
- promoters;
- any financial institution which holds an account for you;
- any organisations or professional advisers involved in providing, managing or administering our products or services such as auditors, accountants, lawyers, custodians, external dispute resolution services, insurers, investment managers or mail houses, within normal business practices;
- 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;
- support services;
- any fund (administrator or trustee) to which your superannuation benefit is to be transferred or rolled over; and
- where otherwise required or authorised by law.

We will also disclose your personal information if you give us your consent.

If other organisations provide support services to us, they are required to appropriately safeguard the privacy of the personal information provided to them.

Where personal information collected is no longer needed for any purpose that is permitted by the Privacy Act, we will delete, securely destroy or permanently de-identify the personal information.

Use of Commonwealth government identifiers

We do not use Commonwealth government identifiers (Identifiers) as our own identifier of individuals. We will only use or disclose Identifiers in the circumstances permitted by the Privacy Act.

Purposes of collection

We will only collect personal information from an individual or third party which is reasonably necessary to provide our products or services (primary purpose). We collect personal information for the following primary purposes, including:

- processing applications and other transactions for products and services offered by us and our clients;
- providing information and communications to members and other account holders, necessary
- for the operation of products and services offered by us and our clients, or to comply with the requirements of the Corporations Act 2001 (Cth);
- to record and maintain member and investor details necessary for providing the services offered by us and our clients;
- establishing accounts or other banking facilities on an individual's behalf with third party financial institutions and administering an individual's accounts or other banking facilities;
- communicating with clients and investors, including for the purposes of direct marketing communications (where permitted by law);
- conducting our internal business operations, including meeting any relevant regulatory or legal requirements;
- as agent, collecting information to enable our clients to comply with Anti-Money Laundering and Counter-Terrorism Financing Law; and
- assessing applications for employment.

We will only collect sensitive information from an individual for the purpose of administering their account.

If we use or disclose personal information for direct marketing or a purpose other than the primary purpose (secondary purpose), to the extent required by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), we will ensure that:

- the individual has consented to the use or disclosure of their personal information for the secondary purpose; or
- the secondary purpose is directly related to the primacy purpose; and
- the individual would reasonably expect us to use or disclose the information for this secondary purpose.

Individuals can request not to receive direct marketing communications by following the opt-out method provided within the communication.

Personal (and/or sensitive) information may also be disclosed where for example it is required by law, or a permitted general or health situation exists in relation to the use or disclosure. This may include for example situations in which the entity reasonably believes that the disclosure of personal information is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or that of the public.

Accessing your personal information or making a complaint

Any individual about whom we hold personal information, can contact us to access and correct their personal information. We may charge a reasonable fee to cover our costs.

We will take all reasonable steps to provide access to or amend any personal information that is incorrect. If we are unable to correct your personal information, or give you access to the information, we will advise you with an explanation in writing.

If you believe that we have not dealt with your personal information in accordance with this Policy or the APPs, you may make a complaint to us.

You can contact us to either access or correct personal information, or complain about any breach of the APPs by writing to the Privacy Officer at:

Compliance Department

PO Box 1282

Albury NSW 2640

We will acknowledge your complaint in writing within 7 days of receipt, and process and respond to your complaint within 30 days. If we cannot resolve your complaint within 30 days of receipt, we will contact you with an explanation and ask permission for an extension of time.

If (after 30 days) you are not satisfied with our response, you can raise your concerns with the Office of the Australian Information Commissioner:

Online: www.oaic.gov.au
Phone: 1300 363 992
Email: enquiries@oaic.gov.au
Fax: +61 2 9284 9666
Mail: GPO Box 5218, Sydney NSW 2001 or GPO Box 2999, Canberra ACT 2601.

Disclosing personal information overseas

Some of our third party contractors and service providers may perform certain services overseas. As a result, personal information collected by us may be disclosed to a recipient in a foreign country. We outsource back office administrative services and anti-money laundering counter-terrorism financing screening services to providers who operate overseas. The countries in which such overseas recipients are likely to be located are the United Kingdom, United States, Canada, France, Singapore, the Netherlands, Switzerland and India.

We take reasonable steps to ensure these overseas recipients comply with the APPs by implementing contractual arrangements with overseas service providers to ensure the personal information is appropriately safeguarded and to ensure that these overseas service providers comply with the APPs.

Availability of our Privacy Policy

Our Privacy Policy is available free of charge on our public website.