

## PRIVACY POLICY

This Privacy Policy has been published to provide a clear and concise outline of how and when personal information is collected, disclosed, used, stored and otherwise handled by Natixis Australia Pty Limited (“we”, “us”, “our” or “NAPL”) registered with the Australian Securities & Investments Commission and holds an Australian Financial Services License (No. 317114).

We are committed to safeguarding the personal information that we receive in accordance with our own corporate values, as well as the standards required by the Australian Privacy Principles and the Privacy Act 1988 (Cth) (“Australian Privacy Act”).

Personal information that we collect about you will only be used for the purposes we have collected it or as allowed under the law.

### **What is personal information that we collect?**

#### - Personal information

We mean information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can be reasonably be ascertained, from the information or opinion. Personal information we may collect include, but is not limited to, names, contact details, gender, identification document information, employment details and history, shareholdings and other ownership arrangements, and criminal history information.

NAPL lawfully and fairly collects personal information that is reasonably necessary for its business to function. The information NAPL collects and holds will depend upon the services the client requests from NAPL.

You have the right not to provide us with your personal information, however, due to the nature of NAPL’s services and business, it is impracticable for NAPL to deal with clients who do not wish to identify themselves or who wish to use a pseudonym.

#### - Sensitive information

This is a subset of personal information and we mean information or an opinion that is also personal information about an individual (membership of a political association, memberships of professional or trade associations or trade unions, criminal record), health information about an individual, genetic information, biometric information to be used for the purpose of automated biometric verification or identification, or biometric templates.

For example, sensitive information may be collected during the recruitment process or as part of “know your client” checks.

We will not generally collect sensitive information, but if it is reasonably necessary to collect and record sensitive information, NAPL will obtain the individual’s specific consent. Sensitive information can also be collected when it is required or authorised by or under an Australian law or a court/tribunal order, or a permitted general situation exists in relation to the collection of the information by NAPL. NAPL will treat this information with a high degree of security and confidentiality.

### **Why we collect your personal information**

We may collect and use your personal information for any of the following purposes:

- deciding whether to provide services to you

**NATIXIS AUSTRALIA PTY LIMITED**

Level 26, 8 Chifley Square Sydney NSW 2000 - Phone: +61 2 8063 1700 - Fax: +61 2 8063 1733 - [www.natixis.com](http://www.natixis.com)  
ABN 51 122 500 690 – AFSL No.317114

- providing services to you
- identifying you
- considering an application for employment
- managing our relationship with you
- legal, regulatory, compliance or governance
- risk management or crime prevention
- operating and managing our business
- marketing, planning, product or service development
- research, analytics or business improvement

We may also collect, use and share your information for other reasons that the law allows or requires. If we need to disclose personal information to a third party, it will be done to the extent that it is permitted by law and in accordance with this policy.

### **How we collect your personal information?**

Where reasonable and practical we collect your personal information directly from you. We may collect information by way of face-to face meetings, completed forms, business cards, telephone conversations, applications, interview, emails, invitations and electronic interactions.

In some circumstances, we may collect personal information about you from a third party. Some examples of third-party sources include referees, your authorised representatives, publicly available records and registers.

We will notify you at or before the time or, if that is not practicable, as soon as practicable after we collect personal information from someone other than the client or individual, unless authorised or required by law or otherwise as permitted under the Privacy Act.

### **How we disclose your personal information?**

The information NAPL collects is used for the purpose disclosed at the time of collection of otherwise as set out in this privacy policy.

NAPL will not use your personal information for any other purposes without first seeking your consent, unless authorised or required by law or otherwise as permitted under the Privacy Act.

We may disclose your personal information to:

- share registries
- related entities and their officers, employees, agents and contractors
- entities that provide financial services eg stockbrokers, fund administrators, custodians and responsible entities
- other organisations that are involved in managing or administering our financial services
- other organisations such as third-party suppliers, printing and postal services
- our technology providers and administrators
- our service providers, including software as a service provider
- anyone, where you have provided your consent
- any person where we or our related entity is required to do so by law
- any person or entity considering acquiring an interest in our business or assets

When we disclose your personal information it may be to entities that are overseas including to our related entities in France, Singapore and Hong Kong and to our Software as a Service Providers in France and European Union.

Under the Privacy Act, we have the obligation to take such steps as are reasonable in the circumstances to ensure that the overseas entities do not breach the Australia Privacy Principles before disclosing the personal information. Such obligation does not apply when we expressly inform the individual of the cross-border disclosure of personal information and the individual still consents to the disclosure after being informed.

### **Updating your personal information**

It is important to us that the personal information we hold about you is accurate, complete and up to date.

Please let us know if any of your personal information changes or is incorrect. You can contact us via the contact details set out at the bottom of this Privacy Policy.

### **Access to and correction of your personal information**

You can contact us via the contact details at the end of this Privacy Policy to ask for access to personal information that we hold about you, or to correct that personal information. We will aim to respond within 30 days. We will ask you to verify your identity before we give you access to information or correct it.

There may be situations where we are not required to provide you with access to your personal information or to make a correction that you have requested. If we refuse to give you access to, or correct, your personal information, we will explain why.

We may charge a fee for our costs of retrieving and supplying information to you, depending on its location and volume. We will not charge you for making a request, for correcting your personal information, or for associating a statement with your information.

### **Storage and security of personal information**

NAPL will take all reasonable steps to protect the personal information it holds from misuse and loss from unauthorized access, modification and disclosure.

NAPL securely stores personal information in soft and hard folders with restricted access. We use a range of physical, electronic and other security measures to protect the confidentiality and integrity of the information that we hold. We may store personal information physically or electronically with third party data storage providers. Where we do this, we use contractual arrangements and other measures to ensure those providers protect that information from unauthorised access, use or disclosure.

As the internet is not a whole secure method of transmitting information, NAPL cannot accept responsibility for the security of information the individual or client sends to, or receive from NAPL over the Internet, or for any unauthorised access or use of that information.

We hold information for the period reasonably necessary to provide our services to you, and satisfy our legal, regulatory, compliance, governance, and business needs. We have a dedicated information security and risk management team and also maintain appropriate document storage and data security policies and controls.

### **Destruction of personal information**

If we no longer require your personal information for any of the purposes outlined in this policy, or if the information is unsolicited, and the information is not contained in a Commonwealth record and we are not required by or under an Australian law, or a court/tribunal order to retain the information, we will take reasonable steps to destroy it securely or to ensure that the information is de-identified.

### **Using government identifiers**

We will not adopt a government related identifier of a client as its own identifier of the client unless authorised or required by law or otherwise as permitted under the Privacy Act.

### **Marketing policy**

We may use or disclose personal information (other than sensitive information) for the purpose of direct marketing if and only we collected the information from you, and you reasonably expect us to use or disclose the information for that purpose.

You can unsubscribe from our marketing policy at any time. You can also contact us by emailing [australia.compliance@natixis.com](mailto:australia.compliance@natixis.com) if you prefer not to receive such information. We will not charge you for giving effect to your request.

### **Cookies**

Cookies are small blocks of data that are downloaded onto a visitor's device upon visiting a website. Any web server (including our web server) may from time to time:

- Store one or more cookies on your web browser;
- Request your browser to send data back to our web server; and/or
- Request your browser to send a cookie which has been stored on your web browser by another website in the same internet domain.

Our website may store cookies on your web browser to improve your use of our website the next time you visit. Cookies allow a website to track information about use and behavioral patterns on a website. We may use cookies to measure visitor use of our website, but we will not collect or store personal information about you.

### **Complaints**

If you are dissatisfied with how we have dealt with your personal information, or you have a complaint about our compliance with the Privacy Act, or you wish to request further information about how we handle personal information or any privacy issues, you can contact our Compliance Officer at the contact at the bottom of this Policy.

An individual complaint may be lodged by any reasonable means e.g. letter, telephone, e-mail. The team that receives the complaint must investigate and resolve it as soon as possible and in any event complaint needs to be written acknowledged within 24 hours (or one business day) of receipt, or as soon as practicable.

Within 30 business days of receiving a complaint, the team responsible for handling the investigation and resolution of the complaint should send the customer:

- A final response; or
- An explanation for not giving a final response, with reasons for the delay and an estimation of the date when a final response can be given.

A final response means a response which either accepts the complaint (and where appropriate offers redress), offers redress without accepting the complaint or rejects the complaint and gives reasons for doing so.

All reporting and investigation procedures involved in the complaint handling process should be conducted in such manner to protect the identity of customers. Information in relation to a complaint



must be treated as confidential and should be processed by the responsible officer(s) strictly on a need-to-know basis.

**Additional information and contact details**

We may review, revise, and amend our Privacy Policy from time to time including when our information handling practices change. Updates will be published on our website.

A copy of our current policy is available on our website at <https://apac.cib.natixis.com/australia>. Alternatively, if you want a copy of the Privacy Policy, you may contact the Compliance Officer.

If you are dissatisfied with how we have dealt with your personal information, or you have a complaint about our compliance with the Privacy Act, or you wish to request further information about how we handle personal information or any privacy issues, you can contact our Compliance Officer at:

**Post:**

Compliance Officer  
Natixis Australia Pty Ltd  
Level 26, 8 Chifley Square  
Sydney NSW 2000

**Telephone:**

+61 2 8063 1700

**Email:**

[australia.compliance@natixis.com](mailto:australia.compliance@natixis.com)

Last updated: 24.08.2023