Privacy Policy

Version 5.0 | Issued date 7 March 2023

Whittle & Skok Financial Services Pty Ltd (ABN 68 006 923 940 (referred to as Whittle & Skok, we, our, us) 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.

To the extent that it is necessary to do so, Whittle & Skok also complies with the requirements of the EU General Data Protection Regulation (GDPR) as adopted by EU Member States. The APPs and the GDPR Policy share many common requirements. Where an obligation imposed by the APPs and the GDPR are the same, but the terminology is different, Whittle & Skok will comply with the terminology and wording used in the APPs, and this will constitute Whittle & Skok's compliance with the equivalent obligations in the GDPR.

If the GDPR imposes an obligation on Whittle & Skok that is not imposed by the APPs, or the GDPR obligation is more onerous than the equivalent obligation in the APPs, Whittle & Skok will comply with the GDPR (see Annexure A).

All third parties (including clients, suppliers, sub-contractors, or agents) that have access to or use personal information collected and held by Whittle & Skok, must abide by this Privacy Policy and Collection Statement (Privacy Policy). Whittle & Skok makes this Privacy Policy available free of charge and can be downloaded from its website whittleskok.com.au.

In this Privacy Policy:

- ***Disclosure*** of information means providing information to persons outside of Whittle & Skok;
- ***Personal information*** means information or an opinion relating to an individual, which can be used to identify that individual;
- ***Privacy Officer*** means the contact person within Whittle & Skok for questions or complaints regarding Whittle & Skok's handling of personal information;
- ***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 Whittle & Skok.

What kind of personal information do we collect and hold?

We may collect and hold a range of personal information about you to provide you with our services, including:

- name, date of birth, address, phone numbers and email addresses;
- occupation, employer and employment arrangements;
- bank account, superannuation and pension account details;
- driver's licence, passport and other details that can be used to verify your identity;
- financial information, including details of:

- your assets and liabilities;
- income, expenses and taxation information;
- your insurance policies;
- social security benefits and entitlements;
- estate planning strategies; and
- health information, including Covid vaccination and check-in information in accordance with relevant health directions.

How do we collect personal information?

We generally collect personal information directly from you. For example, personal information will be collected through our application processes, forms and other interactions with you in the course of providing you with our products and services, including when you visit our website, use a mobile app from us, call us or send us correspondence.

We may also collect personal information about you from a third party, such as electronic verification services, referrers and marketing agencies. If so, we will take reasonable steps to ensure that you are made aware of this Privacy Policy. We may also use third parties to analyse traffic at our website, which may involve the use of cookies. Information collected through such analysis is anonymous.

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 do not give you the option of dealing with a third party anonymously, or under a pseudonym. This is because it is impractical, and, in some circumstances, illegal for Whittle & Skok to deal with individuals who are not identified.

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.

Website collection

We collect personal information when we receive completed online generated forms from our website www.whittleskok.com.au. We may also use third parties to analyse traffic at that website, which may involve the use of cookies. Information collected through such analysis is anonymous. You can view and access our Privacy Policy by clicking on the relevant link on our website.

To use our website, you must consent to our use of cookies. You can withdraw or modify your consent to our use of cookies at any time. If you no longer wish to receive cookies, you can use your web browser settings to accept, refuse and delete cookies. To do this, follow the instructions provided by your browser. Please note that if you set your browser to refuse cookies, you may not be able to use all of the features of our website.

Cookies do not contain personal information in themselves but can be used to identify a person when combined with other information. Cookies are small text files which are transferred to your computer's hard drive through your web browser that enable our website to recognise your browser, capture and remember certain information. This includes facilitating your use of certain elements within our website such as the client portal and web forms.

We also use cookies to understand how users interact with our website, to compile aggregate data about our website traffic, including where our website visitors are located, and interaction so that we can offer better user experiences.

From time to time, we will delete all data obtained through cookies.

We may also use analytics on the site. We do not pass any personally identifiable information through this function, however, the data we collect may be combined with other information which may be identifiable to you.

As we use website cookies, and are required to comply with the GDPR, we have a created a 'pop up' message on our website, which states:

"This website uses cookies for analytics and personalised content. By using this website, you agree to the use of cookies in accordance with our Privacy Policy."

Why do we collect and hold personal information?

We may use and disclose the information we collect about you for the following purposes:

- provide you with our products and services;
- review and meet your ongoing needs;
- provide you with information we believe may be relevant or of interest to you;
- let you know about other products or services we offer, send you information about special offers or invite you to events;
- consider any concerns or complaints you may have;
- comply with relevant laws, regulations and other legal obligations;
- help us improve the products and services offered to our customers and enhance our overall business; and/or
- a financial planner may collect and hold personal information to assist in providing wealth management, financial planning, personal risk advice and stockbroking services.

We may use and disclose your personal information for any of these 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.

Who might we disclose personal information to?

We may disclose personal information to:

- a related entity of Whittle & Skok;
- an agent, contractor or service provider we engage to carry out our functions and activities, such as our lawyers, accountants, debt collectors or other advisers;
- organisations involved in a transfer or 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;
- regulatory bodies, government agencies, law enforcement bodies and courts;
- financial product issuers; and
- anyone else to whom you authorise us to disclose it or is required by law; and

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.

Sending information overseas

We may disclose personal information to related entities, product providers and suppliers that are located outside Australia in some circumstances. It is not practical to list all of the countries in which personal information is likely to be disclosed, however, they are likely to include:

- New Zealand
- United States of America
- United Kingdom
- Member states of the European Union (EU)

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.

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.

Your personal information is generally stored in our computer database. Any paper files are stored in secure areas. In relation to information that is held on our computer database, 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;
- all computers which contain personal information are secured both physically and electronically;
- data is encrypted during transmission over the network; and
- print reporting of data containing personal information is limited.

Where our employees work remotely or from home, we implement the following additional security measures:

- two-factor authentication is enabled for all remote working arrangements;
- password complexity is enforced, and employees are required to change their password at regular intervals;
- 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 use audit trails and audit logs to track access to an individual's personal information by an employee;
- we monitor access to personal information, and will investigate and take appropriate action if any instances of unauthorised access by employees are detected;
- employees must ensure that screens are angled so that they cannot be used by anyone else, and are locked when not in use;
- employees 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.

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.

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 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.

Accessing your 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 Whittle & Skok's Privacy Officer. 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 require identity verification and specification of what information is required. An administrative fee for search and photocopying costs may be charged for providing access.

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.

Responsibilities

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.

Incidents, Complaints handling & making a complaint

We have an effective complaints handling and dispute resolution process in place to manage privacy risks and issues. Please refer to our Public Disputes Resolution Policy for further details, available on our website www.whittleskok.com.au.

The complaints handling process involves:

- identifying (and addressing) any systemic and/or 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 Privacy Officer.

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:

- calling - (03) 9261 8100
- emailing - ClientServices@whittleskok.com.au
- writing - Privacy Officer
  Level 1, 260 High Street
  KEW VIC 3101

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:

- calling - 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

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.

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.