

Privacy Policy and Collection Statement (Privacy Policy)

Privacy Policy and Collection Statement

(Privacy Policy)

1. Introduction

Aureus Funds Investment Management Pty Ltd and A.C.N. 677 255 131 (referred to as **Aureus Funds, we, our, us**) is bound by the *Privacy Act 1988* ('the 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, Aureus Funds also complies with the requirements of the EU General Data Protection Regulation ('GDPR') as adopted by EU Member States.¹ 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, Aureus Funds will comply with the terminology and wording used in the APPs, and this will constitute Aureus Funds' compliance with the equivalent obligations in the GDPR.

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

All third parties (including clients, suppliers, sub-contractors, or agents) that have access to or use personal information collected and held by Aureus Funds, must abide by this Privacy Policy and Collection Statement ('Privacy Policy'). Aureus Funds makes this Privacy Policy available free of charge and can be downloaded from its website www.AureusFunds.com.au.²

In this Privacy Policy:

- **Disclosure** of information means providing information to persons outside of Aureus Funds.
- **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 Aureus Funds for questions or complaints regarding Aureus Funds' 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.
- **Use** of information means use of information within Aureus Funds.

2. 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;
- address;
- phone numbers;
- email addresses;
- occupation;

- bank account details;
- driver's licence details;
- financial information, including details of:
 - your investments;
 - your insurance policies;
 - estate planning strategies;
 - taxation information; and
 - health information;
- Covid check-in information in accordance with current health directions.

3. 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 them anonymously, or under a pseudonym. This is because it is impractical, and, in some circumstances, illegal for Aureus Funds to deal with individuals who are not identified.

4. 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.

5. 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.

6. Website collection

We collect personal information when we receive completed online generated forms from our website www.AureusFunds.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 privacy button 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 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 enables our website to recognise your browser and capture and remember certain information.

We 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 created a 'pop up' message on our website, which states:

7. 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;

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.

8. Who might we disclose personal information to?

We may disclose personal information to:

- a related entity of Aureus Funds;
- 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;
- 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.

9. Sending information overseas

We do not disclose personal information overseas.

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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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 Aureus Funds' 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.

15. 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.

16. 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.

17. 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.

18. Incidents / Complaints handling / Making a complaint

We have an effective complaint handling process in place to manage privacy risks and issues.

The complaints handling process involves:

- identifying (and addressing) any systemic/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:

- writing – PO BOX 210, Jimboomba, QLD, 4280
- emailing – Phillip.Dwyer@AureusFunds.com.au

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:

- telephoning – 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

19. 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.

20. 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.

Annexure A: GDPR

The following are key terms used in the GDPR which are not used in the APPs:

Controller means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. *(This is an APP entity under the Privacy Act).*

Data Subject means an identified or Identifiable Natural Person. *(This is an individual under the Privacy Act.)*

Identifiable Natural Person means one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *(This is an individual under the Privacy Act.)*

Personal data means any information relating to a Data Subject. *(This is similar to personal information under the Privacy Act.)*

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptations or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. *(There is no single concept in the Privacy Act that is equivalent. The Privacy Act uses concepts of 'collection', 'use' and 'disclosure'.)*

Processor means a natural or legal person, or other body which processes personal data on behalf of the controller. *(There is no direct equivalent concept in the Privacy Act other than references to 'third parties' who deal with personal information on behalf of or for an APP entity.)*

Item no	Obligation	Australian Privacy Act requirement	Aureus Funds will comply with the GDPR requirement
1	Use or disclosure of personal information/data for secondary purpose	Aureus Funds may use personal information for a secondary purpose if the individual has consented, it is within their reasonable expectations, or another exception applies.	Aureus Funds will only process personal data where the data subject has consented to one or more of the specific purposes of the processing, or another listed scenario applies. For example, where the processing is necessary to perform a contract or comply with a legal obligation.
2	Collection of solicited personal information/data	Aureus Funds will only collect personal information where it is reasonably necessary or when it is directly related to Aureus Funds' functions or activities, and by lawful and fair means. Sensitive information will only be collected with consent, or where a listed exemption applies.	Aureus Funds will only collect personal data for the specified explicit and legitimate purposes described, and all personal data will be processed lawfully and fairly.
3	Notification of collection of	Aureus Funds' Privacy Collection Notice is drafted	Aureus Funds provides the following additional information to EU citizens:

Item no	Obligation	Australian Privacy Act requirement	Aureus Funds will comply with the GDPR requirement
	personal information/data	in accordance with the APP requirements.	<ul style="list-style-type: none"> The contact details of our data protection officer are <i>[insert contact details if you are required to have a data protection officer under GDPR requirements]</i> Where Aureus Funds is collecting information only for Aureus Funds' own legitimate interests, those interests are: <i>[insert your legitimate interests if this applies to you]</i> Aureus Funds will store personal data for <i>[insert period]</i> OR # will store personal data for a period that <i>[insert criteria for determining the period]</i>
4	Direct marketing	<p>Aureus Funds will comply with the 'Direct marketing' section of this Privacy Policy.</p> <p>Aureus Funds may only use or disclose personal information for direct marketing purposes if certain conditions are met. In particular, direct marketing messages must include a clear and simple way to opt out of receiving future messages, and must not be sent to individuals who have already opted out. Sensitive information about an individual may only be used for direct marketing with the consent of the individual.</p>	Aureus Funds will ensure that individuals have the right to object at any time to the use of their personal data for direct marketing purposes.
5	Dealing with unsolicited personal information	<p>Aureus Funds will comply with the 'Unsolicited personal information' section of this Privacy Policy.</p> <p>Aureus Funds will destroy or de-identify all unsolicited personal information.</p>	Aureus Funds will not collect personal data without a specified, explicit purpose.
6	Cross border disclosure of	In accordance with the 'Sending information overseas' section of this Privacy Policy, before	Aureus Funds will only transfer personal data outside of EU jurisdiction where the recipient jurisdiction has been assessed as 'adequate' in terms of data protection,

Item no	Obligation	Australian Privacy Act requirement	Aureus Funds will comply with the GDPR requirement
	personal information	<p>Aureus Funds discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information.</p> <p>Personal information may only be disclosed where the recipient is subject to a regulatory regime that is substantially similar to the APPs, where the individual has consented, or another listed exception applies.</p>	where sufficient safeguards (such as a binding contract or corporate rules) have been put in place, or a listed exception applies.
7	Correction of personal information	In accordance with the 'How do we keep personal information accurate and up-to-date?' section of this Privacy Policy, Aureus Funds takes reasonable steps to correct personal information they hold about an individual, on request by the individual.	Aureus Funds ensures that data subjects can insist on the rectification of inaccurate personal data concerning, without delay.
8	Consent	<p>Aureus Funds ensures that when obtaining consent from an individual, the following elements are complied with:</p> <ul style="list-style-type: none"> the individual is adequately informed before giving consent; the individual gives consent voluntarily; the consent is current and specific; and the individual has the capacity to understand and communicate consent. 	Aureus Funds ensures that when obtaining consent from an individual, the consent must be freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the individual.
9	Data breach notification	From February 2018, Aureus Funds has in place policies and procedures which comply with the	Aureus Funds shall without delay and, where feasible, not later than 72 hours after having become aware of a personal data breach, notify the personal data breach to the supervisory authority.

Item no	Obligation	Australian Privacy Act requirement	Aureus Funds will comply with the GDPR requirement
		mandatory data breach notification scheme.	Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, Aureus Funds shall communicate the personal data breach to the data subject without undue delay.
10	Complaints	In accordance with the 'Incidents/Complaints Handling/Making a complaint' section of this Privacy Policy, individuals may lodge a complaint about Aureus Funds' handling of their personal information with the Office of the Australian Information Commissioner.	<p>Aureus Funds advises individuals that:</p> <ul style="list-style-type: none"> • they can make a complaint to the supervisory authority in the Member State of the individual's habitual residence, place of work or place where the breach arose. Supervisory authority can impose an administrative fine; • they have the right to seek judicial remedy in the Member State of the data subject's habitual residence, the place of work or place where the breach arose, even if Aureus Funds has no presence in a Member State; and • they have the right to seek compensation for damage suffered as a result of a breach.
11	Right to restriction of processing	Nil	<p>Aureus Funds will ensure that the individual has the right to obtain from Aureus Funds restriction of processing (where a specified ground applies). Restriction of processing means the ability to have stored personal information marked with the aim of limiting its processing in the future. The specified grounds for the restriction of processing are:</p> <ul style="list-style-type: none"> • where the accuracy of the personal data is contested by the data subject, it can be restricted for a period to enable us to verify the accuracy of the personal data; • the processing is unlawful and the data subject opposes the erasure of the personal data and requests restriction instead; • we no longer need the personal data for the purpose of processing, but the personal data is required by the data subject for legal purposes; • the data subject has objected to the processing pending the verification

Item no	Obligation	Australian Privacy Act requirement	Aureus Funds will comply with the GDPR requirement
			<p>of whether our legitimate interests override those of the data subject.</p> <ul style="list-style-type: none"> Where processing has been restricted, with the exception of storage, Aureus Funds will only process the personal data with the data subject's consent, or for the purposes of: <ul style="list-style-type: none"> legal proceedings; to protect the rights of another natural or legal person; or for reasons of public interest of the Union or a Member State.
12	Right to be forgotten	Aureus Funds will destroy or de-identify personal information that they no longer require for a lawful business purpose (see the 'Unsolicited personal information' section of this Privacy Policy).	<p>The individual is entitled to request that Aureus Funds will erase an individual's personal information without delay, and Aureus Funds will act in accordance with this request without delay, where a specified ground applies. The specified grounds are:</p> <ul style="list-style-type: none"> the personal data is no longer necessary for the purpose which it was collected; the data subject withdraws consent to the processing of the data and there is no other legal ground; the data subject objects to the processing of the data and there are no overriding legitimate grounds for the processing; the personal data was unlawfully processed; the personal data has to be erased to comply with a legal obligation in the Union or Member State to which Aureus Funds is subject; or the personal data has been collected in relation to the offer of information society services.
13	Data profiling	Nil	<p>Aureus Funds will obtain the individual's specific consent to data profiling.</p> <p>'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural</p>

Item no	Obligation	Australian Privacy Act requirement	Aureus Funds will comply with the GDPR requirement
			<p>person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.</p> <p>Profiling includes the use of website analytics, which are automated data collection methods used to determine a person's preferences on the website, and also often used to determine location of website visitors.</p> <p>Aureus Funds will ensure that, where required, it will obtain the individual's specific consent to data profiling, by ensuring that a website pop-up prompts the individual to provide their consent when undertaking profiling through Aureus Funds' website.</p>
14	Monitoring behaviour	Nil	<p>Aureus Funds will obtain the individual's consent to monitoring an individual's behaviour in so far as it takes place in the EU.</p> <p>Monitoring includes the use of cookies, which are files embedded onto the data subject's computer, meaning that the 'monitoring and tracking' occurs wherever the data subject's computer is based.</p> <p>Monitoring includes the following activities conducted by Aureus Funds:</p> <ul style="list-style-type: none"> • tracking the behaviour and browsing history of individuals on the internet; • using the tracking processes to profile the individual, to enable Aureus Funds to make decisions concerning the individual, or to enable Aureus Funds to analyse or predict their personal preferences, behaviours and attitudes. <p>Aureus Funds will obtain the individual's consent to using cookies as a monitoring tool, by ensuring that the individual consents to the use of cookies (via a cookie popup message), before Aureus Funds undertakes any monitoring activities.</p>

Endnotes

¹ The EU General Data Protection Regulations (GDPR) can apply to companies outside of the EU. You will need to be aware of whether you are required to comply with the GDPR.

Examples of when a company situated outside of the EU will have to comply with the GDPR are:

- if you process personal data of an EU citizen on behalf of, or in connection with another business, or an office situated in the EU;
- if you offer of goods or services to EU citizens (this requires some type of actively marketing goods or services to EU citizens); or
- you have website cookies and/or use website analytics.

If you do not have to comply with the GDPR requirements, please delete all references to GDPR in this template, including Annexure A. If you are required to comply with the GDPR, you may need to have in place additional measures to address this obligation.

² APP 1.5 requires an APP entity (that is, an entity which comes within the ambit of the privacy legislation) to take reasonable steps to make the Privacy Policy available to individuals, free of charge and in an appropriate format. In order to comply with this requirement, we suggest that you make it available on your website. If you don't have a website, or have a significant group of customers who do not have access to the internet, you could:

- display your policy at the entrance to your premises
- include details about how to get a copy of the policy on your correspondence
- provide a print out of the full policy on request; or
- tell individuals via telephone message how they can access the policy when they call.