adrians

PRIVACY POLICY

Adrians Group: all entities outlined on Page 2 below

Version 4.0

Meaning of personal information and sensitive information 2

When this Policy applies 2

Why we collect, hold, use and disclose personal information 3

What personal information we collect and hold 3

How we collect personal information 4

Who we share personal information with 5

Who we share your information with - Tax agent and BAS agent services 6

Disclosure of personal information overseas 7

Use of technology 7

Use of AI (Artificial Intelligence) 7

Automated Decision-Making (ADM) 8

How we protect personal information 9

Unsolicited information 9

Consequences of not providing personal information 10

Accessing and correcting personal information 10

Using our websites 11

Direct marketing 11

Use of testimonials and social media content 12

Complaints about privacy 12

Complaints related to AFS licensee entities within the Adrians Group 13

Complaints related to tax agent and BAS agent services 13

About this Policy 13

Adrians Group (us, we, our) understand that the privacy of your information is important to you, and we respect the confidentiality of the information that you provide to us. This Privacy Policy (Policy) has been proudly developed in accordance with the Privacy Act 1988 (Cth) (Privacy Act), including the Australian Privacy Principles (APPs). It details how we manage the collection, storage, use and dissemination of your personal information either through use of our services or via our website, how you can seek access to and correction of your personal information and, if necessary, how you can make a complaint relating to our handling of your personal information.

All representative entities of Adrians Group, including Adrians Capital Pty Ltd ACN 623 449 043, Adrians Wealth Management Pty Ltd ACN 640 216 539 (AFSL 522841), Adrians Corporate Services Pty Ltd ACN 693 866 803, Adrians Partners Pty Ltd ACN 130 472 258 (personally and as trustee for Adrians Unit Trust ABN 69 040 062 556), Adrians Private Wealth Pty Ltd ACN 619 714 377 (CAR of AFSL 522841), Optimum Financial Planning Services Pty Ltd ACN 694 936 368 (CAR of AFSL 522841), Optimum Financial Planning Pty Ltd ACN 159 437 573 (CAR of AFSL 522841), Adrians Insurance Pty Ltd ACN 688 846 960, and Adrians Partners Pty Ltd ACN 130 472 258 (Adrians Group) are responsible for the processing of your information as described in this Privacy Policy, unless specified otherwise. Each entity listed with an 'AFSL' (Australian Financial Services Licence) number is an Australian Financial Services Licensee (AFS licensee) and each entity listed as a 'CAR' of an AFSL is a Corporate Authorised Representative of an AFSL.

Meaning of personal information and sensitive information

The term 'personal information' has the meaning given to it in the Privacy Act when used in this Policy. Generally, it is any information or an opinion about an identified individual or a reasonably identifiable individual, regardless of whether it is true. If the definition of 'personal information' under the Privacy Act changes, that new definition will apply to this Policy.

The term 'sensitive information' has the meaning given to it in the Privacy Act when used in this Policy. Generally, it means any information or an opinion (that is also personal information) about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional association, trade association, or trade union, sexual orientation or practices, or criminal record, health information about an individual, genetic information about an individual that is not otherwise health information, and biometric information. If the definition of 'sensitive information' under the Privacy Act changes, that new definition will apply to this policy.

Business information provided to us will not ordinarily fall within the definition of personal information under the Privacy Act, but it may do so when the business information relates to sole traders and partnerships. Business information may also contain some personal information or sensitive information.

When this Policy applies

This Policy applies to the processing of information collected by us when you:

- use the services of any Adrians Group entity;
- visit or interact with our websites that display or link to this Policy or our branded social media pages;
- visit our offices or other premises;
- receive communications from us or otherwise communicate with us, including but not limited to emails, phone calls, texts or faxes;
- register for, attend or take part in our events, webinars, programs, trainings or other events;

- act as or work for a service provider or supplier to the Adrians Group, to the extent that we collect your information;
- are employed by a person or entity using our services where your information has been shared with us; or
- participate in surveys, research or other similar data collection facilitated by us.

This can include accountants, financial advisers, employees, and other people who we do business with, such as service providers and suppliers.

Why we collect, hold, use and disclose personal information

We collect and hold personal information that is reasonably necessary for, or directly related to, our functions and activities. The nature of the personal information we collect and hold, and where it comes from, will vary depending on the circumstances in which we are dealing with you and the services being provided.

We collect, hold, use and disclose personal information so we can provide our goods and services to you (including business advice, tax compliance services, Australian Securities and Investments Commission (ASIC) compliance advice, financial advice, financial product advice and related services relevant to your needs), to administer our organisation, and comply with our regulatory obligations. Specific purposes for which we may collect, hold, use and disclose your information include for:

- complying with our legal obligations, such as (without limitation) verifying your identity;
- assisting with your questions, rectifying problems, managing our relationships, and responding to feedback and complaints;
- arranging for or facilitating services to be provided by third parties;
- internal operations, such as record keeping, billing, data analytics, auditing or training;
- making, or assisting us to make decisions using computer programs (Automated decision-making);
- helping us provide and improve the products and services offered to our clients and enhance our overall business;
- considering an individual's job application;
- enforcing any agreements between you and us;
- operating our website and performing administrative and operational tasks; and
- promoting of other products and services that may be of relevance to you.

Our legal obligations may include (without limitation) complying with the 'Customer Due Diligence' requirements in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act). We may need to collect your personal or sensitive information to establish and verify your identity before providing certain services to you or the person you are acting on behalf of to assess and manage potential money laundering, terrorism financing, and proliferation financing risks or related compliance risks associated with the provision of our services, make reports required by law under the AML/CTF Act, and meet record keeping obligations under the AML/CTF Act.

What personal information we collect and hold

We collect and hold personal information that is necessary to assist us in providing relevant services and products to you. The types of personal information or sensitive information we collect and hold could include:

- your identity data, such as your full name, date of birth, gender, occupation, and age;

- where we are required to verify or establish your identity (whether to comply with the AML/CTF Act, tax practitioner regulations, or our other legal requirements), your identity documents such as your driver licence, passport, or similar documents, and any photo ID;
- your contact data, such as your residential address, business address, email, and telephone number;
- your employment data, such as your employment details;
- your relational data, such as your marital status and personal information about your family and dependants;
- your financial data, such as your income, savings, assets, liabilities, expenses, transactions, insurance policies, financial goals, objectives and risk tolerance, bank accounts, and other financial information and billing information;
- other information generated as part of providing our services or advice to you, such as call and meeting records and AML/CTF screening results (including sanctions, politically exposed person and adverse media); and
- other information where it is relevant to the service or advice being provided or necessary for us to comply with our legal obligations. For example:
  - sensitive information about your medical history, health and lifestyle to provide you with financial advice about life insurance products, with your consent;
  - your government related identifiers, such as your Tax File Number (TFN) and Director Identification Number (DIN) where you are receiving tax and ASIC services from us. We will only request or collect your TFN information (as defined in the Privacy Act) where authorised at law and in the manner required at law.

We are also required by law to destroy or permanently de-identify certain data components (e.g., TFNs, credit card details etc) when they are no longer necessary for the reason they were collected.

We keep the information we collect for as long as required to achieve the purpose for which it was collected or where longer retention is required or authorised at law.

We are required to retain your personal information or sensitive information to comply with certain record keeping obligations at law, which will vary depending on the type of information we collect and the nature of the services we are providing. For example, and without limitation, we are required to retain accurate client records for at least five years after tax advisory services have been provided to you, 'Customer Due Diligence' records under the AML/CTF Act for at least 7 years after a business relationship ends or a relevant transaction completes, and records of advice (including information relied on) given by an AFS licensee for at least 7 years after the day the advice is given.

How we collect personal information

In most instances, we collect personal information or sensitive information directly from you when you:

- register with us or give us permission to collect data;
- interact with us or our services including online interactive tools such as a budget planner;
- sign up for promotional or marketing materials;
- communicate with us directly (e.g., in person, phone, email, internet, or in writing) or through social media;
- complete data collection documentation;
- complete a financial product or credit product application form;
- complete an identification form;
- provide documentation to us; or
- otherwise as described in this policy.

We may collect personal information from other people and organisations if you consent, the collection is required or authorised at law or by a court order, the collection is reasonably necessary for, or related to, our provision of services to you, is required in order for us to comply with our regulatory or reasonable internal requirements, or where direct collection is unreasonable or impracticable. These may include (but are not limited to):

- from other entities in the Adrians Group in the ordinary course of business;
- someone you have authorised to act on your behalf like a partner, family member, agent or power of attorney or guardian;
- government agencies or law enforcement agencies;
- a financial adviser;
- a mortgage broker or other credit representative;
- professionals who act on your behalf, such as a lawyer or accountant;
- from third parties such as credit agencies or referral services;
- health professionals;
- other organisations, who jointly with us, provide products or services to you; and
- social media and publicly available sites.

Who we share personal information with

From time to time, we may share your personal information with other entities both within and outside of Adrians Group. We may disclose your information to a third party where you have given your consent, where you would reasonably expect us to disclose your information to that third party, where it is reasonably necessary for, or related to, our provision of services to you, or where we are required or authorised by law. The third parties and circumstances in which we will disclose your personal information will vary according to the service or product we are providing you, but could include:

- our related entities, affiliates or partners, representatives and companies in the Adrians Group, to carry out the functions and activities of a corporate group, or the functions and activities of individual companies within the group;
- any person acting on your behalf, including your financial adviser, solicitor, accountant, executor, administrator, trustee, guardian or attorney;
- third party service providers to provide, improve and streamline our services to you and others, such as software or IT service providers;
- third party service providers in arranging or facilitating their provision of goods or services to you and others;
- financial product and service providers, including financial planning software providers and paraplanners;
- for corporate superannuation members, your employer or your employer's financial adviser;
- medical practitioners and health service providers, such as pathology services;
- companies involved in the payments system including financial institutions, merchants and payment organisations;
- social network providers when social network widgets, plugins or buttons are used in our services;
- advertising and marketing (which may, with your consent, include location data);
- organisations who assist us with certain business functions, such as auditors, compliance consultants, direct marketing, debt recovery and information and communication technology support;
- our professional advisers (such as solicitors), our insurers, and courts, tribunals and dispute resolution organisations;

- another third party where you request that we do so, for example, if you wish to cease using our services and require us to transfer your details and accounts to a different service provider;
- other organisations who provide us with products and services so that they may provide their products and services to you or contact you on our behalf;
- identity verification service providers; and/or
- anyone to whom we, or our service providers, are required or authorised by law to disclose your personal information to (for example, law enforcement agencies, Australian and international government and regulatory authorities, or where a permitted general situation exists under the Privacy Act).

We take reasonable steps to ensure that these organisations are bound by privacy obligations in relation to the protection of your personal information. However, this Policy applies solely to information collected, held, and used by us. Where a third party collects personal information directly from you or handles it for its own purposes, that third party's handling of the information is governed by its own privacy policy.

Who we share your information with - Tax agent and BAS agent services

Where tax agent services or business activity statement (BAS) services are provided to you (together, Tax Agent Services), our registered tax agents and BAS agents (tax practitioners) must comply with the privacy and confidentiality obligations in the Code of Professional Conduct under the *Tax Agent Services Act 2009* (Cth) (TASA). These stricter obligations apply to any information relating to your affairs, whether or not it belongs to you or has been directly provided by you (client information). Despite anything else in this Policy, where the services we provide you are Tax Agent Services, our tax practitioners will not disclose client information collected in the course of providing those Tax Agent Services to a third party (being any person or entity other than you and the tax practitioner) unless:

- you have given us your permission to do so, which we will generally ask you to give in your signed engagement letter or another signed consent;
- there is a legal duty to make the disclosure (such as in response to a notice from the Tax Practitioners Board under section 60-100 of the TASA or the Australian Taxation Office under section 353-10 in Schedule 1 of the *Taxation Administration Act 1953 (Cth)*, in response to a court or tribunal order or direction, where required under the AML/CTF Act, where required upon request from an AFS licensee under section 912G of the *Corporations Act 2001* (Cth), or where required to report a breach of the Code of Professional Conduct under the TASA);
- the disclosure is permitted, and solely to the extent permitted, at law (such as where the whistleblower provisions under the *Tax Administration Act 1953* (Cth) apply); or
- there is a need for the tax practitioner to obtain legal advice in respect of dealing with a complaint and defending a claim.

Our tax practitioners will not rely on your reasonable expectations, or on the other grounds for disclosure described in 'Who we share personal information with' above, to disclose client information in connection with Tax Agent Services.
When you obtain Tax Agent Services, our engagement letter will request your permission to disclose your client information to certain third parties. These third parties include:

- entities and organisations within the Adrians Group, including any AFS licensee (including CAR of the AFSL) that the tax practitioner is an authorised representative of;
- our external IT, software and cloud service providers, and other offshore service providers as described in 'Disclosure of personal information overseas' below; and

- certain AI tools as described in 'Use of AI (Artificial Intelligence)' and 'Automated Decision-Making (ADM)' below.

Client information is disclosed to these third parties for the purpose of you receiving the Tax Agent Services and, insofar as it relates to disclosure of information to other entities within the Adrians Group, to carry out the functions and activities of our corporate group and business (or where it is required for us to operate our business, such as where shared IT systems are used).

Client information collected and held by our tax practitioners will be managed and protected in accordance with 'How we protect personal information' and 'Unsolicited information' below.

Disclosure of personal information overseas

We may disclose your personal information to service providers who operate outside Australia. We may also disclose your personal information to the following persons located in the countries specified below, and your information may be held in those countries to:

- our overseas service providers in the Philippines who are engaged to assist with administrative, operational, accounting, taxation compliance, business advisory and financial services support;
- certain software or IT tools (including AI tools) that process information offshore, notably Microsoft (including for Microsoft 365 Copilot) in the United States of America; and
- data hosting providers with servers located in Australia and in some instances overseas such as Singapore.

It is not reasonably practicable to list all the countries to which your information may be transmitted from time to time. However, when we send your personal information to overseas recipients, we make sure appropriate data handling and security arrangements are in place. In accordance with APP 8.1 of the Privacy Act, all reasonable steps will be taken to ensure that offshore service providers comply with the Privacy Act.

Use of technology

We may, from time to time, record meetings, calls and communications through video conferencing, telephone or online platforms. Recordings are used for record-keeping, training, compliance and quality assurance purposes. You will be notified of any recording at the commencement of a meeting or call where practicable. These recordings are stored securely and accessed only by authorised personnel and may be retained and disclosed as required by law and this Policy. If you do not wish for a conversation to be recorded, please advise us prior to or at the start of the meeting or call. Where a meeting or call is held by video conference, telephone or online platform, we may ask you to confirm who is present with you, and we may take steps to confirm the identity of each person attending, before we discuss information relating to your matter. We do this so that your information is not disclosed to anyone you have not permitted to receive it.

Use of AI (Artificial Intelligence)

We may use artificial intelligence (AI) and automated technology tools in the provision of our services, including to assist with research, document preparation, client communications and administrative functions, to analyse personal information to improve service quality and efficiency, and to offer insights or recommendations. AI tools are used to support our services only and all material outputs, decisions, recommendations and communications remain subject to human review, judgement and oversight. We currently use the following AI tools (which may vary and updated from time to time):

- Microsoft 365 Copilot;
- VerifiMe;
- Plaud; and

- Elfworks.

Our privacy obligations will apply to any personal information input into an AI system, as well as the output data generated by AI (where it contains personal information). Any personal information generated or inferred by an AI system (even if it is incorrect) is considered to be the collection of personal information by us, and will only occur by lawful and fair means where it is reasonably necessary for our functions or activities.

Personal information will only be used or disclosed to AI for the primary purpose or reasonably related purposes for which we have collected that information, or otherwise with consent.

We will not enter your TFN or TFN information into an AI tool except as permitted under the *Privacy (Tax File Number) Rule 2015* (Cth).

Automated Decision-Making (ADM)

We may use computer programs in some of our processes. These include rules-based software, algorithms, programs, applications and artificial intelligence tools, some of which are provided by third-party service providers. In some cases, a computer program may make a decision or do something that is substantially and directly related to making a decision based on the information we have collected from you which could reasonably be expected to significantly affect your rights or interests.

Kinds of personal information used

The kinds of personal information used in the operation of these computer programs may include:

- identity information and identity documents (including photo ID), and the results of AML/CTF screening (including sanctions, politically exposed person and adverse media checks);
- financial information, such as your income, assets, liabilities, expenses, transactions and tax information;
- employment and occupation details, and information about your family and dependants;
- your financial goals, objectives and risk tolerance, and your responses to our questionnaires and fact-finding documents; and
- with your consent, health and lifestyle information where relevant to advice about life insurance products.

Decisions made solely by a computer program

We do not currently make any decisions that could reasonably be expected to significantly affect your rights or interests solely by the operation of a computer program.

Decisions where a computer program assists us

Computer programs do things that are substantially and directly related to making the following kinds of decisions:

- whether we can verify your identity and accept you as a client, including through electronic verification of your identity documents;
- whether we can start or continue to provide a service to you, including the outcome of screening against sanctions, politically exposed person and adverse media lists, and the risk rating we assign to you under our anti-money laundering and counter-terrorism financing obligations;
- the financial advice and recommendations we provide to you, including your risk profile and the product, strategy and insurance cover recommendations generated with the help of financial planning software and calculators; and

- the preparation and lodgement of your tax returns and other tax, ASIC and compliance documents, including calculations and pre-filled data generated by tax and accounting software.

Where a computer program assists with any of these decisions, a member of our team reviews the output and is responsible for the final decision. If you have any questions about how a computer program has been used in a decision that affects you, or you would like us to reconsider a decision, please contact our Privacy Officer (details below).

How we protect personal information

We strive to ensure that the personal information that you provide to us is stored safely and securely. We take precautions to protect the personal information we hold about you from misuse, interference and loss, and from unauthorised access, modification or disclosure.

We store most information about you in computer systems and databases operated by either us or our external service providers. Some information about you is recorded in paper files that we store securely.

We implement and maintain a range of processes, security measures, practices and policies to protect personal information we hold from misuse, interference or loss, and from unauthorised access, modification or disclosure. These include:

- educating our staff and representatives about how to protect your personal information and updating them about cybersecurity developments, threats and scams;
- securing passwords in accordance with stringent password management policies;
- using Multi-Factor Authentication (MFA);
- using secure client portals and/or password protection;
- restricting employee access to certain sections of the system (as relevant to their role);
- strict confidentiality arrangements restricting third parties' use or disclosure of personal information for any unauthorised purposes;
- data and cyber security assessments of third-party providers and systems;
- secure destruction and disposal of IT equipment and paper records;
- employing firewalls, intrusion prevention systems, web/email filtering and antivirus/antimalware tools; and
- internal policies and procedures, including artificial intelligence usage guidelines, and a Cybersecurity Policy, Cyber Incident Response Plan, and Data Breach Response Plan.

We require our representatives to protect your personal information by adhering to a range of cybersecurity measures.

Where personal information is no longer required for the purposes for which it was collected, at law, or for any secondary purpose permitted under the APPs, we will take steps to de-identify or destroy the information in a secure manner.

Unsolicited information

In certain circumstances, we may receive personal information about third parties unsolicited from individuals who contact us or supply us with personal information belonging to others (including in documents they provide). We will handle this information in accordance with this Policy and the Privacy Act.

Where we receive unsolicited personal information that we do not need to deliver services to you (for example in correspondence that you may send to us), we will destroy or de-identify this information where it is reasonable to do so. Where we retain this information, we will handle it in accordance with this Policy and the Privacy Act.

Consequences of not providing personal information

In some circumstances the law requires us to collect your personal identification information including obtaining and verifying details of photographic and non-photographic identification documents for us to provide services, in which case you cannot remain anonymous or use a pseudonym when dealing with us.

It is your choice whether to provide your personal information. You have the right to not provide personal information, including about your identity. However, in this case, your accountant or adviser will warn you about the possible consequences and how this may impact on the quality of the services and/or advice provided. Your accountant or adviser may also decline to provide services or advice if they feel they have insufficient information to proceed. In some instances, we will decline to provide services or advice if we feel we have insufficient information for the scope of the service or advice requested.

If you wish to remain anonymous or to use a pseudonym when dealing with us, we may only be able to provide you with limited information or services. In many cases it will not be possible for us to assist you with your specific needs.

Accessing and correcting personal information

You, or someone that you nominate, can request access to personal and financial information we hold about you. Should you require access to your personal or financial information, please request access by contacting our Privacy Officer (details below) and be specific about the information you require.

We will need to validate the identity of anyone making an access request, to ensure that we do not provide your information to anyone who does not have the right to access that information. We will deal with requests for access to your personal information as soon as possible and aim to respond within 30 days. The time we require will depend on the type of information requested and whether it is in physical or electronic format.

There may be a cost involved with locating, copying or sending you the information you request, and we may charge you for our reasonable expenses for providing or facilitating your access. The cost will be discussed and agreed with you at the time.

Gaining access to your personal and credit information is subject to some exceptions allowed by law. Factors affecting a right to access include where:

(a) we reasonably believe that access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
(b) access would have an unreasonable impact on the privacy of others;
(c) the request for access is frivolous or vexatious;
(d) giving access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process;
(e) access would be unlawful;
(f) denying access is required or authorised by or under an Australian law or a court/tribunal order;
(g) we have reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to our functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter;

(h) access would prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(i) the information relates to existing or anticipated legal proceedings between you and us, and it would not be accessible by the process of discovery, or the information would prejudice negotiations with you.

If we refuse access, or refuse to give access in the manner requested, we will notify you in writing of the reasons for the refusal unless it would be unreasonable to do so. If you disagree with our decision, you may make a privacy complaint using the complaints procedure below.

We take reasonable steps to ensure that your personal information is accurate, up to date, complete and relevant. If you believe the personal information collected or used by us or a third party is false or inaccurate, you have a right to have this information corrected and we will endeavour to do so within a reasonable timeframe, at no expense to the relevant individual. If we are unable or refuse to correct your personal information, you may ask us to include a statement that you believe your personal information is inaccurate, out of date, irrelevant or misleading.

In most cases, you can update your personal information over the phone, by contacting your accountant or adviser.

Using our websites

Some personal information may be collected whilst navigating through and interacting with the content of our websites (Site). The electronic methods of collection we use include cookies, log files, web beacons, pixels and analytical tools. The information we collect by these electronic means is generally not stored for long – they are temporary records – and can include device-specific data or log data such as your IP address, device screen size, device type, browser information, referring domain, pages visited, the date and time website pages were visited, and geographic location (country only).

Cookies record information about your visit to our websites, and it is used to improve your website experience, to serve you with relevant information and to manage your access to certain parts of our websites. You can choose if and how a cookie will be accepted by changing your browser settings; but please be aware that this may affect your access to some parts of our websites.

Web beacons help us better manage content on our websites by allowing us to understand usage patterns, fix issues, and improve the products and services offered to you on our websites. Log files contain information about the devices and browsers used to access our websites and help us to diagnose problems, analyse trends, administer the site or mobile application.

The Site may link directly to websites operated by third parties (Linked Sites). You acknowledge that Linked Sites are not operated by us. We encourage you to always read the applicable privacy policy of any Linked Site. We are not responsible for the content or practices of the Linked Sites or their privacy policies regarding the collection, storage, use and dissemination of your personal information.

Direct marketing

We may only use personal information we collect from you for the purpose of direct marketing without your consent if:

- the personal information does not include sensitive information;
- you would reasonably expect us to use or disclose the information for the purpose of direct marketing;
- 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.

We may use personal information to send information about our products and services, notify you of new legislative developments that relate to the services we provide you, or for other commercial communications from us which may be secondary to the primary reason we have collected that information, where you would reasonably expect us to do so or have consented to us doing so.

Each direct marketing communication will include a simple means of opting out (such as an 'unsubscribe' link). You can also contact us to 'opt out' should you wish not to receive direct marketing, however you agree and acknowledge that even if you 'opt out' of receiving marketing material, we will still send you essential information that we are required to send you relating to the services we provide.

Use of testimonials and social media content

If you provide a testimonial or engage with our accounts or pages via social media or public forums, you acknowledge that such content may be publicly visible and may be used by us in our promotional or marketing materials. We may, with your express consent or where permitted by the relevant platform's terms, use your testimonial or comments for promotional purposes. You may request the removal or amendment of content that you have contributed by contacting us.

Complaints about privacy

If you have any privacy related questions or would like further information on our privacy and information handling practices or are concerned about how your personal information has been collected, used or disclosed and you wish to make a complaint, please contact us.

Mail:	GPO Box 1050, Brisbane QLD 4001
Phone:	07 3832 7544
Email (Business and Tax Advisory):	info@adriansgroup.com.au
Email (AFS licensees):	licensee@adriansgroup.com.au
Email (Privacy Officer):	treddacliff@adriansgroup.com.au
Website:	adriansgroup.com.au

If you have a complaint about the way in which we have handled your personal information, including in relation to your request for access or correction of your personal information, you should contact the Privacy Officer listed above. We will acknowledge a complaint within 5 business days, investigate it, and give you a written response setting out our findings and any action we will take, usually within 30 days.

If you are not fully satisfied with our response, you can contact an external body. In cases of privacy related complaints, this is generally the Office of the Australian Information Commissioner (OAIC).

Complaints related to AFS licensee entities within the Adrians Group

If you have a complaint about the way in which one of the AFS licensees in the Adrians Group has handled your personal information, including in relation to your request for access or correction of your personal information, or an AFS licensee in the Adrians Group generally, you should contact the Privacy Officer or AFSL specific-contact listed above. We will acknowledge receipt of a complaint within 1 business day, however, where this is not possible, acknowledgement will be made as soon as practicable. We will then investigate the complaint and respond to you within 30 days. Some complex matters may require an extension to thoroughly investigate the complaint and bring it to resolution. If additional time is required, we will advise you in writing.

The contact details for OAIC are:

Mail	GPO box 5218, Sydney NSW 2001
Phone	1300 363 992
Email	enquiries@oaic.gov.au
Online	www.oaic.gov.au

You may also direct privacy complaints related to financial advice to the Australian Financial Complaints Authority (AFCA). The contact details for AFCA are:

Mail	GPO Box 3, Melbourne, VIC 3001
Phone	1800 931 678 (free call)
Email	info@afca.org.au
Online	www.afca.org.au

Complaints related to tax agent and BAS agent services

If you have a complaint about a Tax Agent Service, including the way we have handled your client information, please contact us using the details under 'Complaints about privacy' above. You can also make a complaint to the Tax Practitioners Board (TPB) at any time. The TPB maintains a public register of registered tax agents and BAS agents, which you can search on its website.

The contact details for the TPB are:

Mail	GPO Box 1620, Sydney NSW 2001
Phone	1300 362 829
Online	www.tpb.gov.au

About this Policy

We may amend or update our Privacy Policy as required by law or as our business processes or technology changes. If we introduce new processes or change our processes (particularly in relation to our use of AI and ADM), or any changes to the Privacy Act, APP or other laws or regulations we are subject to change, and will update, this Privacy Policy and take reasonable steps to notify you beforehand. We will post the updated policy on our website – adriansgroup.com.au. We encourage you to check our website from time to time to view our current policy or contact us for a printed copy.