AD Advisory Services Pty Ltd

ABN 68 005 830 802

Australian Financial Services License No. 237058

Privacy Management Procedures
(including Privacy Policy)

DOCUMENT MANAGEMENT

Responsibility for Procedure*— Jonathan Thomas — Director

Revision History

Note: *Version(s) numbering is Licensee Compliance Solutions' current template supply sequence and not necessarily that of AD Advisory Services.*

Date	Version	Description Of Review	Author
July 2023	V0623	Review and re-write of Procedure simplifying guidance and procedures.	K Hockley
June 2022	V0622	Review of Procedure conducted. Minor updates.	T Everitt
June 2021	V0620	Review of Procedure conducted.	K Hockley
June 2020	V0620	Review of Procedure conducted with updates to the definitions, procedures, appendices and User Note inclusions.	K Hockley

Approval

Version	Approval	Date	Privacy Officer	From	To
V0623	Jonathan Thomas	January 2024	Jonathan Thomas	Inception	Current
V0622	Jonathan Thomas	January 2023	Jonathan Thomas	Inception	Current
V0620	Jonathan Thomas	30/11/20	Jonathan Thomas	Inception	Current
5.0	Jonathan Thomas	August 2019	Jonathan Thomas	Inception	Current

Version Control Management

Version	Original Document Location
V0623	AFSL Compliance Manager — Dropbox / 1 AD Advisory Services / POLICIES & PROCEDURES / 2 Privacy Management Procedures
5.0, V0620, V0622	Archived

*** Note:** *This document is designed to provide an overview of the regulatory requirements and you will need to make sure all aspects of the document are appropriate for your business, and any Representatives. If it is not correctly tailored by you and kept up to date it may not comply with regulatory requirements. Licensee Compliance Solutions (LCS) is not responsible for the final tailoring, customisation, implementation, circulation or use of the document and or any applicable resources, worksheets, procedures, registers etc. While every care is taken in the preparation of this document* ***LCS recommends that legal advice, by suitably qualified legal practitioner, be obtained before finalising this document its appendicles and their use as applicable to your license and operations.*** *LCS makes no representation that this document is fit for you or your Representatives' purpose and accepts no responsibility for any loss or damage or cost incurred as a result of its use.*

Confidentiality

This document is confidential to AD Advisory Services Pty Ltd and must not be disclosed to any third party without their express written approval.

TABLE OF CONTENTS

1. Purpose of the Procedure 4
2. Governing Framework 4
3. Scope of the Procedure 4
3.1 Other Relevant Policies 4
4. Definitions 4
5. Procedure and Obligations Overview 6
5.1 Responsibility 6
5.2 Key Requirements 6
5.3 Introduction 7
5.4 What does the Privacy Act regulate? 7
5.5 Other Legislation 7
5.6 Tax file numbers 8
5.7 Privacy Officer 8
5.8 Privacy Compliance Plan 8
5.9 Open and Transparent Management of Personal Information 8
5.10 Compliance with the Australian Privacy Principles (APPs) 9
5.11 Use and disclosure of personal information 11
5.12 Data quality and security of information 11
5.13 Data security 11
5.14 Openness 12
5.15 Access and correction of Personal Information 12
5.16 Identifiers 14
5.17 Anonymity 15
5.18 Cross border data flows 15
5.19 Tax Relevant Providers and Privacy Consent 16
5.20 Privacy Breaches 16
5.21 Eligible Data Breaches 17
5.22 What is serious harm? 17
5.23 When does a Data Breach become an eligible Notifiable Data Breach (NDB)? 17
5.24 Data Breach Response Plan 17
5.25 Complaints Handling and Incident Reporting 17
5.26 Privacy Consent Forms 18
5.27 Monitoring and supervision 18
6. Approval and Review 18
Annexure A – Privacy Management Plan 19
Appendix 1 – Summary of the Australian Privacy Principles 22
Table 1 – Australian Privacy Principles Flow Chart 23
Appendix 2 – Collection Statement Handout EXAMPLES 24
Appendix 3 – Privacy Policy EXAMPLE 25
Appendix 4 – Letter of Authority to Access Information EXAMPLE 32
Appendix 5 – Privacy Access Request Refusal Letter EXAMPLE 33
Appendix 6 – Declaration and Privacy Consents 34
Appendix 7 – Verbal Privacy Consent Checklist 35
Appendix 8 – Representatives Privacy Checklist 36
Appendix 9 – General Data Protection Regulation (GDPR) 37

[**User Note**: Any Appendices in this document with the word EXAMPLE in the title or 'User Note', are supplied as an 'example' template. Carefully review your methodology to ensure it is compliant, tailored, fit for purpose and accurately reflects what happens in practice.]

PRIVACY MANAGEMENT PROCEDURES

1. Purpose of the Procedure

This document sets out the procedures for AD Advisory Services Pty Ltd ("AD Advisory Services", the Licensee), as the holder of an Australian Financial Services Licence (AFSL), to describe the obligations, under the *Privacy Act 1988* (Cth), AD Advisory Services has and what needs to be done in order to meet those obligations. The Appendices contain various example documents that can be tailored, when and where applicable, for the operations of AD Advisory Services and its Representatives.

2. Governing Framework

Corporations Act 2001

National Consumer Credit Protection Act 2009

Privacy Act 1988 (Cth)

ASIC Corporations and Credit (Reference Checking and Information Sharing Protocol) Instrument 2021/429

3. Scope of the Procedure

As noted above in 'Purpose of the Procedures Policy', the scope takes into account guidance as referred to above in the Governing Framework.

This procedure applies to Directors, Responsible Managers, Senior Managers, Contractors, Consultants, Representatives, Employees and all other persons within AD Advisory Services. You must follow AD Advisory Services' Privacy Procedures and Privacy Policy when collecting and using personal information.

3.1 Other Relevant Policies

This procedure should be read in conjunction with, including but not necessarily limited to:

- Complaints Handling Policy;
- Incident and Breach Reporting Policy (including Privacy Act Eligible Data Breaches);
- Representatives: Appointing Reference Checking and Reference Giving Policy; and
- Risk Management Policy.

4. Definitions

Compliance Manager means a person nominated and formally appointed by AD Advisory Services who is responsible for monitoring, supervising and overseeing the compliance requirements of AD Advisory Services reporting to the Responsible Managers and Director. Currently, the oversight of this role is held by Keith Hockley and Licensee Compliance Solutions. AD Advisory Services has determined a number of base hours for the performance of this service by the external compliance manager. Note: The Compliance Manager is not responsible for ensuring that this policy is implemented and monitored within AD Advisory Services unless formally named as the Responsible Person on page 2, or requested by the Director, and accepted in writing.

Consumer credit means credit that is intended to be used wholly or primarily:

- for personal, family or household purposes;
- to acquire, maintain, renovate or improve residential property for investment purposes; or
- to refinance credit that has been provided for the above purposes.

Credit information is a sub-set of personal information because the individual's identity is provided with the credit information. There are specific types of financial information that fall within this definition.

Credit provider includes banks, building societies, credit unions, and companies where a substantial part of their business is the provision of loans. Businesses will also be treated as credit providers if they are agents or servicers of credit providers or suppliers of goods or services that defer payment for more than seven days, such as electricity and telecommunications providers.

Director means a Director of AD Advisory Services Pty Ltd.

Employee means all staff of AD Advisory Services; including support staff who are involved in providing financial services and other staff who do not provide financial services.

Notifiable Data Breaches refer to the Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act, which established requirements for entities in responding to data breaches. Entities have data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

OAIC is an abbreviation for the 'Office of the Australian Information Commissioner'.

Personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, or whether it is oral or in writing and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. In effect, it is information or an opinion that can identify a person, for example, their name, physical description, address, date of birth, sex, phone number, email address, driver's licence number and information about their employer / place of work, salary and employment, business activities, investments, assets and liabilities – or any combination of these.

Privacy Amendment (Enhancing Privacy Protection) Act 2012 set out the Australian Privacy Principles (APPs), these Principles aim to ensure that organisations that hold information about people handle that information responsibly.

Privacy Officer referred to in this document is named above in the 'Approval' section of the 'Document Management' on page 2. They report to the Director and Compliance Manager. The Privacy Officer is responsible for monitoring, supervising or overseeing the privacy procedures of the organisation and persons within AD Advisory Services. In the Privacy Officer's absence, the Director remains responsible for this role and task.

Representative under the *Corporations Act 2001*, means:
A person (or company, trust or other entity) who is appointed to act as an Authorised Representative of a Licensee to provide financial services under their AFS Licence. This includes:

- an employee or Director of AD Advisory Services (appearing on the ASIC's Financial Adviser Register) and called a 'Financial Adviser';
- an employee or Director of a related body corporate of AD Advisory Services (appearing on the ASIC's Financial Adviser Register) and called a 'Financial Adviser' and or an 'Authorised Representative'; or
- any other person (an 'Individual', including a company, trust or other entity) acting on behalf of AD Advisory Services (excluding external legal counsel) appearing on the ASIC database as an Authorised Representative

who are authorised in writing to provide financial services on behalf of AD Advisory Services.

Responsible Managers means persons nominated and formally appointed by AD Advisory Services under its AFSL whose expertise and skills are relied upon for the provision of the financial services activities authorised under its AFS License and responsible for significant day-to-day decisions about the ongoing provision of AD Advisory Services' financial services. See the Fit and Proper Persons & Responsible Managers Policy, and its appendices (*Responsible Manager & Compliance Management – Table of Organisational Competence*), for our current Responsible Managers.

Responsible Person referred to in this document is named above in the 'Approval' section of the 'Document Management' on page 2, is responsible for ensuring that this policy is implemented and monitored within AD Advisory Services. They report to the Director and Compliance Manager. In the Responsible Persons absence, the Director remains responsible for the obligations of the Responsible Person.

Sensitive information is personal information about such things as race or ethnic origin, political opinions, religion or philosophical beliefs or affiliations, membership of a trade or professional association or a trade union, sexual preferences, criminal record or health information (including biometric and genetic information). Health information includes recording an illness or pregnancy on an application form or information collected to support a hardship application. (Additional obligations apply to the collection, use and disclosure of sensitive information.)

Telecommunications Act 1997 **(Cth**) regulates the activities of a number of participants in the telecommunications industry, including 'carriers' and 'carriage service providers'

Third Party refers to a party, individual or organisation who is collecting information from someone other than the person to whom it relates.

The Spam Act 2003 **(Cth)** prohibits the sending of unsolicited commercial electronic messages linked with Australia, including (but not limited to) email, SMSM, multimedia message service or instant messaging without the consent of the receiver.

The Privacy (Tax File Number) Rule 2015 (TFN Rule) regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN information. The TFN Rule only applies to the TFN information of individuals and does not apply to TFN information about other legal entities such as corporations, partnerships, superannuation funds and trusts.

5. Procedure and Obligations Overview

All staff including Responsible Managers, Corporate Authorised Representatives, Representatives and other employees must comply with and adhere to the requirements identified in this procedure.

5.1 Responsibility

The Responsible Person will be responsible for implementing this policy with the assistance of the external Compliance Manager. This policy is reviewed every year by the external Compliance Manager. If there is a major breach in areas of this policy, the external Compliance Manager shall review, with the assistance of the Responsible Person, the relevant procedure.

Ensure

- We follow privacy requirements when we collect personal information
- We adopt Privacy Policy and Collection Statement ('Privacy Policy') and post it on our website
- We comply with a client request to view file and correct information
- We comply with *ASIC Corporations and Credit (Reference Checking and Information Sharing Protocol) Instrument 2021/429* ('The Protocol')
- We address all suspected or known data breaches

Collect

- Only relevant client information
- Signed privacy agreements where disclosing to third parties
- Written consent before asking for a reference from a 'referee licensee' regarding a prospective representative
- Where required for COVID-19 contact tracing, personal information from individuals

Maintain

- Accuracy and security of client files
- Security of Tax File Number information

Do not

- Collect personal information from a third party except in certain circumstances
- Use or disclose client personal information for direct marketing purposes, unless express consent has been obtained
- Continue to hold TFN information if it is no longer required.

5.2 Key Requirements

Licensee

Do	When
Develop, adopt, and post a Privacy Policy and Collection Statement (Privacy Policy) on our website	Immediately

Representative

Do	When
Provide our client a Privacy Policy and Collection Statement (Privacy Policy)	Before collecting personal information
Only collect, use, and hold relevant client information which we have disclosed in our Privacy Policy and Collection Statement (Privacy Policy)	At all times

DO NOT	
Do not collect personal information from a third party	Unless it is unreasonable or impractical to collect it directly from our client

5.3 Introduction

As a private sector organisation, AD Advisory Services is bound by the *Privacy Act 1988* (Cth) (Privacy Act), which sets out rules about information handling, including how businesses may collect, use, store and disclose personal information.

It must also comply with the Australian Privacy Principles (APPs) as set out in the Privacy Act – *Privacy Amendment (Enhancing Privacy Protection) Act 2012*. The APPs aim to ensure that organisations that hold information about people handle that information responsibly. They also give people some control over the way information about them is held. A summary of the APPs, along with an APPs flow chart, is included in Appendix 1 – Summary of the Australian Privacy Principles.

Note: The Privacy Act applies to any business that:

(a) had a turnover greater than $3,000,000 in the previous financial year; or

(b) is a subsidiary of a company that had a turnover of more than $3,000,000; or

(c) regardless of turnover, discloses personal information about an individual for a benefit, service or advantage.

Financial services and finance industry participants do not fall within the small business operator exemption as they disclose personal information about individuals for a benefit, service, or advantage, and so must comply with the Privacy Act.

The Privacy Act has a separate set of provisions dealing with the collection, use, and disclosure of:

(a) personal information; and

(b) credit information.

The Privacy Act extends to acts done or practices engaged in and outside Australia if:

- the *personal information* relates to an Australian citizen;
- the organisation has a continued presence in Australia; and
- the *personal information* was collected or held by the organisation in Australia either before or at the time of the act or practice.

5.4 What does the Privacy Act regulate?

The *Privacy Act 1988* (*Privacy Act*) regulates how personal information is handled. The Privacy Act defines personal information as:

> *"…information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable".*

Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.

The Privacy Act includes thirteen Australian Privacy Principles (APPs), which apply to some private sector organisations, as well as most Australian and Norfolk Island Government agencies. These are collectively referred to as 'APP entities'. The Privacy Act also regulates the privacy component of the consumer credit reporting system, tax file numbers, and health and medical research.

5.5 Other Legislation

The *Spam Act 2003* (Cth) prohibits the sending of unsolicited commercial electronic messages.

Broadly, an electronic commercial message is an email, SMS, or other such message that contains an offer to supply goods or services or other investment opportunity. In summary:

(a) it is illegal to send most commercial electronic messages to or from Australia without the recipient's consent;

(b) certain commercial electronic messages are exempt from the consent requirement;

(c) those commercial electronic messages which can be lawfully sent must include accurate information about the sender and generally contain a functional unsubscribe facility;

(d) it is illegal to supply, acquire, or use address-harvesting software or a harvested address list; and

(e) civil penalties of up to $1,100,000 per breach, per day apply to these illegal activities.

Inferred consent can arise where the recipient has a reasonable expectation that the message will be sent. It may be reasonable to infer consent from an existing relationship with the individual.

Note: Also see the *Telecommunications Act 1997 (Cth).* If you use electronic marketing intensely you will need to more fully understand both the Spam and Telecommunications Acts.

5.6 Tax file numbers

The Privacy (Tax File Number) Rule 2015 (TFN Rule) regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN information. The TFN Rule only applies to the TFN information of individuals and does not apply to TFN information about other legal entities such as corporations, partnerships, superannuation funds and trusts.

The TFN Rule is legally binding. A breach of the TFN Rule is an interference with privacy under the Privacy Act.

If a client file includes a tax file number (TFN), then the file must also include a written authority from the client for us to use the TFN.

We explain the legal basis and intended purpose for collecting the client's tax file number (for example, collecting the TFN as required under taxation legislation in order to provide the client with professional services connected with that legislation). We also make the client aware that declining to provide it is not an offence, as well as the consequences of not quoting the TFN.

This is because the tax file number is now required for a different and separate purpose.

We ensure that the TFN is protected by security safeguards to prevent unauthorised access, use or disclosure.

If we no longer require TFN information, we do not continue to hold it and we destroy it securely.

For example: if we collect TFN information from a client for the purpose of reporting that information to the Australian Tax Office, then after that report is made, the relevant TFN information is not retained. One way of achieving this is by 'blacking out' the TFN data in the relevant documents on file.

Unauthorised use or disclosure of a tax file number is an offence which carries significant penalties.

5.7 Privacy Officer

The Privacy Officer is to be familiar with the *Privacy Act 1988* (Cth) (Privacy Act) *the Privacy Amendment (Enhancing Privacy Protection) Act 2012*, Australian Privacy Principles, Eligible Data Breach Reporting Obligations and any supplementary guidelines issued by the OAIC.

The Privacy Officer, in addition to their normal duties, is responsible for:

- monitoring changes to privacy legislation as it applies to AD Advisory Services;
- suggesting changes to business practices, policies and procedures to maintain compliance with its privacy obligations;
- monitoring compliance with this procedure;
- providing or organising training on privacy awareness, practices and procedures;
- acting as the primary reference point for staff with queries about application of the privacy guidelines;
- managing and or facilitating AD Advisory Services' procedures with Representatives, allowing clients to access or correct their personal information;
- managing complaints and incidents/breaches in relation to privacy; and
- acting as the primary contact point for the OAIC.

5.8 Privacy Compliance Plan

The OAIC's Privacy Management Framework outlines steps for AD Advisory Services and its Representatives to take to meet ongoing obligations under the Australian Privacy Principles ('APP'). Annexure A outlines the Privacy Management Plan of AD Advisory Services.

5.9 Open and Transparent Management of Personal Information

Personal information must be dealt with openly and transparently by implementing practices, procedures and systems to ensure that licensees comply with obligations under privacy laws and appropriately handle any enquires or complaints about privacy. A clear and up to date Privacy Policy that documents managing personal information should include:

- the kinds of personal information that we collect and hold as an entity, and how we collect and hold it;
- the purposes for which we collect, hold, use and disclose personal information;
- how an individual can access the personal information about them that we hold, and if necessary, seek to have that information corrected;
- how we secure our clients' personal information, and ensure that it is protected from misuse, interference, or unauthorised access, modification or disclosure;
- how an individual can complain about a breach of the Australian Privacy Principles;
- whether we are likely to disclose personal information to overseas recipients, and, if so, the countries in which those recipients are likely to be located; and
- whether we are required to comply with the EU General Data Protection Regulations (GDPR), and, if yes, the way in which we comply with those obligations.
- Reporting serious breaches of the privacy laws to the OAIC and any affected individuals.

AD Advisory Services' Privacy Policy outlines how we manage our privacy obligations. Our Privacy Policy is available free of charge to anyone who asks for it, by either giving them a copy, sending it to them by post, email or if we have a web site, directing them to it.

5.10 Compliance with the Australian Privacy Principles (APPs)

Personal information is governed by the APPs. For a summary of the APPs please refer to Appendix 1 – Summary of Australian Privacy Principles.

The following sections outline AD Advisory Services' approach to compliance with the APPs, specifically with regards to clients' personal information, which has been identified as a higher compliance risk. However, the same principles apply to all personal information handled by AD Advisory Services. Where particular guidelines apply to a type of information other than client personal information, these are noted.

Collection

AD Advisory Services only collects the type of personal information about our clients which is described and included in our Privacy Policy.

When gathering information about a client, the information must be relevant for our purpose of providing financial services, as well as our obligation to comply with requirements imposed by law. For instance, questions about a client's job and income are directly relevant to their financial position, whereas in most circumstances, their religion or ethnic background is irrelevant. Details about religion, ethnic background, political beliefs, criminal record, trade union membership, and sexual orientation are all types of sensitive information for the purposes of the privacy legislation, and heightened obligations apply to the management of sensitive information. This is another reason to avoid collecting this information in the first instance.

AD Advisory Services has restricted the type of personal information its staff and Representatives can collect from clients through the use of standard client enquiry, profile, data collection, assessment and application forms. No additional personal information may be collected from clients unless expressly authorised to do so by the Privacy Officer. Client enquiry, profile and assessment forms are reviewed periodically to ensure that the information collected remains necessary and related to the primary purpose of collection.

At or before the time (or, if that is not practicable, as soon as practicable after) information is collected about clients, they must be made aware of the following matters:

- AD Advisory Services' identity and contact details;
- The fact that they can obtain access to the information;
- The purpose(s) for which the information is collected;
- The organisations (or types of organisations) to whom AD Advisory Services usually discloses the information (including related entities);
- Any law that requires the information to be collected; and
- The main consequences if the information is not collected.

For this purpose, a short statement has been included in AD Advisory Services' standard documentation. For example wording, refer to Appendix 2 – Collection Statement Handout.

AD Advisory Services does not collect personal information about a client from a third party unless it is unreasonable or impractical to collect it directly from the client. AD Advisory Services will endeavour to ensure that the person about whom the information is collected is aware of the above matters.

Collection from Third Parties
Only collect information from the client directly, unless it is unreasonable or impracticable to do so. If you need to collect information from someone other than the person to whom it relates, ensure that the person that the information is about is made aware of:

- The fact that their information has been collected;
- When and how this was done;
- Who provided their information to you; and
- Any additional matters set out in your Privacy Collection Statement.

Disclosing and providing information under the new reference checking protocols
AD Advisory Services ensures that we comply with ASIC Corporations and Credit (Reference Checking and Information Sharing Protocol) Instrument 2021/429 ('the Protocol') when employing/authorising representatives or responding to a reference request. Compliance with the Protocol is required when there are reasonable grounds to suspect that a prospective AFSL representative will provide personal advice to retail clients about relevant financial products. Similarly, the Protocol will also apply to prospective ACL representatives when there are reasonable grounds to suspect that the potential representative will provide credit assistance in relation to credit contracts secured by mortgages over residential property, and be a mortgage broker or a director, employee or agent of a mortgage broker.

As a 'recruiting licensee' we take reasonable steps to seek a written consent in the form set out in the Protocol from a prospective representative before we ask for a reference from a 'referee licensee'. If consent is refused, we cannot request a reference from a referee licensee under the Protocol. Consents will cease after 12 months it is given, or earlier if withdrawn. Information we obtain is handled consistently with the consent given and used only for:

- Considering a prospective representative's suitability for employment or authorisation, and
- Complying with the general conduct obligations of a licensee.

AD Advisory Services will address or making a request under the Protocol' in accordance with our 'Representatives Appointing Reference Checking and Reference Giving Policy'.

Disclosing client's information to Third Parties
When we disclose **personal information** of a client to a third party (e.g. accountant or lawyer), we will ensure that the third-party recipient signs a privacy agreement or acknowledgement whereby they agree to treat the personal information in accordance with the obligations set out in the privacy laws.

Sensitive information
In some circumstances, AD Advisory Services may need to collect sensitive information from third parties. Always obtain an individual's express consent when you collect or disclose sensitive information. Express consent to collect related sensitive information directly from those third parties must always obtained from clients. Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement. If given orally, consent must be confirmed in writing as soon as possible.

For a sample 'Letter of Authority to Access Information', that can be tailored for use and used as applicable, please refer to Appendix 6 – Declaration and Privacy Consents.

You must not collect sensitive information without consent unless:

- The collection is required by law; or
- It is reasonably necessary for one of more of our activities.

Always consult the Privacy Officer if you are unsure.

Unsolicited Information
If we inadvertently receive personal information (i.e., we do not solicit or directly collect it), we can only retain it and use it if it is information that we would have been permitted to collect in the first place – i.e., because we need it for the functions and services we provide.

Make an assessment of unsolicited information as soon as possible after you receive it. If we would not have collected it or it is not relevant to the services or functions, we provide, destroy it or de-identify it.

If in doubt, consult the Privacy Officer who will provide instructions on what to do with the unsolicited information.

5.11 Use and disclosure of personal information

Personal information should only be used or disclosed for the primary purpose for which it was collected.

It can be used or disclosed for secondary purposes, i.e., different purposes than the main purpose for which we collected the information, where:

- The secondary purpose is related to the primary purpose and the individual would reasonably expect us to use or disclose it for the secondary purpose. An indirect relationship is sufficient unless the information is sensitive information in which case the secondary purpose must be directly related to the primary purpose; or
- The individual has consented to the use or disclosure; or
- The use or disclosure is required by law or by order of a court or tribunal; or
- We have reason to suspect that unlawful activity has, is or may be engaged in and use of the information is a necessary part of our investigation of the matter or in reporting our concerns to the relevant persons or authorities; or
- It is necessary for the establishment, exercise or defence of a legal or equitable claim or the purposes of a confidential alternative dispute resolution process.

When in doubt whether the use or disclosure of information is appropriate, the matter must be referred to the Privacy Officer.

In no circumstances will AD Advisory Services trade, rent or sell personal information to a third party.

You must not provide personal information to anyone other than the organisations to whom the client has expressly or impliedly authorised us to provide it to.

It may be permissible to use or disclose information in some other unusual circumstances. If you want to use or disclose personal information for any reason other than those described above, or are in any doubt about our obligations, consult the Privacy Officer who will provide advice and/or obtain legal advice where necessary.

5.12 Data quality and security of information

AD Advisory Services must ensure that personal information it collects, uses and discloses is accurate, complete, up-to-date and relevant.

Due care is taken to keep it protected from misuse, interference and loss or from unauthorised access, modification or disclosure. When in doubt, AD Advisory Services will contact individuals to confirm that information they hold about them is accurate, complete and up-to-date.

Where possible, access is restricted to the Privacy Officer for correction requests and to preserve the integrity of the record of what has been collected.

The security measures used to protect information should be commensurate with its level of risk. As the amount of information and/or sensitivity increases, so should the steps you take to protect it. Ensure you are aware of the information you handle, where it is kept and the risks associated with it.

The Privacy Officer will regularly review the security of personal information and AD Advisory Services' document management and record keeping procedures. The Privacy Officer will assess whether information that is no longer required to comply with the law can be destroyed.

5.13 Data security

AD Advisory Services has adopted the following measures to protect the personal information it holds from misuse and loss, and from unauthorised access, modification or disclosure:

General

Before disclosing any personal information to a client, the identity of the client is confirmed to ensure that the person requesting the information is who they claim to be. This is done through industry-standard identification procedures, confirming basic personal details (e.g., full name, date of birth, address, phone number). Any requests for access

outside of *normal business activities* of AD Advisory Services and its representatives must be referred to the Privacy Officer, in accordance with section 5.15 below.

Physical security

- All premises, offices and filing cabinets containing paper-based personal information are locked overnight;
- Paper-based documents containing personal information that is no longer needed by AD Advisory Services are archived for seven years in a secure archive room before being securely destroyed by an outsourced service provider;
- Any document destruction bins, as well as any stored in an archive room, are locked overnight; and
- A 'clean desk policy' is encouraged throughout the organisation.

Computer and network security

Information stored on AD Advisory Services' computer systems can only be accessed by those entrusted with authority and computer network password. The information is regularly backed up in accordance with AD Advisory Services' Business Continuity including IT, Disaster Recovery and Succession Plan.

5.14 Openness

Prior to clients accessing or completing AD Advisory Services' client enquiry, profile/fact finder, and assessment forms we include a statement, or Representatives discuss with clients, how we handle clients' personal information (For sample wording see Appendix 2 — Collection Statement Handout EXAMPLES).

Any person asking for more information about AD Advisory Services' Privacy Policy, can be provided with a copy of its Privacy Policy, either hard copy or electronic form. This document, of which an example is included in Appendix 3 – Privacy Policy, explains to clients of how personal information is collected, used and disclosed, how it is kept secure and how it is made available for access or correction.

5.15 Access and correction of Personal Information

A client may seek details of personal information held about them and AD Advisory Services will respond within a reasonable period and where possible, allow access in the manner requested (e.g., send copies of records or allow the person to inspect them at our office). Any requests outside of '*normal business activities'* of AD Advisory Services and its representatives, should be referred to the Privacy Officer.

Before providing access, the Privacy Officer must confirm that the person requesting the information is who they claim to be, through thorough identification procedures.

The information may be provided by the most appropriate, cost-effective method, including:

- Letting the person inspect the information you hold and take notes of its content – however take care to ensure that they only see their own information;
- Letting the person view the information and provide an explanation of its contents;
- Providing a photocopy, fax or email of the information;
- Providing a printout of information held in electronic form; and/or
- Providing a summary of the information.

Particular care must be taken to ensure that personal information belonging to someone else is not inadvertently disclosed.

Timeframe

Requests for access will be acknowledged within 7 days and fulfilled within 7-14 days. More complex requests will be fulfilled within 30 days.

Correction of information will be actioned within 30 days of a request. Often this would occur after a person has requested access to their information.

Charges
AD Advisory Services will not generally charge for providing information. However, if the request is complex, the person requesting access could be charged the marginal cost of providing the access (e.g. staff costs of locating and collating information, reproduction costs, photocopy charges and the cost of having someone explain information etc.). The person should be notified that there would be a cost related to the access at the time of acknowledging the request for access and obtain their permission to incur costs prior to doing so.

Refusing access
You must allow them access unless:

- You reasonably believe it would pose a serious threat to life, health or safety;
- It would have an impact on the privacy of others;
- The request is frivolous or vexatious (i.e. trivial), made to pursue an unrelated grievance against us or is a repeated request for the same information;
- The request relates to existing or anticipated litigation or access would prejudice your position in respect of a negotiation (seek legal advice if you think this may apply);
- You are legally obliged to refuse access (seek legal advice if you think this may apply);
- You have reason to suspect unlawful activity or serious misconduct access would be likely to prejudice the taking of appropriate action;
- Access would be likely to prejudice enforcement related activities; or
- Would reveal commercially sensitive information.
- The information relates to existing or anticipated legal proceedings against us by the person and the information would not be discoverable in those proceedings;
- Provision would reveal our intentions in negotiations with the person in such a way as to prejudice the negotiations; or
- It is unlawful to provide access, the law permits or requires access to be denied or it would prejudice the activities of enforcement bodies.

The Privacy Officer will assess whether access should be refused.

If we do refuse to allow access, we will explain our reasons for doing so in writing and include information about AD Advisory Services' privacy complaints process in the communication.

Before providing access, AD Advisory Services will:

- check what particular information the person wants to ensure that we are not providing more than is required; and
- confirm that the person requesting the information is who they claim to be.

Correcting personal information
If it is found that the information held in AD Advisory Services' records is inaccurate, incomplete, out of date, irrelevant or misleading, then it will be corrected. If a client asks AD Advisory Services to correct any information, we will do so within a reasonable period and AD Advisory Services will not charge for correcting information.

On receipt of a request for correction:

- Check what particular information the person wants to correct and identify where it is stored;
- Confirm that the person requesting the information is who they claim to be by **[USER NOTE: Describe your procedures for verifying a person's identity]**; and
- Update the information accordingly.

Often this will occur after a person has requested access to their information. However, if the records are inaccessible and/or no longer required, the information will be destroyed or de-identified.

Timeframe
Requests for correction of information will be acknowledged within 7 days and corrected within 7-14 days. More complex requests will be fulfilled within 30 days.

If you are asked to notify the correction to others who have received the person's personal information (i.e. other companies we deal with), do so immediately unless it is impracticable or unreasonable to so do.

AD Advisory Services cannot charge for correcting information.

Refusing access
We may refuse to correct personal information if we do not agree that it is inaccurate, out of date, incomplete, irrelevant or misleading.

The Privacy Officer will decide whether a correction request should be refused. Refer any correction request to the Privacy Officer if you believe we may have grounds to do so.

If we do not agree that information needs to be corrected, we must provide written reasons for our refusal and tell the person who submitted the request about our procedures for making a privacy related complaint. If requested, we must also attach a statement to the information we hold (e.g., to the client file) which notes that the client believes it is out of date, incomplete, inaccurate, irrelevant or misleading.

The Privacy Officer must approve all correction refusals before they are communicated to the person who has made the request.

Give reasons
Reasons for denial of access or refusal to correct information should be given to the person, under the supervision of the Privacy Officer. However, this would not be required where such a disclosure would prejudice an investigation against fraud or other unlawful activity.

5.16 Identifiers

AD Advisory Services or its Representatives may collect tax file numbers (TFNs) or other government identifiers (e.g.: Medicare or drivers licence number) where it is necessary for the provision of our services, assessment or other verification purposes, identification, insurance or lenders requirements. We only collect the identifiers to provide our services to clients and will not adopt as our own any identifiers that the client may provide to us.

When you collect a client's TFN, you must:

- Only collect the TFN where it is necessary and relevant;
- Tell the client the reason why you are collecting the TFN and that it is not an offence to refuse to provide a TFN;
- Take reasonable steps to ensure the manner of collection does not unreasonably intrude in the client's affairs; and
- If it is necessary to retain client tax file numbers, ensure that you obtain consent in writing from the client, keep the files in a lockable secure area and restrict access to TFN only to staff who need to access the information.

In addition, we must not use or disclose a person's government related identifier unless:

- It is reasonably necessary for us to do so to verify the person's identity or fulfil our obligations to a government agency or authority;
- It is required or authorised by law;
- We have reason to suspect that unlawful activity has, is or may be engaged in and use of the information is a necessary part of our investigation of the matter or in reporting our concerns to the relevant persons or authorities;
- We have reason to believe that it is reasonably necessary for enforcement related activities conducted by an enforcement body.

If we receive any documents with a government related identifier on it (such as a copy of a drivers licence, passport, Medicare card, Centrelink statement or tax return), and we do not need it, we must redact (i.e. black out) the identifier so that it is no longer identifiable.

Use or Disclosure – Do not use or disclose a client's TFN for any purpose other than the legal purpose for which it was obtained or for the purpose of giving the client information we hold about them (e.g. responding to an access request).

Storage and Destruction – If a client's TFN is collected, or incidentally appears on documents we obtain, we must:

- Protect it from misuse, loss and unauthorised access, use, modification and disclosure; and
- Ensure that access to records containing it is restricted to people who need to access it for the legal purpose for which it was collected.

If we do not need a TFN either because we did not request it or it is no longer required by law or for the legal purpose for which it was collected, we must take reasonable steps to securely destroy or permanently de-identify it (e.g. with permanent white-out, black ink or similar).

Best practice client file security must be employed to protect TFN information.

Staff training – We ensure that staff are aware of the need to protect privacy when handing TFNs. We do so by ensuring that all staff who collect or access TFNs are aware of:

- The circumstances in which they can be collected; and
- Prohibitions on their use and disclosure.

5.17 Anonymity

Clients may wish to remain anonymous when dealing with AD Advisory Services; however, in these circumstances, AD Advisory Services may not be able to provide them with the product or service required.

5.18 Cross border data flows

Cross Border Disclosure – If we provide personal information to an overseas recipient we need to take reasonable steps to ensure that they will not breach the Australian Privacy Principles unless:

- They are subject to a law which provides similar protection to the Australian Privacy Principles and the individual whose information is being disclosed can enforce that law;
- The individual has consented to the disclosure and agreed that our cross-border disclosure obligations will not apply; and/or
- The disclosure is authorised by law.

We must obtain written agreement (or acknowledgement of service providers) to AD Advisory Services that overseas recipients of personal information comply with the Australian Privacy Principles.

If AD Advisory Services needs to send personal information overseas, it must take reasonable steps to ensure that the recipient doesn't breach the Australian privacy laws - AD Advisory Services can be liable if they do.

There are 3 acceptable options for managing this risk.

Option 1 – Informed Consent
Seek the client's consent to send their information to the overseas recipient on the understanding that:

- AD Advisory Services or you, the Representative, will not be accountable for the recipient's breach of Australian privacy laws; and
- They, the client, will not be able to seek redress under those laws.

The consent must be active and voluntary, e.g. via a signature/acceptance of terms from the client acknowledging their consent to send their information to the overseas recipient.

Option 2 – Similar Law
Satisfy yourself that the international recipient is subject to similar laws to the Australian privacy regime and that the client can easily enforce their rights without undue cost.

AD Advisory Services might need legal advice on the comparability of the overseas law to use this option.

Option 3 – Reasonable Steps
Put a legally binding agreement in place with every overseas business to whom AD Advisory Services sends personal information requiring them to:

- Warrant that they will comply with the Australian privacy laws and will require third parties (e.g. their contractors) to do the same;
- Only use the personal information AD Advisory Services sends them for the purposes AD Advisory Services specifies;
- Implement a data breach response plan which includes notifying AD Advisory Services of and remedying any suspected data breach;
- Allow AD Advisory Services to monitor their compliance; and

- Indemnify AD Advisory Services (and your clients) if they breach the Australian privacy laws.

5.19 Tax Relevant Providers and Privacy Consent

Representatives who are qualified tax relevant providers and provide tax (financial) advice services, as regulated by Treasury, must obtain a client's permission to disclose any information relating to the client's affairs to a third party, unless the Representative has a legal duty to disclose the information.

This applies to all information relating to a client's affairs – not just personal information.

It also applies to the disclosure of client information to any third party. Some examples of ways you may disclose client information to third parties that require disclosure are:

- Storing client data in a data centre or in the cloud, or your planning software stores client data in the cloud;
- Using marketing apps to measure client engagement;
- Using electronic signature solutions; and
- Providing client information to related businesses, like subsidiaries or overseas branches, that operate as separate legal entities.

Whether Representatives must obtain the express, rather than implied, consent of clients to their information being disclosed to third parties is a grey area because 'permission' is not defined in the TPB Code of Professional Conduct for tax relevant providers. They do suggest "*This permission may be by way of a signed letter of engagement, signed consent or other communication with the client."*

Representatives should obtain the express consent from clients i.e. a positive step from the client to authorise the disclosure such as an 'opt-in' or signed consent. The ideal time to do this is early on in the relationship. This should include information about how you will use and disclose your client's information in your client engagement letter, fact find, a privacy consent form or other onboarding documents. You can do this by placing the 'Privacy Collection Statement' in the relevant document. You should discuss it with your client and ask them to give their consent by signing the document.

To ensure you comply with both the Privacy Act and the TPB Code, you need to identify all the third parties you disclose client information to and make sure they are described in your consent document. Ideally, you would tell your client each and every third party you are disclosing their information to, but this can be complex and lengthy. It is sufficient to provide a generic description of the types of businesses you may provide their information to.

5.20 Privacy Breaches

A privacy breach occurs if we hold personal information about an individual and breach:

- Our legal obligations in relation to its collection, handling, storage or disclosure; or
- The provisions in these Privacy Management Procedures.

A data breach occurs when personal information is accessed or disclosed in an unauthorised way or is lost.

A data breach could occur in a number of ways. Some examples include:

- a mobile phone, laptop or removable storage device containing personal information is lost or stolen;
- sending an email containing personal information to the wrong recipient;
- accessing or disclosing personal information outside the requirements or authorisation of their employment;
- databases or an email account containing personal information are 'hacked' into or otherwise illegally accessed by an individual;
- a client file is lost or stolen;
- paper records are stolen from insecure recycling or garbage bins.

When you identify an actual or possible privacy breach, report it to the Privacy Officer immediately.

If we act quickly and manage the breach to ensure that it will not cause any serious harm to an individual, we may not be required to report a Notifiable Data Breach (NDB).

5.21 Eligible Data Breaches

When an 'eligible data breach' occurs, under the NDB scheme, we must usually report it to the OAIC and affected individuals within strict timeframes. This may not be required if we act quickly to manage the breach and ensure that it will not cause any serious harm to an individual.

A privacy breach is an eligible data breach if it results in:

- Unauthorised access to or disclosure of personal information; or
- Information being lost in circumstances where unauthorised access to or disclosure of personal information is likely to occur, and this is reasonably likely to result in serious harm to an individual.

Where there is a reasonable suspicion that an eligible data breach has occurred, but there is not enough information to have reasonable grounds to believe that there has been an eligible data breach considering all the circumstances, AD Advisory Services' Privacy officer must carry out a 'reasonable and expeditious assessment'. AD Advisory Services must take reasonable steps to ensure that this assessment is completed within 30 days of AD Advisory Services becoming aware of the grounds of suspicion.

Refer to the 'Incidents and Breach Reporting Policy' which includes our Data Breach Response Plan.

5.22 What is serious harm?

Serious harm can be caused by a data breach and can include identity theft and serious physical, psychological, emotional, financial or reputational harm.

Some kinds of personal information breaches are more likely than others to cause serious harm. Serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm. For example, theft of personal information, such as, Medicare, drivers licence or passport or financial information). Combinations of different types of personal information (as opposed to a single piece of information) may be more likely to result in serious harm.

If an eligible data breach involves personal information that you and another organisation hold on file by any means (e.g. an outsourced service provider or joint venture partner), only one of us needs to assess and report the breach to the OAIC and affected individuals. If no-one undertakes the assessment or makes the report, we could both be liable for a breach of the requirements.

As a general rule, the entity that has the most direct relationship with the affected individual(s) should report the breach. However, it is AD Advisory Services policy that you must advise the Privacy Officer of any incidents or breaches.

AD Advisory Services ensures that its service and other relevant contracts include provisions:

- Requiring compliance with the data breach reporting regime;
- Requiring the other party to notify you and in turn you notifying AD Advisory Services if there is a privacy breach and cooperate with any investigation and remediation you undertake; and
- Setting out who is responsible for assessing and reporting data breaches.

5.23 When does a Data Breach become an eligible Notifiable Data Breach (NDB)?

Notification obligations are triggered when AD Advisory Services has reasonable grounds to believe that there has been a data breach that results in an eligible data breach. This can apply when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach. See 5.24 below.

5.24 Data Breach Response Plan

Our Privacy Officer will investigate and deal with privacy breaches in accordance with our 'Incidents and Breach Reporting Policy' which includes our Data Breach Response Plan. See the Incidents and 'Breach Reporting Policy' for further details. When we notify clients of a notifiable data breach, we will provide recommendations about steps that the client can take in response to the breach and or to contain the breach.

5.25 Complaints Handling and Incident Reporting

Should a client raise a complaint or issue that relates to the privacy of their personal information, the Privacy Officer will directly deal with the matter and seek to resolve it in accordance with AD Advisory Services' Complaints Handling Procedure. Should the matter be unable to be resolved, it may be referred to the OAIC. This process will also be followed for complaints made in response to a cyber security incident.

Incidents or breaches that relate to privacy must be referred to the Privacy Officer who will handle the matter in accordance with AD Advisory Services' 'Incident and Breaches Policy' and with consideration to the Guide to Handling Personal Information Security Breaches, published by the OAIC, which provides general guidance on the key steps and factors for organisations to consider when responding to a personal information security breach.

5.26 Privacy Consent Forms

The following appendices contain various privacy consent forms and checklists for use by AD Advisory Services, and its Representatives as applicable, to comply with privacy requirements when assisting clients:

- Appendix 4 – Letter of Authority to Access Information
  - For a 'Letter of Authority to Access Information' that is a client's 'express consent', example template, for a third party to release information.
- Appendix 5 – Privacy Access Request Refusal Letter
  - For a 'Privacy Access Request Refusal Letter', example template letter Refusal to access personal information.
- Appendix 6 – Declaration and Privacy Consents by client(s).
  - For obtaining client consent to collect, access, use, hold, disclose and release personal information generally.
- Appendix 7 – Verbal Privacy Consent Checklist
  - For discussing matters with a client that need to be discussed and documented when obtaining 'verbal consent', over the phone, to collect and hold personal information.
- Appendix 8 – Representatives Privacy Checklist
  - For matters that need to be included in a Representatives client file check list.

Applicable consent form(s) are to be tailored appropriately and completed in full to be effective to release or act on any instructions contained within the consent form.

Consent forms are to be appended to the client file with scanned copies sent to other professionals where required (e.g. other financial service providers, credit providers, credit reporting agencies and debt collection agencies, insurance companies, or insurance reference services).

5.27 Monitoring and supervision

The Privacy Officer is responsible for monitoring compliance with this Procedure.

AD Advisory Services' compliance review programme includes monitoring compliance with this Procedure and our Privacy Policy, periodic consideration of new privacy risks and the adequacy of existing privacy practices and procedures.

To ensure that our staff and Representatives are aware of our Privacy Policy, obligations and these Privacy Procedures (including our Data Breach Response Plan), we include a privacy component in our induction and compliance refresher training. Staff also receive on the job training as and when required.

6. Approval and Review

The Director must approve this Procedure and the Privacy Policy and is responsible for updates and circulation ensuring that Representatives, employees, consultants and any outsourced providers of AD Advisory Services are aware of, and understand, the requirements of this Procedure, as applicable to them.

The Compliance Manager will review this Procedure annually (including our Data Breach Response Plan which is included in our Incident and Breach Reporting Policy) or as required by legislation or regulatory changes, or if there are systemic problems within AD Advisory Services to ensure that they remain effective and up to date.

Open and transparent management of personal information
We will manage personal information, including financial and credit information, in an open and transparent manner. In doing so, we ensure that individuals are notified at the time of collecting their personal information of:

- what type of personal information is being collected;
- who that personal information will be disclosed to; and
- how we use that personal information.

We have appointed a Privacy Officer, who will deal with any queries regarding access to or correction of personal information or any privacy related complaints. We ensure all our employees are trained at regular intervals to ensure they understand our obligations under the Privacy Act, including the Australian Privacy Principles.

We regularly update our privacy policy and will provide a copy of our privacy policy free of charge on request and in a suitable format.

Anonymity and pseudonymity
Generally, due to the nature of our services, we are not able to deal with customers who do not wish to identify themselves. However, where possible and appropriate we will provide information of a general nature to unidentified individuals.

Collection and use of personal information
We collect personal information for the following purposes:

- providing individuals with the products or services they have requested from us, our related entities and or referral partners;
- managing our relationship with individuals;
- protecting individuals and ourselves from error or fraud; or
- complying with regulatory requirements.

Where possible, we collect personal information directly from the individual.

We may collect sensitive information from individuals when they apply for an insurance related product.
We only collect sensitive information directly from the individual and with the individual's consent.

We may also collect sensitive information when it has been provided as part of a loan application. Any sensitive information that is collected in this way is only used for the purpose for which it is provided, and is collected with the individual's consent.

Unsolicited personal information
If we receive unsolicited personal information we will determine whether we could have collected that personal information by lawful and fair means, and whether it is related to one of the purposes of collecting personal information above. We will do this by looking at our relationship with the individual and whether the personal information relates to our relationship with them.

If we could not have collected the personal information by lawful and fair means, or the personal information does not relate to one of our purposes for collecting the personal information, we will destroy the personal information.

Notification of the collection of personal information
When we first collect personal information from an individual we will notify them that we have collected their personal information. We will require the individual to sign a notification and consent form detailing how we will use and disclose their personal information.

This notification will provide the individual with information about:

- the purposes of the collection of their personal information and credit information;
- those entities that we usually disclose personal information or credit information to;
- what happens if the individual chooses not to provide us with personal information;
- direct marketing that may be undertaken by us or any related companies;

- when we are required to collect personal information under an Australian law, such as the *Corporations Act* (Cth) 2001, *National Consumer Credit Protection Act* (Cth) 2009 or the *Anti-Money Laundering and Counter Terrorism Financing Act* (Cth) 2006;
- our privacy policy and where it can be found; and
- any disclosure of personal information that we make to an overseas entity.

If we know that as part of our relationship with the individual we will disclose their personal information to another identifiable entity, such as a specific lender, we will notify the individual of the following matters at the time we first collect their personal information:

- the identity and contact details of that organisation; and
- why their information may be disclosed to the organisation.

Use and disclosure of personal information
The purpose of collecting an individual's personal information will be outlined in the notification and consent received by the individual.

If during our relationship with the individual we wish to use an individual's personal information for an additional purpose, we will obtain their consent unless the purpose is related to the primary purpose or we are permitted under law to do so.

Direct marketing
We notify individuals at the time of collecting their personal information that their personal information will be used by us and any associated businesses for the purposes of direct marketing.

In all our direct marketing communications we will provide a prominent statement about how an individual can elect not to receive direct marketing. If the direct marketing communication is an email we will provide an 'unsubscribe' function within the email.

We will keep appropriate records to ensure those individuals that have made requests not to receive direct marketing communications do not receive them. We do not apply a fee to unsubscribe from direct marketing communications.

We do not sell personal information. We do not use sensitive information for the purposes of direct marketing.

If we purchase personal information for the purposes of direct marketing we will conduct appropriate due diligence to ensure appropriate consents from the individuals have been obtained.

Cross-border disclosure of personal information
If AD Advisory Services, or its Representatives, needs to send clients' personal information overseas, it must take reasonable steps to ensure that the recipient does not breach the Australian privacy laws.

We may use cloud storage and IT servers that may be located overseas to store the personal information we hold.

Adoption, use or disclosure of government related identifiers
We do not generally use government related identifiers to identify individuals.

We may receive tax file numbers and only disclose these to relevant financial service and credit service providers for the purpose for which they were supplied.

Quality of personal information
We rely on individuals to help us to ensure that their personal information is accurate, up-to-date and complete.

If we become aware that personal information is inaccurate, out-of-date or incomplete, such as when mail is returned, we will update our systems accordingly.

Security of personal information
We hold personal information on secure IT systems. All IT systems are appropriately updated with passwords, virus scanning software and firewalls when needed.

Any paper records are only accessible to employees and others as they are needed. Any paper records are held within an office that is locked and security protected at night.

We will usually destroy personal information that is held electronically and in paper form seven years after our relationship with the individual ends. We will do this by shredding paper copies and deleting electronic records containing personal information about the individual or permanently de-identifying the individuals within those records.

Access to personal information
Individuals may request access to any personal information that we hold about them. We will not charge an individual for requesting access to their personal information.

We will verify the individual's identity prior to disclosing any personal information.

When an individual requests access to their personal information we will conduct a search of our customer relationship database. This search will also indicate if there are any paper records that contain personal information.

We will not give access to the personal information that we hold about an individual where it is unreasonable or impracticable to provide access, or in circumstances where the request would likely:

- pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- unreasonably access the privacy of other individuals;
- be frivolous or vexatious;
- relate to anticipated legal proceedings, and the correct method of access to personal information is by the process of discovery in those legal proceedings;
- reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- be unlawful or in breach of an Australian law;
- prejudice the taking of appropriate action in relation to a matter where unlawful activity or misconduct that relates to our functions or activities;
- prejudice an enforcement related activities of an enforcement body (such as ASIC, the OAIC or AUSTRAC); or
- reveal commercially sensitive information.

When we receive a request for access we will usually respond to the individual with 7 days. Depending on the nature of the request we may be able to provide the personal information at the same time as when the request is made.

If the individual is requesting a large amount of personal information or the request cannot be dealt with immediately, then after we have investigated the request for access we will advise the individual what personal information we hold and provide details of that personal information.

We will comply with all reasonable requests by an individual to provide details of the personal information that we hold in the requested format.

If we do not provide access to the information we will provide written reasons setting out why we do not believe we need to provide access. We will also advise the individual they can access our Internal Dispute Resolution (IDR) and External Dispute Resolution (EDR) schemes if they are dissatisfied with a decision not to provide access to personal information. Please see our **Privacy Access Request Refusal Letter** below for our template.

Correction of personal information
If we hold personal information about an individual and we are reasonably satisfied that the information is inaccurate, out of date, incomplete, irrelevant or misleading, or we receive a request to correct the information, we will take reasonable steps to correct the information.

If we correct any personal information that we have previously disclosed, we will take reasonable steps to notify the entity to which we disclosed the information of the correction. We may not always make corrections to an individual's personal information. When we do not make requested corrections, we will provide reasons for our refusal to make the correction and provide details of our IDR and EDR procedures.

If after notifying the individual of our refusal to correct personal information, the individual requests us to issue a statement on the record that contains the personal information, we will take reasonable steps to do so.

Appendix 1 – Summary of the Australian Privacy Principles

Personal information is governed by the Australian Privacy Principles (**APPs**). The following is a brief summary of the APPs. This summary does not replace reading the APPs in full, which can be accessed at the web site of the Office of the Australian Information Commissioner at www.oaic.gov.au.

APP1: Have a privacy policy which is available free of charge, and which should be displayed on a website. The over-riding obligation is to manage *personal information* in an open and transparent way, so that individuals know how their *personal information* will be used.

APP2: If practical, deal with customers on an anonymous basis.

APP3: Only collect *personal information* that is reasonably necessary.

APP4: *Personal information* that is received without a request must be destroyed unless it could have been collected under APP3.

APP5: As soon as practical before or after collecting *personal information* provide prescribed information about how the information will be used. This is what the Privacy Consent and your Privacy Policy does.

APP6: Use *personal information* only for the particular purpose for which it was collected unless the individual consents or would reasonably expect the use for another purpose.

APP7: Only direct market if the individual would reasonably expect it, has consented, or it is impracticable to obtain that consent. Messages must provide a way to opt out.

APP8: Only disclose *personal information* overseas if you have verified that the overseas entity will not breach the APPs, is subject to similar laws as the APPs, or the individual consents.

APP9: Do not use government identifiers, such as tax file numbers.

APP10: Take reasonable steps to ensure that *personal information* is accurate, up to date and complete.

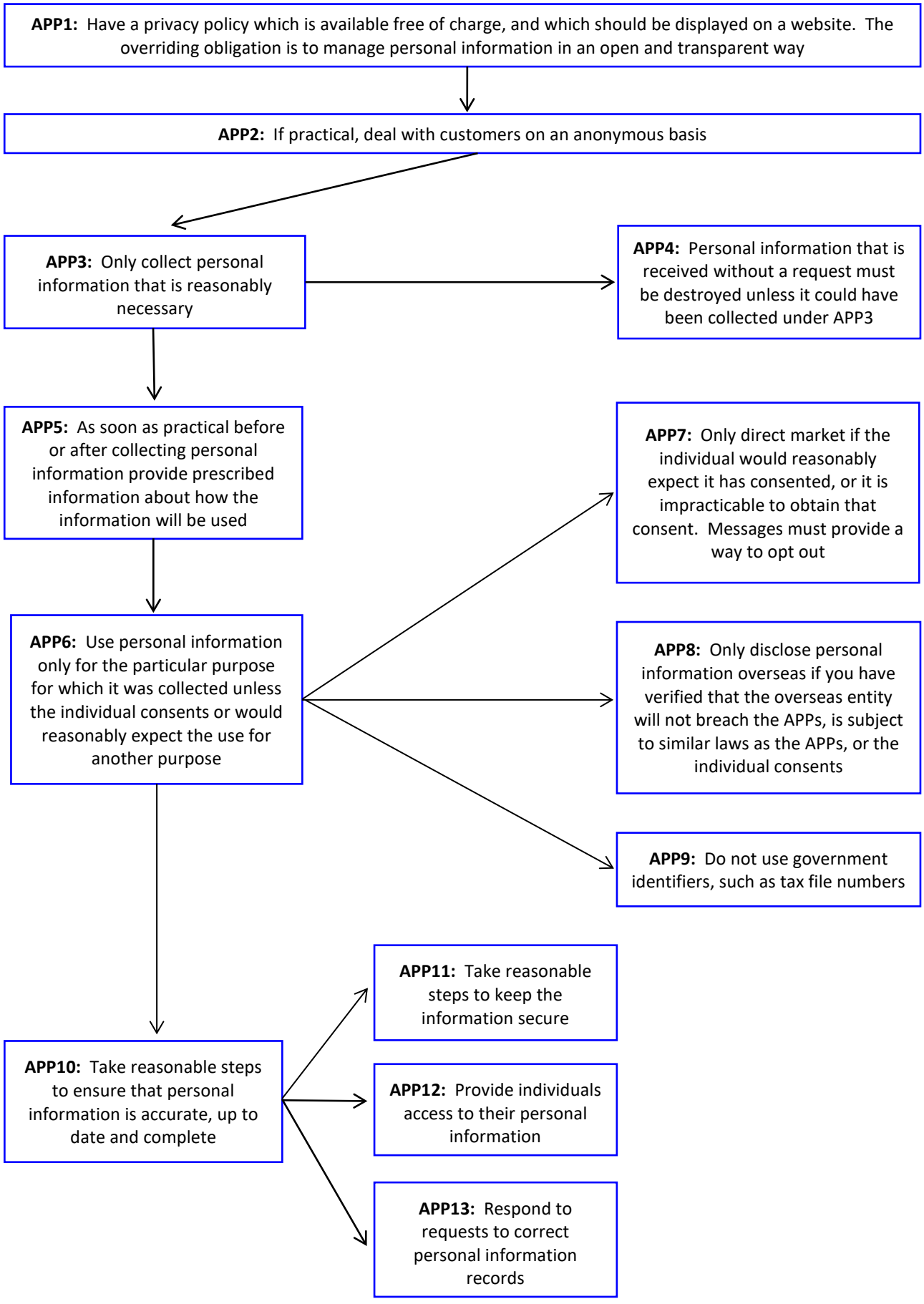
APP11: Take reasonable steps to keep the information secure.

APP12: Provide individuals access to their *personal information*

APP13: Respond to requests to correct *personal information* records.

Please see Table 1 on the next page for an Australian Privacy Principles flow chart.

Table 1 – Australian Privacy Principles Flow Chart



Appendix 2 – Collection Statement Handout *EXAMPLES*

[**User Note**: **This is an example document; it is not necessarily definitive or tailored for your use. Instructions for use:** *The 'Privacy Collection Statement' contains the information that needs to be provided at or before you collect personal information. It, or similar wording, needs to be incorporate into your initial disclosure document(s) (e.g., Letter of Engagement, Disclosure Documents, Offer Documents etc.) or your first correspondence with any person about whom you collect personal information. The Statement may need to be customised for each collection. Ensure the Statement is available across different channels, is easy to understand, and is specific for the user experience].*

On Web Pages:

PRIVACY COLLECTION STATEMENT

At <insert website url> we are committed to protecting your privacy. We use the information you provide to advise about, deal in and assist with your financial affairs. This may include information collected from third parties such as <insert the types of third parties from who you collect information, e.g., AML ID collection and verification providers, your bank, accountant, superannuation fund>. If you don't provide us with full information we request, we can't properly advise or assist you with your financial affairs. We provide your information to financial service providers or other companies with whom you choose to deal (and their Representatives) and our related entities. We do not trade, rent or sell your information.

We may disclose your information to recipients in the United States of America for the purpose of required transaction notifications (E.g. Form W-8 BEN). We may also store your information in the 'cloud' for the purposes of data storage, file backups and or attending to your affairs. These 'cloud' service providers may be in countries not regulated by laws, which protect your information in the way that is similar to the Privacy Act. If a recipient is not regulated by laws, which protect your information in a way that is similar to the Privacy Act, we will seek your consent before disclosing your information to them. When we recommend a provider to you, we will provide you with their disclosure statement which will outline to you their privacy policy. We will not be accountable for any recipient's breach of Australian privacy laws and you will not be able to seek redress under those laws.

User Note: If you do direct marketing, include the following: From time to time, we may use your contact details to send you offers, updates, articles, newsletters or other information about products and services that we believe will be of interest to you. We may also send you regular updates by email or by post. We will always give you the option of electing not to receive these communications and you can unsubscribe at any time by notifying us that you wish to do so.

Our Privacy Policy contains more information about how to access and correct the information we hold about you and how to make a privacy related complaint, including how we will deal with it. Ask us for a copy by contacting us or visiting our website.

In Licensee Documentation:

PRIVACY COLLECTION STATEMENT

At AD Advisory Services Pty Ltd, we are committed to protecting your privacy. We use the information you provide to advise about, deal in and assist with your financial affairs. This may include information collected from third parties such as <insert the types of third parties from who you collect information, e.g., AML ID collection and verification providers, your bank, accountant, superannuation fund>. If you don't provide us with full information we request, we can't properly advise or assist you with your financial affairs. We provide your information to financial service providers or other companies with whom you choose to deal (and their Representatives) and our related entities. We do not trade, rent or sell your information.

We may disclose your information to recipients in the United States of America for the purpose of required transaction notifications (E.g. Form W-8 BEN). We may also store your information in the 'cloud' for the purposes of data storage, file backups and or attending to your affairs. These 'cloud' service providers may be in countries not regulated by laws, which protect your information in the way that is similar to the Privacy Act. If a recipient is not regulated by laws, which protect your information in a way that is similar to the Privacy Act, we will seek your consent before disclosing your information to them. When we recommend a provider to you, we will provide you with their disclosure statement which will outline to you their privacy policy. We will not be accountable for any recipient's breach of Australian privacy laws and you will not be able to seek redress under those laws.

User Note: *If you do direct marketing, include the following*: From time to time, we may use your contact details to send you offers, updates, articles, newsletters or other information about products and services that we believe will be of interest to you. We may also send you regular updates by email or by post. We will always give you the option of electing not to receive these communications and you can unsubscribe at any time by notifying us that you wish to do so.

Our Privacy Policy contains more information about how to access and correct the information we hold about you and how to make a privacy related complaint, including how we will deal with it. Ask us for a copy by contacting us.

Appendix 3 – Privacy Policy *EXAMPLE*

[**User Note**: **This is an example document**, including but not necessarily limited to, matters that need to be included in your Privacy Policy. **It is not necessarily definitive or tailored for your use**. Modify, as with all templates, for your specific business use. Also, look out for OAIC and other industry bodies requirements and updates, basis Codes and other Regulations or Legislation changes that occur from time to time. Delete this User Note, once you have tailored the document for your specific use.]

Privacy Policy

1. Introduction

AD Advisory Services Pty Ltd (referred to as 'AD Advisory Services', ***we***, ***our***, ***us***) ACN 005 830 802, are 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, AD Advisory Services 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, AD Advisory Services will comply with the terminology and wording used in the APPs, and this will constitute AD Advisory Services' compliance with the equivalent obligations in the GDPR.

If the GDPR imposes an obligation on AD Advisory Services that is not imposed by the APPs, or the GDPR obligation is **more onerous** than the equivalent obligation in the APPs, AD Advisory Services will comply with the GDPR (see Appendix 9).

All third parties (including clients, suppliers, sub-contractors, or agents) that have access to or use personal information collected and held by AD Advisory Services, must abide by this Privacy Policy and Collection Statement (**Privacy Policy**).

AD Advisory Services makes this Privacy Policy available free of charge and can be downloaded from its website [insert details].

In this Privacy Policy:

- ***Disclosure*** of information means providing information to persons outside of AD Advisory Services;
- ***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 AD Advisory Services for questions or complaints regarding AD Advisory Services' 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 AD Advisory Services.

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: [**User Note:** Amend this section to include all of the personal information that you collect and hold about individuals.]

- name;
- address;
- phone numbers;
- email addresses;
- occupation;
- bank account details;
- driver's licence and or passport 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 AD Advisory Services 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
- third parties with whom we come into contact.

[**User Note: expand this list**, if appropriate for your business, to include any other individuals about whom you will collect personal information, then delete this user note and the grey highlights.]

6. Website collection

We collect personal information when we receive completed online generated forms from our website [**User Note**: insert website details]. 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 [**User Note:** insert your method for how people should opt out of their information being collected via cookies, e.g. '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 [**User Note:** insert *our website/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 enables our website to recognise your browser and capture and remember certain information. This includes facilitating your use of [**User Note:** insert details of what the information collected by the cookies is used for].

We also use cookies to [**User Note:** insert details of any additional use of analytics and cookies, e.g. 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].

We will delete all data obtained through cookies every [**User Note:** insert text].
[**User Note:** Delete this paragraph if you do not use website analytics. Check with your analytics provider (e.g. Google Analytics) on what disclosure you must make here. Google Analytics has a link that it allows partner sites to use in their privacy statements.] 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.

[**User Note**: Delete this box if you are not required to comply with the GDPR – see Appendix 9] 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 [OK].

[**User Note**: The user must 'opt in' to the use of cookies, so there should be a button or a function such as [OK] for the user to opt in.]

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;
- [**User Note**: include any other purposes for which you collect personal information, e.g. a financial planner may collect and hold personal information to assist in providing wealth management, financial planning, personal risk 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.

8. Who might we disclose personal information to?

We may disclose personal information to:

- a related entity of AD Advisory Services;
- 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
- [**User Note**: include any other recipients you are likely to disclose personal information to].

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

[**User Note:** This section should set out whether you are likely to send information overseas, and, if yes, details of who it is sent to, where it is sent and the procedure that it follows to ensure compliance with the Act.]

[**User Note:** If you do not disclose personal information overseas, delete this section and state:]
We do not disclose personal information overseas.

[**User Note:** If you do disclose information to overseas recipients, insert the following paragraph:]
We may disclose personal information to [insert the details of types of recipients to whom you will disclose personal information, and where those recipients are located outside of Australia (e.g., related entities, suppliers). (Please note that if you use cloud computing, you are likely to be disclosing information to overseas recipients.)] that are located outside Australia in some circumstances. These recipients may be located in the following countries:

- [**User Note**: **insert countries**. If it is not practical to specify all of the countries where information could be disclosed, you should list 2 or 3 countries where information is likely to be disclosed, and then insert wording to the effect that 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 [insert 2 or 3 countries].]

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: [**User Note**: Please amend the list of security controls as appropriate for your business.]

- 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: [**User Note:** Please amend as appropriate for your business.]

- 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 AD Advisory Services' 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 complaints handling process in place to manage privacy risks and issues. [**User Note**: You will need to include additional details about your complaints handling process – either link to a document explaining it, or set out a summary.]

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 – [insert details]
- emailing – [insert details]

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 Ac*t. 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.

21. Acknowledgement

[**User Note:** This section needs to appear where the customer enters their information as part of the onboarding process. Also, it must be included before the customer enters any personal information into a form. Also, please ensure that this entire section appears in both online and hard copy versions of the Privacy Policy.

Also, each of the boxes in this section must be ticked by the customer before the customer's application proceeds.

We also note that before the customer can tick the 'agree' box, or press a button that says 'agree', you should require them to open the Client Agreement and scroll to the bottom. This is known as the 'click wrap' method and is more likely to be enforced by a court than simply allowing a customer to tick the box without opening the agreement.]

☐ I have read AD Advisory Services' (**you, your**) **Privacy Policy and Collection Statement** located here [insert hyperlink], and the **Website Terms and Conditions** located here. [insert hyperlink]

☐ I consent to you **collecting sensitive information about me** for the purposes of you providing services to me.

☐ I consent to you **sending my personal information to the recipients located outside Australia** as described in the Privacy Policy and Collection Statement.

☐ I agree to receive information about your **products, services or promotions**.

☐ By proceeding to use our services, you agree that you fully understand and agree to be bound by the terms and conditions contained in our Client Agreement. If you would like to clarify anything, please contact us or consult an adviser.

Appendix 4 – Letter of Authority to Access Information *EXAMPLE*

[**User Note**: **This is an example document**, including but not necessarily limited to, matters that need to be included in an express consent to collect personal or sensitive directly from a third party **It is not necessarily definitive or tailored for your use**. Modify, as with all templates, for your specific business use. Also, look out for OAIC, other industry bodies requirements and updates, basis Codes and other Regulations or Legislation changes that occur from time to time. Delete this User Note, once you have tailored the document for your specific use.]

LETTER OF AUTHORITY TO ACCESS INFORMATION

Client Authorisation for Release of Information
from other Professionals, Institutions or Advisors/Representatives

To whom it may concern

I/We:

Client: _____ **DOB:** _____
Please Print

Client: _____ **DOB:** _____
Please Print

Of: _____
Address

_____

If, *on behalf of*, a **Legal Entity:** _____
Legal Entity

I/We, [NAME] of [ADDRESS] authorise <insert name> ('the Representative') and or <insert CAR's Name> (Corporate Authorised Representative No. XXXXXX) of <insert address of both>, Representatives of AD Advisory Services Pty Ltd, AFSL No. 237058, ACN No. 005 830 802, to be provided with details of my personal/sensitive information. I authorise all information requested by the above person/entities in relation to my/our:

- Bank accounts and statements;
- Existing loans;
- Financial records, tax returns, lodgements, company records (incl. constitutions, deeds etc.);
- Development Approvals, Contracts, Presale details, Guarantors etc.;
- Life-Risk and General Insurance Policies, Investments and other Financial Products;
- Superannuation Funds (incl. SMSFs, trust deeds, etc.); and or
- Any other financial or personal information requested you might hold.

The purpose of this authority is to enable the above listed person(s), to obtain relevant information for use when needed in connection with my financial advice / financial planning arrangements.

At no stage does this authority allow any of these Representatives to conduct any changes, transactions or directly request communication that could lead to a financial transaction on my behalf.

I understand that this authority is to remain in place for a period of three [3] years, effective from the date of signing this authority unless withdrawn by me/us prior.

_____ _____
Client Signature Client Signature

Date: Date:

Appendix 5 – Privacy Access Request Refusal Letter *EXAMPLE*

[**User Note**: **This is an example document; it is not necessarily definitive or tailored for your use**. Modify, as with all templates, for your specific business use. Insert Licensees Name, AFSL number and ABN in footer of letter. Delete this User Note, once you have tailored the document for your specific use.]

[date]

[Title, First, Last Name]
[Client's address]

Dear [insert name]

Re: [insert File Number / Case Number / Reference Number]

We are writing about the request you made on [insert DD/MM/YY] to access your personal information held by us.

Unfortunately, we cannot provide you with access because [insert reason for refusal].

If you are not satisfied with the way we have handled your request, please contact us via:

Phone: [insert details]

Email: [insert details]

Post: [insert details]

If your complaint cannot be resolved immediately or within a very short time period, we will acknowledge it and try to resolve it as quickly as we can. We aim to resolve complaints within 10 to 15 days, or if it might take longer to investigate the complaint, we will let you know. If you are unhappy with our response, you may contact:

The Australian Financial Complaints Authority, of which AD Advisory Services Pty Ltd is a member:

Address: GPO Box 3, Melbourne, VIC, 3001

Phone: 1800 931 678

E-mail: info@afca.org.au

Website: www.afca.org.au

Alternatively, under the Privacy Act, you may wish to complain to the Office of the Australian Information Commissioner about the way we have handled your personal or credit information:

Address: GPO Box 5218, Sydney, NSW, 2001

Phone: 1300 363 992

Online: https://forms.business.gov.au/smartforms/landing.htm?formCode=APC_PC

Website: www.oaic.gov.au

Yours sincerely

[Insert signature]
[Insert Name]

Appendix 6 – Declaration and Privacy Consents

[**User Note**: **This is an example document**, including but not necessarily limited to, matters that need to be included in a 'client declaration/consent to collect and hold etc personal information'. **It is not necessarily definitive or tailored for your use**. Delete this User Note, once you have tailored the document for your specific use.]

Privacy Consent

Reference to <insert name> ('the Representative') and or <insert CAR's Name> (Corporate Authorised Representative No. XXXXXX) of <insert address of both>, Representatives of AD Advisory Services in the following clauses, means AD Advisory Services Pty Ltd, ACN. 005 830 802, Australian Financial Services License No. 237058 of Level 9, 488 Queen Street Brisbane QLD 4001. Collectively 'us' and 'you' below.

Authority for AD Advisory Services to collect, access, use, hold, disclose and release personal information

I/We authorise AD Advisory Services to collect, access, use, hold, disclose and release my/our personal information to enable you to advise on my/our financial situation, needs and objectives and to provide product(s) or service(s) for which I/we have inquired about, applying for or AD Advisory Services supplies.
I/We acknowledge:

1. My/Our personal or sensitive information provided or collected will be held by you.
2. You may use financial, personal, credit information and any other information I/we provide to you to arrange or provide financial and other services.
3. You may hold my/our Tax File Numbers for the purposes of which it was provided by me/us.
4. You may exchange the information with the following types of entities, some of which may be located overseas.
    - Persons or entities who provide financial services, financial reports, administration services and or reports, finance or other products to you, or to whom an application has been made for those products or services;
    - Financial consultants, accountants, lawyers, Representatives/financial advisers, insurers, guarantors or intending guarantors of a proposed credit facility and or referee(s);
    - Any industry body, tribunal, court or otherwise in connection with any complaint regarding our services;
    - Any person where you are required by law to do so;
    - Any of your associates, related entities or contractors;
    - Your referees, such as your employer, to verify information I/we have provided;
    - Any person considering acquiring an interest in your business or assets;
    - Any organisation providing online verification of my/our identity;
    - External data storage providers to backup and ad-hoc store your electronic data.
5. We may gain access to the personal information that you hold about me/us by contacting you. A copy of your privacy policy can be obtained by contacting you. Your privacy policy contains information about how I/we may access or seek correction of the information you hold about me/us, how it is managed and your complaints process.

If I/we do not provide the information needed, you may be unable to assist or appropriately advise me/us or provide other services.

I/we agree that you may collect use and disclose my/our information as specified above.

_____	_____
Name (please print)	Name (please print)
_____	_____
Signature	Signature
_____	_____
Date	Date

Appendix 7 – Verbal Privacy Consent Checklist

[**User Note**: **This is an example document**, including but not necessarily limited to, matters that need to be discussed and documents with a client when obtaining 'verbal consent' to collect and hold personal information. **It is not necessarily definitive or tailored for your use**. E.g., Providing your client with a 'Credit Information Policy' handout may be required if you are providing personal information to a Credit Reporting Agency. Modify, as with all templates, for your specific business use. Also, look out for ASIC, other industry bodies requirements and updates, basis Codes and other Regulations or Legislation changes that occur from time to time. Delete this User Note, once you have tailored the document for your specific use.]

To enable us to assess your enquiry you need to be aware of the following information and provide us your consent to collect and use your personal information. Without your consent, AD Advisory Services Pty Ltd, will not be able to consider your enquiry or provide a financial service.

NOTE: Verbal privacy consent must not be taken for Guarantors

Applicant(s) details

Applicant 1	**Applicant 2**
Name:	Name:
Date:	Date:

Verbal privacy consent checklist	**Applicant 1**	**Applicant 2**
Do you authorise us to collect and use your personal information for the purpose of your enquiry, financial advice or financial planning?	☐ Yes ☐ No	☐ Yes ☐ No
Do you authorise us to gather from and/or disclose to Financial Institutions, Credit Reporting Agencies/other banks/your guarantor(s) your personal information for the purposes of assessing and providing you with the product or service you enquired about or applied for?	☐ Yes ☐ No	☐ Yes ☐ No
Would you like to receive supporting documents or your applications/contracts electronically? If so, could you please provide us in writing your email address either via email, fax or letter?	☐ Yes ☐ No	☐ Yes ☐ No

Access to personal information

Please read the following paragraph to the Customer:

You may access your personal information at any time by contacting us. Access will be granted in accordance with the *Privacy Act 1988* for a reasonable fee, if applicable. If any of your information is inaccurate, you may request that it be corrected.

You'll need to complete a more comprehensive privacy consent form before we can provide you with the product or service you are applying for.

Representative's declaration

I certify that I have asked the Applicant(s) the above questions and the responses noted above were received from the Applicant(s) on the date indicated above.

Name (print):		Signature:	

This document must be completed by the Representative. Once completed in full, send this checklist along with any other documents requested by financial/credit institution or insurer for assessment or release of information.

Appendix 8 – Representatives Privacy Checklist

[**User Note**: **This is an example document**, including but not necessarily limited to, matters that need to be included in a client file check list. **It is not necessarily definitive or tailored for your use**. Modify, as with all templates, for your specific business use. Also, look out for ASIC, OAIC and other industry bodies requirements and updates, basis Codes and other Regulations or Legislation changes that occur from time to time. Delete this User Note, once you have tailored the document for your specific use.]

Client Referral and Engagement Checklist	**Yes**	**No**
Have you collected, received or acquired in relation to an identified or identifiable individual personal information? If Yes, you have collected personal information	☐	☐
Have you collected, received or acquired information about another individual, for example, a partner or associate? If yes you have collected personal information about that other person?	☐	☐
If information was not collected directly from the individual concerned have you verified the accuracy of the information?	☐	☐
Is the information necessary for one or more of our organisation's functions or activities?	☐	☐
Is it necessary to collect all of the information being collected?	☐	☐
Is the collection being affected fairly and by lawful means?	☐	☐
Are you collecting the personal information from the individual?	☐	☐
Is the information being used or disclosed for one or more of the purposes for which it was collected?	☐	☐
If not, is the information being used for a secondary purpose which is related (personal information) or directly related (sensitive information) to one of the purposes for collection?	☐	☐
AND has the use or disclosure been consented to by the individual(s)? Remember, if it is confidential information, industry Codes of Conduct will also preclude disclosure without the client's consent.	☐	☐
OR is it direct marketing material being directed to the individual in circumstances where is impracticable to seek consent before that particular use, AD Advisory Services will not charge the individual for giving effect to an opt out request, the individual has not made an opt out request and in which an opt out clause has been included?	☐	☐
Have you provided the individual with a copy of your Privacy Collection Statement, Privacy Policy, Disclosure Statement or brought one of these to their attention?	☐	☐

Appendix 9 – General Data Protection Regulation (GDPR)

[User Note: Delete this appendix if you are not subject to the 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, adaptions 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	AD Advisory Services will comply with the GDPR requirement
1	Use or disclosure of personal information/data for secondary purpose	AD Advisory Services may use personal information for a secondary purpose if the individual has consented, it is within their reasonable expectations, or another exception applies.	AD Advisory Services 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	AD Advisory Services will only collect personal information where it is reasonably necessary or when it is directly related to AD Advisory Services' functions or activities, and by lawful and fair means. Sensitive information will only be collected with consent, or where a listed exemption applies.	AD Advisory Services 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 personal information/data	AD Advisory Services' Privacy Collection Notice is drafted in accordance with the APP requirements.	AD Advisory Services provides the following additional information to EU citizens: • The contact details of our data protection officer are [*insert contact details if you are required to have a data protection officer under GDPR requirements*] • Where AD Advisory Services is collecting information only for AD Advisory Services' own legitimate interests, those interests are: [*insert your legitimate interests if this applies to you*]

Item no	Obligation	Australian Privacy Act requirement	AD Advisory Services will comply with the GDPR requirement
			• AD Advisory Services will store personal data for [*insert period*] OR AD Advisory Services will store personal data for a period that [*insert criteria for determining the period]* *You will need to appoint a Data Protection Officer if you:* *a) Process data for a public authority or body;* *b) Have a business where the core activities involve regular and systematic monitoring of data subjects; or* *c) Have core activities which consist of processing a large scale of 'sensitive information'*
4	Direct marketing	AD Advisory Services will comply with the 'Direct marketing' section of this Privacy Policy. AD Advisory Services 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.	AD Advisory Services 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	AD Advisory Services will comply with the 'Unsolicited personal information' section of this Privacy Policy. AD Advisory Services will destroy or de-identify all unsolicited personal information.	AD Advisory Services will not collect personal data without a specified, explicit purpose.
6	Cross border disclosure of personal information	In accordance with the 'Sending information overseas' section of this Privacy Policy, before AD Advisory Services 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. 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.	AD Advisory Services will only transfer personal data outside of EU jurisdiction where the recipient jurisdiction has been assessed as 'adequate' in terms of data protection, 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	AD Advisory Services ensures that data subjects can insist on the rectification of

Item no	Obligation	Australian Privacy Act requirement	AD Advisory Services will comply with the GDPR requirement
		Privacy Policy, AD Advisory Services takes reasonable steps to correct personal information they hold about an individual, on request by the individual.	inaccurate personal data concerning, without delay.
8	Consent	AD Advisory Services ensures that when obtaining consent from an individual, the following elements are complied with: • 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.	AD Advisory Services 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, AD Advisory Services has in place policies and procedures which comply with the mandatory data breach notification scheme. *[Only include this information if this is true.]*	AD Advisory Services 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. Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, AD Advisory Services 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 AD Advisory Services' handling of their personal information with the Office of the Australian Information Commissioner.	AD Advisory Services advises individuals that: • 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 AD Advisory Services 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	AD Advisory Services will ensure that the individual has the right to obtain from AD Advisory Services 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: • where the accuracy of the personal data is contested by the data subject, it can be

Item no	Obligation	Australian Privacy Act requirement	AD Advisory Services will comply with the GDPR requirement
			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 of whether our legitimate interests override those of the data subject. • Where processing has been restricted, with the exception of storage, AD Advisory Services will only process the personal data with the data subject's consent, or for the purposes of: o legal proceedings; o to protect the rights of another natural or legal person; or for o reasons of public interest of the Union or a Member State.
12	Right to be forgotten	AD Advisory Services 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).	The individual is entitled to request that AD Advisory Services will erase an individual's personal information without delay, and AD Advisory Services will act in accordance with this request without delay, where a specified ground applies. The specified grounds are: • 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 AD Advisory Services is subject; or • the personal data has been collected in relation to the offer of information society services.
13	Data profiling	Nil	AD Advisory Services will obtain the individual's specific consent to data profiling. '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 person's performance at work, economic situation, health, personal

Item no	Obligation	Australian Privacy Act requirement	AD Advisory Services will comply with the GDPR requirement
			preferences, interests, reliability, behaviour, location or movements. 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. AD Advisory Services 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 AD Advisory Services' website.
14	Monitoring behaviour	Nil	AD Advisory Services will obtain the individual's consent to monitoring an individual's behaviour in so far as it takes place in the EU. 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. Monitoring includes the following activities conducted by AD Advisory Services: • tracking the behaviour and browsing history of individuals on the internet; • using the tracking processes to profile the individual, to enable AD Advisory Services to make decisions concerning the individual, or to enable AD Advisory Services to analyse or predict their personal preferences, behaviours and attitudes. AD Advisory Services 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 AD Advisory Services undertakes any monitoring activities.