Privacy Policy

Allied Financial Consulting Pty Limited

Company:	Allied Financial Consulting Pty Limited
ACN:	059 732 419
ACL:	393845
Date Updated:	June 2022

TABLE OF CONTENTS

VERSION CONTROL

Version Number	Date Updated	Notes
1	June 2022	Original document prepared and finalised in consultation with Sophie Grace Pty Ltd.

SECTION A – INTRODUCTION

1. INTRODUCTION

1.1 As part of Allied Financial Consulting Pty Limited's ("**Allied**") process to ensure that it continues to maintain the highest levels of professional integrity and ethical conduct, Allied has adopted this Privacy Policy ("**Policy**") to manage Personal Information in an open and transparent manner.

1.2 The provisions of this Policy assist Allied in complying with the requirements of the *Privacy Act 1988* (Cth) and the Australian Privacy Principles in protecting the Personal Information Allied holds about its clients.

2. WHEN DOES THIS POLICY APPLY?

2.1 This Policy applies to all representatives and employees of Allied at all times and the requirements remain in force on an ongoing basis.

3. GLOSSARY

TERM	DEFINITION
Affected Information Recipient	Means: (a) a mortgage insurer; or (b) a trade insurer; or (c) a body corporate who is a related body corporate of the Allied; or (d) a person who: (i) is involved in processing an application for credit made to Allied; or (ii) manages credit provided by Allied; or (e) an entity, a legal adviser of the entity or professional adviser of the entity.
APP Entity	means an agency or organisation as defined in section 6 of the Privacy Act 1988.
Australian law	means (a) an Act of the Commonwealth or of a State or Territory; (b) or regulations, or any other instrument, made under such an Act; or (c) a Norfolk Island enactment; or (d) a rule of common law or equity.
Collects	Allied collects Personal Information only if Allied collects the Personal Information for inclusion in a record or generally available publication.
Court/Tribunal Order	means an order, direction or other instrument made by: (a) a court; or (b) a tribunal; or

	(c) a judge (including a judge acting in a personal capacity) or a person acting as a judge; or (d) a magistrate (including a magistrate acting in a personal capacity) or a person acting as a magistrate; or (e) a member or an officer of a tribunal; and includes an order, direction or other instrument that is of an interim or interlocutory nature.
CR Code	refer to the Privacy (Credit Reporting) Code 2014 (Version 2). This is written code of practice about credit reporting. The CR code supplements the credit reporting provisions contained in Part IIIA of the Privacy Act 1988. A breach of the CR code is a breach of the Privacy Act 1988. The CR code is registered on the OAIC Privacy Register.
Credit Eligibility Information	means Credit Reporting Information that was disclosed to the Credit Provider by a Credit Reporting Body or CP Derived Information. Credit eligibility information is generally held by a Credit Provider and may be disclosed to Affected Information Recipients and other entities in specific circumstances.
Credit Provider	The following entities are included as credit providers for the purposes of the Privacy Act: (a) a bank; (b) an organisation or Small Business Operator if a substantial part of its business is the provision of credit, such as a building society, finance company or a credit union; (c) a retailer that issues credit cards in connection with the sale of goods or services; (d) an organisation or Small Business Operator that supplies goods and services where payment is deferred for seven (7) days or more, such as a telecommunications carriers and energy and water utilities; and (e) certain organisations or Small Business Operators that provide credit in connection with the hiring, leasing or renting of goods. Importantly, the following entities are not credit providers: (a) real estate agents; (b) general insurers; and (c) employers.
CP Derived Information	means any Personal Information (other than Sensitive Information) about an individual: (a) that is derived from Credit Reporting Information about the individual that was disclosed to a Credit Provider by a Credit Reporting Body; and (b) that has any bearing on the individual's credit worthiness; and

	(c) that is used, has been used or could be used in establishing the individual's eligibility for consumer credit.
Credit Information	means Personal Information that is: (a) identification information about the individual; or (b) consumer credit liability information about the individual; or (c) repayment history information about the individual; or (d) a statement that an information request has been made in relation to the individual by a Credit Provider, mortgage insurer or trade insurer; or (e) the type of consumer credit or commercial credit, and the amount of credit, sought in an application: (iii) that has been made by the individual to a Credit Provider; and (iv) in connection with which the provider has made an information request in relation to the individual; or (f) default information about the individual; or (g) payment information about the individual; or (h) new arrangement information about the individual; or (i) court proceedings information about the individual; or (j) personal insolvency information about the individual; or (k) publicly available information about the individual: (i) that relates to the individual's activities in Australia or the external Territories and the individual's credit worthiness; and (ii) that is not court proceedings information about the individual or information about the individual that is entered or recorded on the National Personal Insolvency Index; or (l) the opinion of a Credit Provider that the individual has committed, in circumstances specified by the provider, a serious credit infringement in relation to consumer credit provided by the provider to the individual.
Credit Reporting Body	means a business or undertaking that involves collecting, holding, using or disclosing Personal Information about individuals for the purpose of, or for purposes including the purpose of, providing an entity with information about the credit worthiness of an individual.
Credit Reporting Information	means Credit Information or Credit Reporting Body derived information about an individual.
De-identified	Personal Information is *de-identified* if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.
Holds	Allied *holds* Personal Information if it has possession or control of a record that contains the Personal Information.

Identifier of an individual	means a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual, but does not include: (a) the individual's name; or (b) the individual's ABN (within the meaning of the A New Tax System (Australian Business Number) Act 1999); or (c) anything else prescribed by the regulations.
Permitted General Situation	As defined in s16A of the Privacy Act 1988
Personal Information	means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.
Sensitive Information	means (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also Personal Information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification or biometric templates.
Small Business Operators	is a person or organisation that has an annual turnover of $3,000,000 or less. For the purposes of the Privacy Act 1988 health service providers or businesses that trade in Personal Information are not Small Business Operators.

SECTION B – COLLECTION OF INFORMATION (SOLICITED INFORMATION)

This Section B applies to the collection of information that is solicited by Allied.

4. PERSONAL INFORMATION

4.1 The Personal Information Allied collects may include the following:

(a) name;

(b) address;

(c) date of birth;

(d) gender;

(e) marital status;

(f) occupation;

(g) bank account details;

(h) contact details (including telephone, facsimile and e-mail);

(i) financial information (including transactional and trading history); and

(j) any other information Allied considers necessary to their functions and activities.

4.2 Allied must not collect Personal Information (other than Sensitive Information) unless the information is reasonably necessary for one or more of Allied's functions or activities.

4.3 Allied's functions or activities is to provide credit services to consumers as both a direct lender and broker

5. SENSITIVE INFORMATION

5.1 Allied must not collect Sensitive Information about an individual unless:

(a) the individual consents to the collection of the information and the information is reasonably necessary for one or more of Allied's functions or activities (as described in section 1.1); or

(b) the collection of the information is required or authorised by or under an Australian law or a Court/Tribunal Order; or

(c) a Permitted General Situation exists in relation to the collection of the information by Allied; or

(d) a permitted health situation exists in relation to the collection of the information by Allied.

6. CREDIT-RELATED INFORMATION

6.1 Where Allied receives a request for credit, the prospective client is required to provide Allied with Credit Information. Please refer to Allied's Credit Reporting Policy for further information.

7. MEANS OF COLLECTION

7.1 Allied must only collect Personal Information by lawful and fair means.

7.2 Allied must only collect Personal Information about an individual from the individual (rather than someone else), unless it is unreasonable or impracticable to do so or the individual has instructed Allied to liaise with someone else.

7.3 Allied collects Personal Information from an individual when:

(a) Allied's Application Form is completed;

(b) a Client provides the information to Allied's representatives over the telephone or via email; and

(c) a Client provides the information to Allied on its website.

8. PURPOSE OF COLLECTION

8.1 If an individual is acquiring or has acquired a product or service from Allied, the individual's Personal Information is collected and held for the purposes of:

(a) checking whether an individual is eligible for Allied's product or service;

(b) disclosing an individual's Credit Information to any of Allied's related companies that are also are considering whether to provide credit to the individual;

(c) providing the individual with Allied's product or service;

(d) managing and administering Allied's product or service;

(e) to collect payments that are owed to Allied in respect of any credit that has previously provided to the individual;

(f) protecting against fraud, crime or other activity which may cause harm in relation to Allied's products or services;

(g) responding to a complaint;

(h) where the individual otherwise expressly consents to the use or disclosure.

(i) complying with legislative and regulatory requirements in any jurisdiction; and

(j) to assist Allied in the running of its business.

8.2 Allied may also collect Personal information for the purposes of letting an individual know about products or services that might better serve their needs or other opportunities in which they may be interested. Please refer to Section G for further information.

SECTION C – COLLECTION OF INFORMATION (UNSOLICITED INFORMATION)

9. DEALING WITH UNSOLICITED PERSONAL INFORMATION

9.1 If Allied:

(a) receives Personal Information about an individual; and

(b) the information is not solicited by Allied

Allied must, within a reasonable period after receiving the information, determine whether or not it was permitted to collect the information under Section B above.

9.2 Allied may use or disclose the Personal Information for the purposes of making the determination under paragraph 9.1.

9.3 If Allied:

(a) determines that it could not have collected the Personal Information; and

(b) the information is not contained in a Commonwealth record,

Allied must as soon as practicable, destroy the information or ensure that the information is De-identified, only if it is lawful and reasonable to do so.

SECTION D – NOTIFICATION OF THE COLLECTION OF INFORMATION

10. CREDIT REPORTING AND PRIVACY STATEMENT

10.1 Allied's Director must ensure that at all times it maintains a clearly expressed and up-to-date Credit Reporting and Privacy Statement that:

(a) is current and reflects the latest applicable Australian laws; and

(b) contains the following information:

(i) the kinds of Credit Information, Credit Eligibility Information and Personal Information that Allied collects and holds, and how Allied collects and holds that information;

(ii) the kinds of CP Derived Information that Allied usually derives from Credit Reporting Information disclosed to Allied by a Credit Reporting Body;

(iii) the purposes for which Allied collects, holds, uses and discloses Credit Information, Credit Eligibility Information and Personal Information;

(iv) how an individual may access Credit Eligibility Information and Personal Information held by Allied and seek a correction of such information;

(v) how an individual may complain about a failure of Allied to comply with the Privacy Act 1988 or CR Code and how Allied deals with such a complaint;

(vi) whether Allied is likely to disclose Credit Information and Credit Eligibility Information to entities that do not have an Australian link; and

(vii) where Allied is likely to disclose Credit Information or Credit Eligibility Information to entities that do not have an Australian link, the countries in which such entities are likely to be located.

10.2 Allied must ensure that Allied's Credit Reporting and Privacy Statement is available free of charge and in such form as appropriate.

10.3 If the Credit Reporting and Privacy Statement is requested in a particular form, Allied does take such steps as are reasonable to provide the Credit Reporting and Privacy Statement in the form requested.

SECTION E – USE OR DISCLOSURE OF INFORMATION

11. USE OR DISCLOSURE OF PERSONAL INFORMATION

11.1 Where Allied holds Personal Information about an individual that was collected for a particular purpose ("**the primary purpose**"), Allied must not use or disclose the information for another purpose ("**the secondary purpose**") unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) the individual would reasonably expect Allied to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) directly related to the primary purpose (if the information is Sensitive Information); or

(ii) related to the primary purpose (if the information is *not* Sensitive Information); or

(c) the use or disclosure of the information is required or authorised by or under an Australian law or a Court/Tribunal Order; or

(d) a Permitted General Situation exists in relation to the use or disclosure of the information by Allied; or

(e) Allied reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

11.2 Where Allied uses or discloses Personal Information in accordance with section 11.1(e), Allied keeps a copy of this disclosure (e.g. the email or letter used to do so).

11.3 This section 11 does not apply to:

(a) Personal Information for the purposes of direct marketing; or

(b) government related identifiers.

11.4 If Allied collects Personal Information from a related body corporate, this section 11 applies as if Allied's primary purpose for the collection was the primary purpose for which the related body corporate collected the information.

12. WHO DOES Allied DISLCOSE PERSONAL INFORMATION TO?

12.1 Allied may disclose Personal Information collected from clients and prospective clients to the following:

(a) organisations involved in providing, managing or administering Allied's products or services such as third party suppliers, e.g. printers, posting services and our advisers;

(b) organisations involved in maintaining, reviewing and developing Allied's business systems, procedures and infrastructure, including testing or upgrading Allied's computer systems;

(c) organisations involved in a corporate re-organisation;

(d) organisations involved in the payments system, including financial institutions, merchants and payment organisations;

(e) organisations involved in product planning and development;

(f) other organisations, who jointly with Allied's, provide its products or services;

(g) authorised representatives who provide Allied's products or services on its behalf;

(h) the individual's representatives, including your legal advisers;

(i) debt collectors;

(j) Allied's financial advisers, legal advisers or auditors;

(k) fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct;

(l) external dispute resolution schemes;

(m) regulatory bodies, government agencies and law enforcement bodies in any jurisdiction.

SECTION F – DIRECT MARKETING

13. DIRECT MARKETING

13.1 Allied must not use or disclose the Personal Information it holds about an individual for the purpose of direct marketing.

14. EXCEPTION – PERSONAL INFORMATION OTHER THAN SENSITIVE INFORMATION

14.1 Allied may use or disclose Personal Information (other than Sensitive Information) about an individual for the purposes of direct marketing if:

(a) Allied collected the information from the individual; and the individual would reasonably expect Allied to use or disclose the information for that purpose; or

(b) Allied has collected the information from a third party; and either:

(i) Allied has obtained the individual's consent to the use or disclose the information for the purpose of direct marketing; or

(ii) it is impracticable for Allied to obtain the individual's consent; and

(c) Allied provides a simple way for the individual to opt out of receiving direct marketing communications from Allied;

(d) in each direct marketing communication with the individual Allied:

(i) includes a prominent statement that the individual may opt out of receiving direct marketing; or

(ii) directs the individual's attention to the fact that the individual may opt out of receiving direct marketing; and

(e) the individual has not made a request to opt out of receiving direct marketing.

15. EXCEPTION – SENSITIVE INFORMATION

15.1 Allied may use or disclose Sensitive Information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

16. REQUESTS TO STOP DIRECT MARKETING

16.1 Where Allied uses or discloses Personal Information about an individual for the purposes of direct marketing by Allied or facilitating direct marketing by another organisation, the individual may request:

(a) that Allied no longer provide them with direct marketing communications;

(b) that Allied does not use or disclose the individual's Personal Information for the purpose of facilitating direct marketing by another organisation;

(c) that Allied provides the source of the Personal Information.

16.2 Where Allied receives a request from an individual under section 16.1, Allied:

(a) gives effect to the request under section 16.1(a) or 16.1(b) within a reasonable period after the request is made and free of charge; and

(b) notifies the individual of the source of the information, if the individual requests it, unless it is impracticable or unreasonable to do so.

16.3 This Section F does not apply to the extent that the following laws apply:

(a) the Do Not Call Register Act 2006;

(b) the Spam Act 2003; or

(c) any other Act of the Commonwealth of Australia.

SECTION G – CROSS BORDER DISCLOSURE OF INFORMATION

17. DISCLOSING PERSONAL INFORMATION TO CROSS BORDER RECIPIENTS

17.1 Where Allied discloses Personal Information about an individual to a recipient who is not in Australia and who is not Allied or the individual, Allied must ensure that the overseas recipient does not breach the Australian Privacy Principles (with the exception of APP1).

17.2 Section 17.1 does not apply where:

(a) Allied reasonably believes that:

(i) information is subject to a law or binding scheme that has the effect of protecting the information in a way that is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) Allied has informed the individual that if they consent to the disclosure of information Allied does not take reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles; and

(ii) after being so informed, the individual consents to disclosure;

(c) the disclosure of the information is required or authorised by or under an Australian law or a Court/Tribunal Order; or

(d) a Permitted General Situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1) of the Privacy Act 1988) exists in relation to the disclosure of the information by Allied.

SECTION H – ADOPTION, USE OR DISCLOSURE OF GOVERNMENT IDENTIFIERS

18. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS

18.1 Allied must not adopt a government related identifier of an individual as its own identifier unless:

(a) Allied is required or authorised by or under an Australian law or a Court/Tribunal Order to do so; or

(b) the identifier, Allied and the circumstances of the adoption are prescribed by regulations.

19. USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

19.1 Before using or disclosing a government related identifier of an individual, Allied must ensure that such use or disclosure is:

(a) reasonably necessary for Allied to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) required or authorised by or under an Australian law or a Court/Tribunal Order; or

(d) within a Permitted General Situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1) of the Privacy Act 1988; or

(e) reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) the identifier, Allied and the circumstances of the adoption are prescribed by regulations.

SECTION I – INTEGRITY OF INFORMATION

20. QUALITY OF INFORMATION

20.1 Allied ensures that the Personal Information it collects and the Personal Information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

21. SECURITY OF INFORMATION

21.1 Allied does ensure that it protects any Personal Information it holds from misuse, interference, loss, unauthorised access, modification and disclosure.

21.2 Allied does take reasonable steps to destroy or de-identify Personal Information it holds where:

(a) Allied no longer needs the Personal Information for any purpose for which the information may be used or disclosed by Allied; and

(b) the information is not contained in a Commonwealth record; and

(c) Allied is not required to retain that information under an Australian law, or a Court/Tribunal Order.

22. STORAGE OF INFORMATION

22.1 Allied stores Personal Information in different ways, including:

(a) hard copy on site at Allied's head office; and

(b) electronically secure data centres which are located in Australia and owned by either Allied or external service providers.

22.2 In order to ensure Allied protects any Personal Information it holds from misuse, interference, loss, unauthorised access, modification and disclosure, Allied implements the following procedure/system:

(a) access to information systems is controlled through identity and access management;

(b) employees are bound by internal information securities policies and are required to keep information secure;

(c) all employees are required to complete training about information security; and

(d) Allied regularly monitors and reviews its compliance with internal policies and industry best practice.

SECTION J – ACCESS TO PERSONAL INFORMATION

23. ACCESS

23.1 Allied must give an individual access to the Personal Information it holds about the individual if so requested by the individual.

23.2 Allied must respond to any request for access to Personal Information within a reasonable period after the request is made.

23.3 Allied must give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so and must take such steps as are reasonable in the circumstances to give access in a way that meets the needs of Allied and the individual.

23.4 Allied must not charge an individual for making a request, and must not impose excessive charges for the individual to access their Personal Information.

24. EXCEPTIONS

24.1 Allied is not required to give an individual access to their Personal Information if:

(a) Allied reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access if frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between Allied and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal intentions of Allied in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a Court/Tribunal Order; or

(h) Allied has reason that unlawful activity, or misconduct of a serious nature, that relates to our functions or activities has been, or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within Allied in connection with a commercially sensitive decision-making process.

25. REFUSAL TO GIVE ACCESS

25.1 If Allied refuses to give access in accordance with section 23 or to give access in the manner requested by the individual, Allied gives the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

25.2 Where Allied refuses to give access under section 24.1(j) Allied may include an explanation of the commercially sensitive decision in its written notice of the reasons for denial.

SECTION K – CORRECTION OF INFORMATION

26. CORRECTION OF INFORMATION

26.1 Allied must take reasonable steps to correct all Personal Information, having regard to the purpose for which the information is held where:

(a) Allied is satisfied the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(b) the individual requests Allied corrects the information.

26.2 Where Allied corrects Personal Information about an individual that Allied previously disclosed to another APP Entity and the individual requests Allied to notify the other APP

Entity of the correction, Allied must take reasonable steps to give that notification, unless it is impracticable or unlawful to do so.

27. REFUSAL TO CORRECT INFORMATION

27.1 If Allied refuses to correct Personal Information as requested by the individual, Allied gives the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

28. REQUEST FROM A CLIENT TO ASSOCIATE A STATEMENT WITH THEIR INFORMATION

28.1 If:

(a) Allied refuses to correct Personal Information as requested by the individual; and

(b) the individual requests that Allied associate a statement noting that the information is inaccurate, out of date, incomplete, irrelevant or misleading, with the individual's information,

Allied must take such steps as are reasonable in the circumstances to associate the statement (as described in section 28.1(b)) with the individual's Personal Information. The statement should be associated with the information in such a way that it makes the statement apparent to users of the information.

29. DEALING WITH REQUESTS

29.1 Allied must:

(a) respond to requests under this Section K within thirty (30) days after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the Personal Information or for associating the statement with the Personal Information.

SECTION L – MAKING A PRIVACY COMPLAINT

30. COMPLAINTS

30.1 Allied offers a free internal complaint resolution scheme to all customers. Should a client have a privacy complaint, they are to contact Allied to discuss their concerns using the following contact details:

(a) Email: jim@alliedfc.com.au; and

(b) Post: Ground Floor, 3 Spring St, Sydney NSW 2000

30.2 To assist Allied in helping customers, Allied asks customers to follow a simple three-step process:

(a) gather all supporting documents relating to the complaint;

(b) contact Allied to review your situation and if possible, resolve your complaint immediately; and

(c) if the matter is not resolved to the customer's satisfaction, customers are encouraged to contact Allied's Complaints Officer on [insert number] or put their complaint in writing and send it to [insert address].

30.3 Allied will rectify any breach if the complaint is justified and takes necessary steps to resolve the issue.

30.4 In certain situations, to deal with a complaint it may be necessary to consult with third parties. However, any disclosure of Personal Information to third parties will be provided with the customer's authority and consent.

30.5 After a complaint has been received, Allied sends the customer a written notice of acknowledgement setting out the process. The complaint is investigated, and the decision sent to the customer within thirty (30) days unless the customer has agreed to a longer time. If a complaint cannot be resolved within the agreed time frame or a decision could not be made within thirty (30) days of receipt, a notification will be sent to the customer setting out the reasons and specifying a new date when the customer can expect a decision or resolution.

30.6 If the customer is not satisfied with Allied's internal privacy practices or the outcome in respect to complaint, the customer may approach the OAIC with their complaint:

Office of the Australian Information Commissioner

Address: GPO Box 5218, Sydney NSW 2001

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Website: oaic.gov.au

SECTION M – MISCELLANEOUS

31. POLICY BREACHES

31.1 Breaches of this Policy may lead to disciplinary action being taken against the relevant party, including dismissal in serious cases and may also result in prosecution under the law where that act is illegal. This may include re-assessment of bonus qualification, termination of employment and/or fines (in accordance with the Privacy Act 1988.

31.2 Staff are trained internally on compliance and their regulatory obligation to Allied. They are encouraged to respond appropriately to and report all breaches of the law and other incidents of non-compliance, including Allied's policies, and seek guidance if they are unsure.

31.3 Staff must report breaches of this Policy directly to the Director.

32. RETENTION OF FORMS

32.1 The Compliance Officer retains the completed forms for seven (7) years in accordance with Allied's Document Retention Policy. The completed forms are retained for future reference and review.

32.2 As part of their training, all staff are made aware of the need to practice thorough and up to date record keeping, not only as a way of meeting Allied's compliance obligations, but as a way of minimising risk.

33. POLICY REVIEW

33.1 Allied's Privacy Policy will be reviewed on at least an annual basis by the Compliance Officer of Allied, having regard to the changing circumstances of Allied. The Compliance Officer then reports to the Director on compliance with this Policy.

Issued by Allied Financial Consulting Pty Limited

June 2022