PRIVACY POLICY

Introduction

The objective of these policies and procedures is to ensure that in our dealings with clients and other people, we comply with the Privacy Act 1988 (Cth) and to the extent applicable, the EU General Data Protection Regulations. The Act seeks to protect individuals' personal information. It does this by limiting the ways in which personal information may be collected and used.

The Privacy Act also requires certain breaches to be notified to the individuals involved and to the Office of the Australian Information Commissioner (OAIC).

The Privacy Act only applies to small businesses with a turnover in excess of $3m per annum however as a financial services business and holder of an Australian Financial Services Licence we have decided to comply with the requirements of the Privacy Act regardless of our turnover.

Complying with the Privacy Act helps us to enhance our client service.

The Board is ultimately responsible for Privacy within the business and for ensuring the both the substance as well as the form of Privacy.

This policy has the full support of all senior management and is seen as a key component in ensuring the long-term success and viability of the business.

This Policy applies to all the personal information we collect, whether from insured parties (and their contractors and employees), their employees or others.

In most cases we obtain consent in the usual course of dealings,

The business has a clear and absolute commitment that we will comply with both the spirit and letter of all requirements placed on the business. This commitment applies equally to staff, customers, suppliers and all other bodies with whom we deal with.

Our approach is to prevent and quickly rectify any breaches of Privacy identified.

It is the responsibility of all management and staff of the business to promptly advise the Compliance Manager of any situations where it appears there is failure or potential failure of the business to comply with its Privacy obligations.

The Privacy Policy and Procedures will be reviewed after any significant Privacy failure and as part of any relevant business planning process.

All staff and advisory Authorised Representatives must be familiar with and comply with this Policy and Procedure, understand the importance the business places on the effective operation of our Policies and Procedures and are encouraged to look for improvements to our procedures.

Updates

These Policy and Procedures are updated on a regular basis. Any material changes to these Policy and Procedures will be advised by management either via Email or at our regular Staff meetings.

This document and associated forms etc are accessible in soft copy via our computer network. We do not store these documents in hard copy. All information can be immediately accessed on the computer network and will be guaranteed to be up to date at all times.

What Is Personal Information?

Personal information is information or opinion about an individual whose identity is apparent or can easily be ascertained from the information or opinion, for example name, address, age etc.

Sensitive Personal Information

Sensitive information is a type of personal information that is given extra protection and must be treated with additional care. It includes any information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. It also includes health information.

Health information is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. Health information also includes personal information collected in the course of providing a health service.

Compliance Manager

Our Compliance Manager will be the Manager who is responsible for the implementation and effective operation of these Policy and Procedures. This person is identified in our Organisational Chart.

Privacy Promotion

We have developed a system to ensure that we have ongoing promotion and reinforcement of Privacy throughout the business. Processes include:

- Requiring all new staff and representatives to undertake privacy training as part of our induction process and read these Policy and Procedures.
- As part of regular staff meetings run internal training sessions on an ongoing basis to ensure that representative's knowledge of the procedures remains current, particularly when changes have been made.

Complaints About Privacy

Refer any complaint about privacy matters to the Compliance Manager. Such complaints will be handled in accordance with our documented Complaints Policy and Procedures.

Contracting Out

Our contractors may not be bound by the Privacy Act. To ensure that our contractors treat personal information in the same way as we do, ensure the issue of Privacy is included as part of our agreement with all contractors.

AUSTRALIAN PRIVACY PRINCIPLES

Australian Privacy Principle 1 – Open and Transparent Management of Personal Information

We will:

- Manage Personal Information in an open and transparent way.
- Comply with the spirit and intent of all of the Australian Privacy Principles.
- Have documented systems to handle enquiries and complaints in regard to privacy.
- Maintain an up to date Privacy Policy Statement that is compliant with the requirements within APP 1:
- Provide a soft or hard copy of our Privacy Policy Statement to anyone who asks for information about our Privacy Policy free of charge and include this document on our Website where relevant and considered appropriate.

Australian Privacy Principle 2 – Anonymity and Pseudonymity

Where practical we will allow customers to deal with us without requiring them to specifically identify themselves. This will usually be limited solely to providing simple product quotations and general queries.

Australian Privacy Principle 3 – Collection of Solicited Personal Information

We only collect personal information that we need in a lawful and fair manner for:

- The Primary Purpose of activities authorised under our Australian Financial Services Licence (AFSL).
- The Secondary Purpose of providing ancillary services typically associated with our AFSL activities e.g. Claims handling, premium funding etc.

Stricter requirements apply to Sensitive Personal Information. We do not collect sensitive information without the individual's prior consent unless:

- The collection is required by law; or
- It is necessary for the establishment, exercise or defence of a claim

Australian Privacy Principle 4 – Dealing With Unsolicited Personal Information

In some situations, we may receive personal information that we have taken no active steps to collect. If and when we receive such information and it is not required by us as part of providing financial services to our clients, we will de-identify or destroy such information as soon as practicable.

Australian Privacy Principle 5 – Notification of the Collection of Personal Information

When collecting personal information we must take the following steps as are reasonable in the circumstances to make the individual aware of:

- When we collect personal information about individuals from various third parties we must make the individual aware that we have collected such information and from where it was sourced.
- The purpose of the collection
- Consequences of not collecting the information.
- Details of other parties that we may give the information to.
- Information on how individuals can access and correct information.
- How individuals can make a complaint about a breach of the Privacy Principles.

- Whether we will disclose information to overseas entities.
- The countries where these overseas entities are domiciled (where practicable).

All of this information is contained in our Privacy Policy Statement

Australian Privacy Principle 6 – Use or Disclosure of Personal Information

We only use or disclose personal information for:

- The Primary Purpose of activities authorised under our Australian Financial Services Licence (AFSL).
- The Secondary Purpose of providing expected ancillary services typically associated with our AFSL activities e.g. claims handling, premium funding etc.

Stricter requirements apply to Sensitive Personal Information. We do not use or disclose Sensitive Personal Information without the individual's prior consent unless:

- The collection is required by law; or
- It is necessary for the establishment, exercise or defence of a claim.

In particular, we do not trade, rent or sell personal information.

Australian Privacy Principle 7 – Direct Marketing

We may market to our clients by sending them information about financial services and related matters from time to time. Each such publication/communication must have prominently displayed, words to the effect:

> "We are delighted to provide this e.g. newsletter as a service to you. Please let us know if you would rather not receive it and we will remove your name from our distribution list."
> Staff are to refer any request to be removed from the list to our Compliance Manager. We do not charge for removing people from our list.
> Where clients request that we do not send them marketing material we must ensure that their file is marked accordingly and no further material is forwarded to them.

Australian Privacy Principle 8 – Cross-Border Disclosure of Personal Information

We are responsible for and can be fined/penalised where we send/hare/tore information with an overseas entity that does not comply with the APP's and a breach of privacy occurs.

In certain situations, it is likely that that some or all of the Personal Information that we collect may be disclosed to businesses that operate overseas. This would only occur where the product provider/intermediary is based overseas – e.g. Lloyds of London syndicates or brokers and other overseas based product providers and intermediaries or in situations where we utilise "Cloud Computing" services that are situated outside Australia.

In all such cases we must make reasonable enquiries to ensure that these organisations either:

- comply with their local privacy legislation where such legislation imposes comparable obligations to those contained in the APP's (Apart from APP1), or
- comply with the APP's (Apart from APP1) in cases where their local legislation is considered inadequate or non-existent.

We have assessed that all suppliers/intermediaries/businesses that operate in the United Kingdom, European Economic Union or the United States have comparable protection provided by their local legislation.

For all other businesses that we use overseas, unless we expressly inform the client and obtain their consent in accordance with Privacy Principle 8.2 (b) we must make reasonable enquiries and document our findings that the business is complying with:

- with their local privacy legislation where such legislation imposes comparable obligations to those contained in the APP's (Apart from APP1), or
- comply with the APP's (Apart from APP1) in cases where their local legislation is considered inadequate or non-existent.

We have created a Privacy Overseas Supplier Table that lists such overseas businesses and documents the findings of our enquiries. This table is maintained by our Compliance Manager

Australian Privacy Principle 9 – adoption, use or disclosure of government related identifiers

We do not use tax file numbers or other governmental identifiers to identify any person.

We collect, use and disclose identifiers of employees in the following circumstances:

- To the trustee of any superannuation fund to which we contribute on behalf of employees, to the Superannuation Holding Accounts Reserve and to other regulated superannuation funds, exempt public sector superannuation schemes and approved deposit funds when the benefits of members are transferred to these funds (unless the owner of the tax file number requests in writing that it not be disclosed);
- To the Tax Office in relation to the preparation of group certificates or tax stamps sheets under the PAYE/PAYG system;
- To the Tax Office in respect of payments made under the Prescribed Payments System or for Reportable Payments Declarations.

The Privacy Act permits us to disclose identifiers in some other unusual circumstances. If you want or are asked to disclose an identifier for any reason other than those listed above, check with the Compliance Manager before doing so.

Australian Privacy Principle 10 – Quality of Personal Information

We must ensure we take all reasonable steps to ensure the information we collect and use is accurate, up to date and complete.

Australian Privacy Principle 11 – Security of Personal Information

We take reasonable steps to protect the personal information we hold from misuse and unauthorised access, modification, interference (such as attacks on our computer system) and disclosure.

We destroy or de-identify personal information when it is no longer needed.

Australian Privacy Principle 12 – Access to Personal information

In principle, we will provide a person with access to the personal information we hold about them on request. The Compliance Manager will be responsible for providing access to personal information.

Before providing access:

- 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.

Provide the information by the most cost-effective and practical method available. This could be:

- Letting the person inspect the information we hold and take notes of its contents – however take care to ensure that they only see their own information;

- Letting the person view the information and provide and explanation of its contents;
- Providing a photocopy or fax of the information;
- Providing a printout of information held in electronic form;
- Providing a summary of the information.

Requests for access should be acknowledged within 7 – 10 days. Straightforward requests for access should be fulfilled within 14 days and if complex within 30 days.

There are no charges for lodging a request for access and we only charge a client for the reasonable costs and outgoings incurred in meeting their request.

We may refuse to provide access to personal information in the following circumstances:

- The request is frivolous, vexatious, i.e. trivial, made to pursue an unrelated grievance against us or is a repeated request for the same information.
- Provision would unreasonably impact on the privacy of others.
- 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.
- 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 Compliance Manager must approve all refusals of access and provide the reasons for the refusal and details of our complaints process.

The Privacy Act permits us to refuse access in some other unusual circumstances. If you want to refuse access for any reason other than those listed above, check with the Compliance Manager before doing so.

Australian Privacy Principle 13 – Correction of Personal Information

If personal information in our records is incorrect, incomplete or out of date we must update the records within a reasonable time to make them accurate. However:

- If the records are inaccessible and no longer required, consider destroying or de-identifying the information; and
- If we do not agree that the information is inaccurate, incomplete or out of date, and if requested, attach to it a statement to the effect that the person to whom the information relates claims that it is inaccurate, incomplete or out of date.
- Where requested we must also advise other Third Parties that we have provided incorrect information to update their records.

The Compliance Manager must approve all refusals to correct information and provide the reasons for the refusal and details of our complaints process.

Give reasons for any denial of access or refusal to correct information. Again, our Compliance Manager should approve these before they are communicated to the person requesting access or correction.

DATA BREACH MANAGEMENT POLICY

Introduction

An information security breach occurs when personal information is exposed to unauthorised access, use, disclosure or modification as a result of a breach of our information security. Information security breaches can occur in a number of ways. Some of the most common information security breaches happen when personal information held by us is lost, misused, mistakenly disclosed or stolen. Some examples include:

- laptops, removable storage devices, or physical files containing personal information becoming lost or stolen
- mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address
- an individual deceiving us into improperly releasing the personal information of another person
- databases containing personal information being 'hacked' into or otherwise illegally accessed by unauthorised external parties and
- employees or representatives accessing personal information outside the requirements of their role.

It is important to recognise that information security breaches are not limited to external malicious actions, such as theft or 'hacking', but may just as often involve internal errors and failures to follow established information handling procedures. While there may be no harm intended, these types of security breach can affect individuals' privacy as much as malicious actions.

Although a key concern relating to information security breaches is the risk of identity theft or fraud (particularly where credit card information is compromised), the risks from information security breaches are not limited to financial harm—for example, leaks of details about an individual's personal affairs or health information can cause other types of harm such as humiliation, damage to reputation or relationships and loss of business or employment opportunities.

We have reviewed and implemented the guide issued by the OAIC - Guide To Securing Personal Information where appropriate and relevant given our business size and the volume and detail of personal Information that we collect and hold. This has involved making changes to the various Policies and Procedures we have in place in relation to Information Technology and Risk Management etc.

The Notifiable Data Breaches Scheme (NDB)

All businesses with a turnover in excess of $3M are legally required to notify all individuals that may be affected by a Personal Information Breach as per the NDB scheme in Part IIIC of the Privacy Act.

We have taken the position that we will adopt compliance with the NDB even where our turnover is below the $3M threshold as part of being a good corporate citizen and providing our services fairly and efficiently as required by our Australian Financial Services Licence.

The NDB scheme requires us to notify individuals and the OAIC about 'eligible data breaches. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by us (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- We have been unable to prevent the likely risk of serious harm with remedial action.

We must also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations. Further information is available from the guideline published by the OAIC - (Guide to Handling Personal Information Breaches).

The primary purpose of the NDB scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm. This has a practical function: once notified about a data breach, individuals can take steps to reduce their risk of harm.

For example, an individual can change passwords to compromised online accounts, and be alert to identity fraud or scams.

The NDB scheme also serves the broader purpose of enhancing our accountability for privacy protection. By demonstrating that we are accountable for privacy, and that breaches of privacy are taken seriously, the NDB scheme works to build trust in personal information handling across industries.

In the event that we identify an eligible data breach, the breach is to be immediately referred to our Responsible Manager(s) - as shown on our Organisation Chart. The Responsible Manager(s) will determine at that time who will be responsible for managing all aspects of the breach including recording and reporting such a breach to the relevant third-party bodies.

We will follow the Privacy Breach Guidelines (Guide to Handling Personal Information Breaches) issued by the OAIC.

Further detail and information for staff and representatives is contained in the Notifiable Data Breaches Overview (Notifiable Data Breach Overview).

Privacy Act Breach Penalties

Under the Privacy Act, the OAIC, has various functions and powers which include:

investigations - the power to investigate and monitor compliance with the privacy obligations and conduct privacy performance assessments;

enforceable undertakings - the power to accept enforceable undertakings by APP entities to take, or refrain from taking, specified actions which may be enforced in court if necessary; and

civil penalty orders - the power to apply to the Federal Court or Federal Circuit Court for a civil penalty order. The Federal Court will have the power to award significant civil penalties for serious or repeated breaches of privacy. Penalties of up to $1.7 million can apply to body corporates and $340,000 to APP entities that are not body corporates, including individuals.

PRIVACY COMPLAINTS

The OAIC can investigate privacy complaints from individuals about our business if we are specifically caught by the *Privacy Act* (Privacy Act).

Before a client can lodge a complaint with the OAIC, they will generally need to complain directly to ourselves and allow 30 days for it to respond. If they do not receive a response within 30 days, or they are dissatisfied with our response, they may then complain to the OAIC.

Complaints to the OAIC must be made in writing. Further information on the complaints process is available for clients wishing to complain regarding a Privacy Breach at www.oaic.gov.au.