

## PRIVACY POLICY

As a business that collects and holds personal information about our clients, we must comply with Code Standard 5 of the Code of Professional Conduct for Financial Advice Services and adhere to the Privacy Act 2020 and its principles.

We only use client information for the purposes that we collect it for, and we do not underestimate the importance of keeping personal information secure during the collection, use, or authorised disclosure when providing our services.

Our key obligations:

- Ensuring all information is kept secure, whether physical or electronic, and can only be accessed by authorised people
- Only collecting information that is needed to provide our services
- Explaining what personal information will be used for when it is collected, and informing the client of their right to access and/or correct their information anytime they wish to
- Only using personal information for those purposes that have been authorised by the client
- Returning or securely disposing of client information once it is no longer needed
- Reporting any data breach that may cause harm to the client/s to the Privacy Commissioner, affected individuals and the FMA.
- Ensuring that all personal information that is collected is protected by safeguards that meet the requirements of New Zealand's privacy laws, including all information that is transferred offshore

### **What is personal information?**

The Privacy Commission provides the following definition on their website:

*Personal information is any piece of information that relates to a living, identifiable human being. People's names, contact details, financial health, purchase records: anything that you can look at and say, "this is about an identifiable person."*

It does not need to include the client name and does not need to be secret or sensitive in nature. It is any information that could be used to identify an individual.

## **The Process**

### **1. Client Authorisation**

When meeting a client for the first time, we discuss the services that we offer and explain the process followed when providing advice. This involves asking the client to complete a Personal Information Authority & Declaration that outlines:

- The purpose for collecting the client's personal information
- What the information will be used for when providing the service
- Permission to obtain information for assessing suitability of products and/or providers
- Consent to send electronic marketing material

- Authorisation to share the information with a third party for the purposes of quality assurance, complaint management or to meet regulatory obligations.
- The clients right to access, review and correct any information that we hold about them

We do not provide any personal information, either verbal or written, without explicit consent from the client.

## **2. Office Security**

- Any time the office is unattended, it is locked.
- We do not work with physical files unless it is necessary. We primarily work online and access all documents via the cloud.
- When files are not being worked on, they are filed away so that there is no unauthorised access to a client's personal information.
- All computers, laptops and electronic devices as well as software programmes are password protected so that they can only be used by those that are permitted.
- We only respond to emails or share information once we are able to verify that we are speaking with the client requesting the information.

## **3. Data Security**

- All electronic devices and software programmes are password protected.
- We only use internet connectivity or emails where there is a secure WiFi network and an inability for others to access data.
- We only use trusted third party service providers that abide by the Privacy Act 2020 and include assurances in their business agreement or contract.
- Our business uses a Customer Relationship Management platform (CRM) provided by The Adviser Platform. Details of how The Adviser Platform fulfils their obligations under The Privacy Act 2020 are included in The Adviser Platform (TAP) Data Privacy & Protection Overview, available on their website.
- Where laptops or electronic devices are unaccounted for, we update passwords for all applicable software programmes to prevent the chance of unauthorised access.
- The CRM provided by The Adviser Platform only allows a user to be logged into a single device at any one time and all users are logged out after a period of inactivity.

## **4. Use of Information**

We only use information for the purposes it is intended and only after the client has given authorisation to do so. Their information may be used for the following purposes:

- Determining suitability of products for the client's needs
- Applying for products supplied by one of our providers
- Underwriting requests from providers when making an offer of terms
- Submitting claims to a provider on the client's behalf
- Quality assurance purposes
- Third party compliance services
- Regulatory requests
- Third party offerings that are necessary in the provision of my services to the client

- Electronic marketing (where consent has been given) with the ability for the client to unsubscribe from further electronic marketing material

All personal information will be handed back to the client and/or destroyed once it is no longer required and at the client's request. We require the information to be held on file for 7 years following the end of the client relationship.

### **5. Breach of Privacy**

Where a breach of privacy is suspected, it is reviewed for potential harm to determine what immediate action needs to be taken to prevent any further breach.

If it is concluded that a breach of privacy has occurred, we notify the affected individuals of the breach and let them know how their privacy has been breached, what steps we are taking to limit the breach, and confirm that we will be reporting the breach to the Privacy Commissioner.

We then notify the Privacy Commissioner using the NotifyUs function on the website of the Privacy Commission:

<https://www.privacy.org.nz/privacy-for-agencies/privacy-breaches/notify-us/>

Where it is determined that there has been a breach of privacy or there was the potential for a breach to have occurred, it is recorded in our Incident & Breach Register and treated in line with our Material Issues and Reporting Policy.

### **How compliance is monitored**

Tom Clarke is the nominated Privacy Officer and is responsible for understanding our responsibilities under the Privacy Act 2020.

We review all our advice files for accuracy and compliance with our obligations under this policy.