The Adviser Platform (TAP) Data Privacy & Protection Overview

Both the Privacy Act 2020 and Code Standard 5 of the Code of Professional Conduct for Financial Advice Services (Protect Client Information) require an adviser to ensure that the information their clients share with them is protected from unauthorised access.

Where an adviser business appoints a third-party service provider (such as TAP) to process personal information on its behalf, the adviser business will remain responsible under the Privacy Act 2020 for ensuring that the Information Privacy Principles (including the security requirements in Principle 5) continue to be met.

TAP utilises both local and offshore staff to provide the services. Any organisation operating in New Zealand is required to comply with the Privacy Act 2020, regardless of where the organisation is based.

Services provided by TAP either in NZ or offshore are provided inline with safeguards set out in the NZ Privacy Act 2020.

To ensure that adviser businesses meet their obligations under the Privacy Act 2020 and deliver services without putting client information at risk, TAP has put measures in place to protect client information.

The Technology behind The Adviser Platform CRM

- The TAP CRM is built using Google OAuth 2.0 protocol for authentication and authorization of TAP APIs.
- Only valid domains are granted web services or application access to their own data stored in Microsoft Azure.
- Each user is granted access to the CRM’s functionalities based on the security groups assigned to them.
- Both the CRM and the API are exchanging data in a secure HTTPs connection (SSL) along with Google's authorization sequence that utilizes a unique access token to validate requests of each API call.
- Microsoft Azure provides a firewall that prevents network access to the server until it is explicitly granted, SQL Authentication for permission control, and Advance Threat Protection to detect unusual behaviour and potential harm.
- Each business has data stored in its own database, making sure that specific business can only access their own information. Each database is replicated on a secondary database through Microsoft Azure's geo-redundancy as part of its Disaster Recovery Plan.
- Adviser businesses’ CRM portals are protected so that only authorised TAP staff are able to have access.
- TAP has the ability to review who has accessed CRM data and when at any time.

TAP Support Staff

- TAP support staff are suitably recruited and screened before commencing employment.
- All employment contracts include privacy and confidentiality clauses in line with NZ standards.
- TAP support staff work in teams with suitable management oversight and quality assurance programs in place.
- Cellphones and/or cameras are not permitted in working areas of the admin support office.
- TAP support staff members can only access data for the specific businesses that they are assigned to. Access is only granted via an email account linked to the specific business's domain.

Office Security

- TAP support staff assigned to carry out services operate from an office that is set up with biometric security meaning that they can only access the building with the use of fingerprint identification.
- The office is under video surveillance at all times with 3 months' retention of data.
- The building is monitored 24/7 by security staff.

Workstation Security & Data Loss Prevention

All computers accessed via TAP's support staff have:

- Enterprise Grade Antivirus (Webroot Endpoint Protection).
- Custom security settings.
- Disabled USB ports.
- Disabled administrator access.
- Auto-lock workstations.
- Patch Management and Security Updates.
- Webroot Antivirus to protect against cyber threats.
- Protection via the Cisco Umbrella Cloud Base Firewall which features content filtering and protects against malware and phishing attacks.
- Quarterly/Annual Audit by external firm.

In line with obligations under the Privacy Act 2020, TAP has a nominated privacy officer. It is their duty to:

- Be familiar with the privacy principles in the Privacy Act.
- Work to make sure the organisation complies with the Privacy Act.
- Manage any complaints from the organisation's clients about possible privacy breaches.

- Manage requests for access to personal information, or correction of personal information.
- Act as the organisation's liaison with the Office of the Privacy Commissioner.

If you have any concerns about a potential breach of the Privacy Act, please contact TAP's privacy officer, Scott Duncan, using one of the following methods:

Email: scott.duncan@tapnz.co.nz
Post: The Adviser Platform
1 Beaumont Street
Freemans Bay
Auckland 1011
New Zealand