PART 1 – PRIVACY POLICY

Purpose

Omnium acknowledges the importance of having an effective and efficient Privacy Policy in accordance with the Australian Privacy Principles (APP's). The Privacy Amendment act introduced significant changes to the Privacy Act 1988 (Cth) (Privacy Act). This Policy provides guidance on how Omnium its entities, officers, advisers, agents, and employees who collect, use and retain personal and sensitive information will comply with the APP's.

Overview

Omnium intends that this policy will apply to all entities of the group and the Privacy Amendment Act states that the APPs apply to individuals, body corporates, partnerships, unincorporated associations or trusts unless they are a small business operator.
For Omnium the privacy policy applies to users of Omnium services.

Definition

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
Whether the information or opinion is true or not; and
Whether the information or opinion is recorded in a material form or not.

AUSTRALIAN PRIVACY PRINCIPLES (APP)

APP1 – Open and transparent management of personal information

Omnium will provide training as and when required to ensure persons to whom this policy applies are aware of their obligations under the APPs. All clients of Omnium are entitled to access their private information upon request. Any complaints regarding the handling of private information shall be referred to the Omnium complaints policy.

How Omnium manages private information will be set out in this policy. This policy shall be made available on websites operated by Omnium and its related companies, agents, and representatives.

On request, clients are to have free access to this policy in any form requested, so long as it is practical to do so.

Members of the Omnium group may collect and hold personal information such as a person's name, address, date of birth, income, tax file number (TFN), ABN, ACN and such other information that may be required from time to time to provide services to clients. This is collected directly from its clients and personal information is held by either company within the Omnium group or its advisers and agents. Any personal information collected by Omnium is solely for the purpose of providing services to clients and meeting licensing obligations and is not to be used for any other purpose without consent. Clients may seek access to their personal information by contacting the appropriate entity of the Omnium Group. If a correction is required to that personal information the client may make that amendment by notifying the appropriate entity within the Omnium Group.

If a client is not satisfied with the outcome of their complaint, they may lodge a complaint with the Office of the Australian Information Commissioner (OAIC). Further information is available on the OAIC's website at www.oaic.gov.au.

Omnium will only disclose personal information of its clients to overseas recipients where such disclosure is required to give effect to the instructions of a client. It is not practical to list all countries to which this applies due to the variety of international financial services available to clients.

APP2 – Anonymity and Pseudonymity

As Omnium and its entities deal primarily with clients in financial services, it is unlikely that it would be practical for services to be provided to those clients without them having identified themselves. Further, in most situations companies within the Omnium group will be required under the terms of the Anti-Money Laundering and Counter-terrorism Financing Act 2006 (Cth) (AML/CTF Act) to appropriately identify clients.

APP3 – Collection of solicited personal information

Omnium is required to collect only information that is reasonably necessary for one or more of its functions. To meet legislative requirements, it is envisaged that Omnium will be required to collect the information needed to comply and store that information including Tax File Number (TFN) and personal medical information.

Where personal information is required to be obtained from clients for them to be provided services from entities within Omnium, those entities must consent to the collection of their personal information.

Omnium entities may be provided with personal information collected from clients of non-related entities for the purpose of providing the services offered by Omnium entities. The information collected from 3rd parties is collected and used only for the purpose of the specific service and is not disclosed or used for any other purpose.

APP4 – Dealing with unsolicited personal information

Omnium entities in receipt of information detailed above should review whether that information could have been necessary or obtained under APP3 and if not then take action to destroy or de-identify that information if it is lawful and reasonable to do so. (For example documents of a personal nature (photos letters emails) accidently included in other information provided).

APP5 – Notification of the collection of personal information

If entities of Omnium utilise 3rd parties to collect information, then they are obliged under this policy to provide the above information.

APP6 – Use and disclosure of personal information

Entities of Omnium if approached for the disclosure of personal information outside its normal business practices (including those above) then approval should be sought from the Privacy Officer.

Personal Information is held, used and disclosed for the primary purpose of enabling Omnium clients to advise and market to their customers and prospective customers. In most circumstances, Omnium clients collect Personal Information which is then disclosed back onscreen, and in written reports or data feeds.

The following conditions will also apply to the use of personal information;

- Omnium may also disclose Personal Information to the extent required or authorised by applicable law. Otherwise, no client data that would breach client privacy is disclosed to any third party.
- Omnium does not sell any Personal Information.
- Omnium may use and sell anonymous data on client quotations made through our service, for the purpose of market analysis and research. Any identifying client data will be removed.
- Omnium does not disclose Personal Information to unauthorised overseas recipients, although data which includes Personal Information may be accessed by Omnium staff located worldwide.
- Omnium applies the highest standards of personal information protection. However, Omnium cannot guarantee the ultimate security of this information. Omnium will not be liable for the loss or misuse of personal information as a result of a security breach of its systems.

APP7 – Direct marketing

Entities of Omnium have direct marketing approved by the licensee and for the purposes of this policy any marketing material that is explicitly provided for clients, e.g., monthly newsletter should provide those clients with an ability to opt-out.

Clients of Omnium can elect to opt-out of receiving direct marketing materials the Privacy Officer at Omnium.

APP8 – Cross-Border disclosure of personal information

Other than in the circumstances outlined in APP1 or financial products and services approved by Omnium, entities of Omnium shall seek approval from the Privacy Officer prior to establishing arrangements that would see personal information transferred out of Australia without the clients' prior approval. (e.g., utilising an overseas based accounting organisation to provide work).

APP9 – Adoption, use or disclosure of government related identifiers

Omnium entities shall not use for example a tax file number as a client reference for filing purposes.

APP10 – Quality of Personal Information

Omnium entities are required to update information held on a regular basis and should not rely on outdated information.

APP11 – Security of personal information

All Omnium entities take reasonable steps to ensure that data is securely stored including password protection on computer files and confidential destruction of paper records.

APP 11 requires Omnium entities to take reasonable steps to destroy or de-identify personal information if the organisation no longer needs it for any authorised purpose.

Under APP 11 there are two exceptions to this requirement:
the personal information is contained in a Commonwealth record, or
the organisation is required by or under an Australian law or a court/tribunal order to retain the information.

Omnium takes reasonable steps to:

- protect Personal Information that is held from misuse, interference and loss and from unauthorised access, modification or disclosure.
- ensure that all data is appropriately backed-up to prevent the loss of Personal Information; and
- destroy or de-identify Personal Information when it is no longer required.

Security measures that are in place to protect Personal Information include the following:

- physical access to Omnium premises is limited;
- policies on document storage security;
- apply website protection security measures;
- all staff are required to sign confidentiality agreements and undergo relevant background checks; and
- ensuring that any third-party providers have appropriate security safeguards to keep Personal Information secure.

APP12 – Access to personal information

Omnium collects Personal Information directly or indirectly from its clients e.g. financial advisers who have an agreement directly with Omnium or through their AFS Licensee. Omnium clients collect Personal Information and enter it into Omnium data stores through secure web applications.

Omnium may also import information from client databases. Omnium holds this Personal Information on secure servers within Australia. Omnium uses the services of Amazon Web Services (AWS) to host its software and personal data. All client information is stored on servers

located in Australia. While Omnium keeps all Personal Information on servers operated by AWS, it always remains under Omnium's effective control. The server host's role is limited to providing a hosting and storage service to Omnium.

If an organisation charges an individual for giving access to the individual's personal information, the charge must not be excessive, and must not apply to the making of the request.

Privacy Complaints

If a client believes that a breach of the APPs has occurred, they can direct their complaint to the Privacy Officer.

The relevant contact details are:

Privacy Officer
24/10 Gladstone Rd
Castle Hill NSW 2153

Tel: 1300 885 871
Email: admin@omnium.com.au

If a client is not satisfied with the outcome of their complaint, they may lodge a complaint with the Office of the Australian Information Commissioner (OAIC). Further information is available on the OAIC's website at www.oaic.gov.au.

Non – compliance with this policy

Non-compliance with this Policy may result in disciplinary action including the termination of a relationship with Omnium if the breach is considered serious.

If you are uncertain about this policy, then contact the Privacy Officer on 1300 885 871.

PART 2 – COMPLAINTS POLICY

Introduction

For the purpose of this Privacy Policy, Omnium Technologies Pty Ltd ('Omnium') consists merely of its officers, agents, employees, contractors, and representatives who will be bound under these arrangements.

This policy is reviewed regularly by Omnium.

Overview

Australian Financial Services Licensees (AFSL) are required to have a publicly available and a readily accessible policy document on how it intends to comply with the requirements outlined in the Regulatory Guide (RG) 271. You may also contact us if you would like to know about our Internal Dispute Resolution (IDR) policy.

You may contact us via online, email, phone or may do so in person. If you need additional assistance, you may contact us directly or your adviser who might be able to assist.

What happens next?

- We will acknowledge your complaint within 24 hours in writing
- We will contact you if we need any clarification
- We will review your complaint which may require requesting additional information from your adviser.
- If we can resolve your complaint within 5 days of receipt, we will advise you but may not provide a written response unless you request in writing.
- In any case, we will respond to your complaint within 30 days of receipt in writing.
- If we are unable to respond within 30 days due to certain circumstances beyond our control, we will contact you to advise you of the delay.
- If you are not satisfied with our response, you may refer the matter to:
    - Australian Financial Complaints Authority (AFCA)
        - GPO Box 3, Melbourne VIC 3001
        - Ph: 1800 931 678