Data & Privacy Policy

US Masters Responsible Entity Limited
ACN 672 783 345, AFSL 553 794

Contents

Definitions

Act or Corporations Act means the Corporations Act 2001 (Cth)

AFSL or AFS licence means Australian Financial Services Licence

ASIC means the Australian Securities and Investments Commission

ASX means ASX Limited (ACN 008 624 691)

Australian Law includes, without limitation, Corporations Act, Corporations Regulations and ASIC regulatory guidance

Board means board of Directors of the Company

Company means US Masters Responsible Entity Limited (ACN 672 783 345, AFSL 553 794)

Compliance Officer means the Compliance Officer of the Responsible Entity

Corporations Regulations means Corporations Regulations 2001

Director means the director of the Company

Fund means US Masters Residential Property Fund (ARSN 150 256 161)

Management Trust means US Masters Residential Property Fund II (ARSN 676 798 468)

Responsible Entity means the Company

Responsible Manager means the responsible managers nominated by the Responsible Entity under its AFSL

Retail Trust means the Fund

Privacy Act means The Privacy Act 1988

Stapled Security means URF

URF refers to each unit in the Retail Trust stapled to a unit in the Management Trust to form the stapled vehicle

Background

US Masters Responsible Entity Limited ACN 672 783 345 (**Company**) is a wholly owned subsidiary of the **Management Trust** which is stapled to the Fund (**Retail Trust**) to form the stapled listed vehicle, URF.

US Masters Responsible Entity Limited is the responsible entity of both the Management Trust and the Retail Trust and is the holder of Australian Financial Services Licence Number 553 794.

Overview

This policy sets out the procedures adopted by the Responsible Entity to manage its obligations under the Privacy Act. The Responsible Entity is subject to legislative and regulatory requirements to obtain and hold detailed information which personally identifies and/or contains information or an opinion about an individual ("personal information").

This means that any information collected on an individual for the purposes of providing financial services including the collection, use and disclosure, among others, must comply with the relevant provisions under the Privacy Act.

The Privacy Act has specified thirteen Australian Privacy Principles (**APPs**) regarding circumstances, under which personal information may be collected, used, disclosed and corrected. A breach of any of those principles may constitute interference with the privacy of the individual. An affected individual may complain to the Office of Australian Information Commissioner (**OAIC**). Where appropriate, the individual may seek compensation for interference their privacy.

The Responsible Entity maintains a separate public facing Privacy Policy and has adopted this internal policy to ensure staff comply with the relevant provisions of the Privacy Act.

In this policy:

- personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable; and

- sensitive information means personal information about an individual's health (including health services provided to them), genetics, biometrics, 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.

Public Privacy Policy

The Responsible Entity has developed a public-facing Privacy Policy which details how the Responsible Entity handles the privacy of client information.

The public-facing Privacy Policy contains the following information:

- the kinds of personal information collected and held;

- how personal information is collected and held;

- the purposes for which personal information is collected, held, used and disclosed;

- how an individual may access personal information about the individual that is held and seek the correction of such information;

- how an individual may complain about a breach of the APPs and how a complaint would be dealt with;

- whether personal information is likely to be disclosed to overseas recipients and if likely, the countries in which such recipients are likely to be located.

The public-facing Privacy Policy is available on the URF website. The public-facing Privacy Policy does not need to be systematically provided to clients. However, as it is a requirement to provide this document on request, it is also the Responsible Entity's policy that the full policy will be promptly provided when requested.

In addition to this policy, a privacy statement's may be utilised to inform the client of the key aspects of this policy. A privacy statement specifically states who is collecting the information, the purpose of the collection, if it is required/authorised by law, to whom the information will be disclosed, how the client may access and correct the information, and how to complain about a breach.

Where a third party is collecting information on behalf of a business unit e.g. a unit registry, the external service provider must provide their relevant privacy statement. This is considered as part of the due diligence processes when considering outsourcing a function or engaging an external service provider.

Privacy Officer

The Compliance Officer of the Responsible Entity will act as the Privacy Officer to oversee the Responsible Entity's privacy framework. The Compliance Officer will be responsible for implementing practices, procedures and systems relating to the Responsible Entity's functions and activities to ensure that it complies with and is able to deal with any inquiries or complaints about compliance with the APPs and this policy.

The Board will be responsible for reviewing the compliance measures including data handling practices on an ongoing basis and more formally at the quarterly Board compliance meetings.

The Compliance Officer will be responsible for reviewing and updating this policy, privacy statements and related documents and procedures as necessary.

Managing, monitoring and supervision of information

All staff are expected to comply with the Responsible Entity's practices, procedures and systems, in particular privacy related matters on an ongoing basis.

The Responsible Entity has adopted a number of processes and guidelines to assist the staff in meeting privacy and information related obligations. These include:

- providing access to the Responsible Entity's compliance policies;
- providing training to staff on data handling, cyber security and client information collection, storage and use on an ongoing basis;
- providing and requiring the use of template personal information collection forms;
- monitoring changes to privacy laws and industry practises and obtaining external advice where necessary;
- monitoring changes to business processes to ensure that any privacy procedure implications are considered;
- engagement of the Privacy Officer to assess projects to determine whether there are any possible risks involving information and form mitigation strategies;
- promoting a culture of continuous improvement and regulatory compliance; and
- monitoring and supervising compliance with the Responsible Entity's data handling practices.

Collection of personal information

Personal information must only be collected by lawful and fair means. Personal information about an individual should only be collected if:

- for personal information - it is reasonably necessary for one or more of the Responsible Entity's functions or activities; or
- for sensitive information - there is consent for the collection of the information and it is reasonably necessary for one or more of the Responsible Entity 's functions or activities; or
- there is approval from the Privacy Officer to collect the information where required or authorised by law.

Where personal information is collected, there are two key requirements that must be followed under the Privacy Act when providing advice or a service:

- provide information about the collection, use, security and disclosure of personal information. The Responsible Entity has a documented public-facing Privacy Policy on its website and provides a privacy statement within its Financial Services Guide;

- obtain client consent to the collection, use and handling of personal information either at or before the time of collection (or as soon as practicable after). Consent to collect information for the purpose described in this policy is generally through completion of relevant service agreements and application forms.

Consent may also be implied when an individual willingly provides personal information verbal in conversation or via the website. Consent can be implied as the client has discretion as to how much information they are prepared to provide and also have the ability to act anonymously.

Records of the above documents, including the individual's name, the date consent was given and the way in which the consent was given (e.g. email) are saved electronically.

Personal information about an individual should only be collected directly unless it is unreasonable or impracticable to do so. Where it is unreasonable or impracticable to collect personal information about an individual directly then information may be collected from a third party or a publicly available source. For example, an individual may provide the Responsible Entity with authority to contact an accountant, or another corporation on their behalf to collect personal information. Generally, third parties should not be used to collect any personal information on behalf of the Responsible Entity unless there is approval from the Privacy Officer.

Where personal information has been received by the Responsible Entity which has not been solicited or it is determined that the Responsible Entity would not have normally collected the personal information, the information must be destroyed or de-identified as soon as reasonably practicable but only if it is lawful and reasonable to do so.

Use and disclosure of personal information

The Responsible Entity, either itself or through external service provides (i.e., unit registry) holds and uses personal information about an individual to provide the products and services requested, to understand and meet the individuals' needs and provide a wide range of financial and other products and services. As per the Privacy Policies, the Responsible Entity may also use and disclose personal information:

- to provide information about a product or service and/or consider whether an individual is eligible for a product or service;

- to process an application for a product or service and/or administer the product or service provided;

- to run Responsible Entity's business and perform administrative and operational tasks such as training staff, developing and marketing products and services, risk management, systems development and testing, including our websites and other online channels, undertaking planning, research and statistical analysis;

- to identify individuals and prevent or investigate any fraud or crime, or any suspected fraud or crime;

- if it will prevent or lessen a serious and imminent threat to somebody's life or health;

- as required by law and regulation or codes binding us, including the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Foreign Account Tax Compliance Act (FATCA) in the U.S.; and

- for any purpose for which the individual has provided express (verbal or written) or implied consent.

Other than these circumstances, generally, to use or disclose personal information, there must be consent from the individual or the individual would reasonably expect the use or disclosure of the information for that purpose.

Approval from the Privacy Officer should be obtained if there is uncertainty around the use or disclosure of personal information.

Information must also not be disclosed to a third party unless authority has been given by the relevant individual e.g. to liaise with an accountant or approved by the Privacy Officer. This is to ensure the third party complies with the APPs and this policy in respect of the handling of such personal information.

Storage and security of personal information

All staff must take reasonable steps to protect personal information that the Responsible Entity holds from misuse, interference and loss and from unauthorised access, modification or disclosure.

The Responsible Entity ensures personal information is protected by implementing the following security measures:

- educating staff as to their obligation with regard to personal information and taking appropriate disciplinary action where there is a breach;
- only giving access to personal information to person who is verified to be able to receive that information;
- electronic security systems, such as firewalls and data encryption on the URF website;
- appropriate security access to office premises;
- providing secure storage for physical records;
- the use of passwords to access database information;
- removal or blacking out identifiers; and
- document shredders/secure storage bins for the disposal of written information.

Access to personal information

Requests for access to limited amounts of personal information, such as checking to see what address or telephone number the Responsible Entity has recorded, can generally be handled over the telephone by the appropriate staff. Requests for access to more substantial amounts of personal information, such as details of what is recorded in a client file are to be made to the Privacy Officer. The Privacy Officer will provide instructions on how to proceed with the request and communication required.

In advising on how to proceed in regard to providing access to information, the Privacy Officer will consider:

- whether there is a complaint history or a current complaint relating to the individual. If a complaint is in process, the Privacy Officer should confer with the professional indemnity insurer and/or legal advisers prior to processing the request;
- whether the file contains any sensitive documents that may adversely affect the position or reputation of the Responsible Entity or its staff. The Privacy Officer may liaise with the staff to assess this;
- whether the file contains any information or documents that may be legally privileged or subject to a lien; and
- whether there are any constraints (i.e. time, physical, monetary) which will affect the issuance of such information. The Privacy Officer will determine and inform the staff of a suitable delivery of the information requested, to overcome these constraints.

Without being required to follow the above procedures, the Privacy Officer is able to authorise straightforward requests for information, which may include a summary of personal information held on file, copies of data collection type forms, or copies of all correspondence issued to the client.

The Privacy Officer may not provide an individual with access to the personal information that the Responsible Entity holds if:

- giving access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;

- giving access would be unlawful; or

- denying access is required or authorised by law.

The Privacy Officer will give an individual access to personal information in the manner requested if it is reasonable and practicable to do so.

If the Privacy Officer decides not to give an individual access to personal information or such access in the manner requested, then the Privacy Officer will:

- take reasonable steps to give access in a way that meets both the individual and the Responsible Entity's needs (which may involve giving access through a mutually agreed intermediary); and

- give a written notice that sets out the reasons for the decision (except to the extent that it would be unreasonable to do so) and mechanisms available to complain about the decision.

Details of all significant requests will be kept in register and will generally include details of: the client name, address, staff member name, date of request, nature of request, date request completed and the authorisation provided or reason why request was denied. The Privacy Officer will respond to a request by an individual for access to personal information within 14 working days, unless impracticable to do so, in which case the Privacy Officer will inform the individual(s) involved.

The Responsible Entity will not charge an individual for making a request to access personal information. A reasonable fee may however be charged to recover the cost of retrieving the information and providing it to the person requesting the information.

Correction of personal information

The Board authorises certain staff to take reasonable steps to correct personal information held about an individual to ensure, having regard to the purpose for which the firm holds the information, that it is accurate, up-to-date, complete, relevant and not misleading. It may be updated where those staff are satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading or the relevant individual requests the information to be corrected.

Subject to the APPs, and this policy, where reasonable and practicable and not unlawful to do so, the Responsible Entity will correct personal information about an individual that has previously been disclosed to another organisation or where requested by that individual.

The Privacy Officer must be referred to where any requests by an individual to correct personal information appear inaccurate, out-of-date, incomplete, irrelevant or misleading.

If the Privacy Officer decides not to correct any personal information that the Responsible Entity holds about an individual, then the Privacy Officer will:

- give the individual a written notice that sets out the reasons for the decision and the mechanisms available to complain about the decision; and

- upon request take reasonable steps to associate with the information a statement apparent to users that it is inaccurate, out-of-date, incomplete, irrelevant or misleading.

The Privacy Officer will aim to respond to a request for correction by an individual within 14 working days, unless impracticable to do so, in which case the Privacy Officer will inform the individual(s) involved.

The Responsible Entity will not charge an individual for making a request for the correction of his or her personal information or for associating a statement with the information.

Compliance with this Policy

The Board of the Responsible Entity is committed to maintaining compliance with all applicable laws and regulations governing its AFSL and to acting in the best interests of the members of URF. The Board expects all Responsible Managers, staff, consultants and service providers to comply with this policy. Failure to comply with the policy may result in disciplinary action, including termination of employment of the Responsible Manager, staff or the engagement of a service provider or consultant.

Policy Review

The Board and the Compliance Officer will ensure this policy is reviewed at least annually or immediately after a change to privacy laws or regulations. A summary of changes to this policy following a review will be documented in the ‘Version Control’ table below.

Training

The Responsible Entity will ensure all new staff, consultants and Responsible Managers will be provided with privacy training as part of their induction process. All staff, consultants and Responsible Managers will be expected to attend refresher training sessions on the Responsible Entity’s privacy policies and procedures which will be provided on a periodic basis.