PM Capital - PRIVACY POLICY (WEBSITE VERSION)

Version:

Issue: April 2018

Issued by: PM Capital Limited

ABN 69 083 644 731, AFSL 230222

Registered address: Level 27, 420 George Street
Sydney NSW 2000

Privacy of your personal information

About this policy
PM Capital Limited ("PM Capital", "we") acts as the Responsible Entity for several managed investment schemes (collectively the 'Schemes') and various external mandates.

PM Capital recognises the importance of, and is committed to, protecting the privacy of individuals when handling their personal information. We consider that our behaviour in relation to privacy to be a reflection of our commitment to meeting high compliance and ethical standards.

The PM Capital Privacy Policy ('Policy') explains in an open and transparent manner how PM Capital will collect, hold, use, disclose, protect and otherwise handle our clients' personal information in accordance with the Australian Privacy Principles contained in the Privacy Act 1988 (Cth).

When you provide PM Capital with personal information you consent to its use, disclosure and handling of your personal information in accordance with this Privacy Policy as amended from time to time.

A copy of this Policy it is available for download from our website at www.PM Capital.com.au, or a copy of the Policy can be obtained from us (free of charge) on request. Should you require a copy of this policy it is available for download or we can post you a copy at your request.

We may update this Privacy Policy from time to time to take into account changes in our practices for the handling of personal information, or to relevant legislation, by publishing an amended Privacy Policy on our Website. You should regularly review the most recent version of this Privacy Policy available on our Website.

1. THE AUSTRALIAN PRIVACY PRINCIPLES

The Australian Privacy Principles (APPs), which are contained in schedule 1 of the Privacy Act 1988 (Privacy Act), outline how PM Capital must handle, use and manage personal information.

While the APPs are not prescriptive, PM Capital takes such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to its business functions or activities that:

(a) will ensure that PM Capital complies with the Australian Privacy Principles and a registered APP code (if any) that binds us; and
(b) will enable PM Capital to deal with inquiries or complaints from individuals about our compliance with the Australian Privacy Principles or such a code.

The APPs cover:

- the open and transparent management of personal information including having a privacy policy;
- an individual having the option of transacting anonymously or using a pseudonym where practicable;
- the collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection;
- how personal information can be used and disclosed (including overseas);
- maintaining the quality of personal information;
- keeping personal information secure;
- right for individuals to access and correct their personal information.

There are also separate APPs that deal with the use and disclosure of personal information for the purpose of direct marketing (APP 7), cross-border disclosure of personal information (APP 8) and the adoption, use and disclosure of government related identifiers (APP 9).

1.1 What is personal information?

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

Note: Section 187LA of the Telecommunications (Interception and Access) Act 1979 extends the meaning of personal information to cover information kept under Part 5-1A of that Act.

2. PERSONAL INFORMATION COLLECTED AND HELD

PM Capital collects personal information directly from you (and/or through our intermediaries) for the purposes of providing to you our investment services and products.

The kinds of personal information that we may collect and hold includes:

- your name;
- place and date of birth;
- tax file number (and other international tax numbers, and residency details);
- email address;
- home address;
- telephone number(s);
- the source of your funds/monies;
- bank account details.

Where you do not provide us with some or all of your personal information that we request then we may not be able to provide you with our products or services.

PM Capital may hold personal information collected in both physical and electronic storage facilities including paper-based files and computer databases.

Electronic records are maintained by a cloud hosting service provider or other third party storage or server provider. All such personal information is maintained with in the effective control of PM Capital. We have arrangements which require third party service providers to maintain the security of the information and we take reasonable steps to protect the privacy and security of that information, however, we are not liable for any unauthorised access or use of that information.

2.1 How is personal information collected?

Personal information may be collected by a variety of means, including by provision of completed Application Forms for our Schemes, in person, by telephone, letter, facsimile, or email. We may also collect personal information by subscribing to, or purchasing, marketing databases.

2.2 Internet and electronic data capture

PM Capital may use cookies, web beacons or similar technologies to collect de-identified information about your visits to our website www.pmcapital.com.au ("Website") for the purpose of improving your experience browsing our Website. As an example, should you visit our Website PM Capital may collect information about your operating system, browser type, pages accessed, documents downloaded, any previous visits, any referring website, including dates and times.

If you disable cookies in your browsers our website may not operate as it should.

Our online enquiry form on our Website also collects the personal information you enter. This information is used for the sole purpose of answering your enquiry.

3. HOW PERSONAL INFORMATION IS USED AND DISCLOSED

PM Capital may use and disclose personal information collected and stored to enable us to provide the financial services and products to you and for other related legal purposes. Accordingly, we may need to disclose your personal information to others, as follows:

- related entities: to related entities of PM Capital;
- your financial adviser or your service providers: to your agent, nominated financial adviser or service providers, with your permission;
- service providers under contract: who help with our financial services business operations included archival, auditing, legal, business consulting, banking, payment, delivery, data storage, data processing, data analysis, fund administration, registry, mailing, marketing, research, investigation, insurance, brokerage, maintenance, website and technology services – where we engage such services providers, our contracts provide that they may only use your personal information in connection with the services they perform for us;
- law enforcement, government agencies or other third parties as required by law: when we need to comply with law or credit card rules, or when we believe that the disclosure of personal information is necessary to prevent harm or financial loss, to report suspected illegal activity or to investigate contraventions of our loan arrangements; and
- credit bureaus, credit reporting agencies and collection agencies: to verify your identity by e-verification, or to obtain information about your source of funds.

3.1 Disclosure to overseas recipients

From time to time, PM Capital may disclose personal information to overseas recipients. These recipients may be in other countries where laws in relation to the processing of personal information are not consistent with the APPs or the Privacy Act.

Nevertheless, under in APP 8.1 we are generally required to implement reasonable steps to ensure that an overseas recipient does not breach the APPs. In this regard we will enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs (other than APP 1).

While PM Capital may take steps to try and ensure that these third parties do not breach the APPs in relation to your personal information, the overseas recipient may breach the *Privacy Act* and/or the Privacy Principles and this may be due to that countries own laws.

By providing us with your personal information you accept that we may make disclosures to overseas recipients on this basis.

3.2 Disclosure by approval

We will only use or disclose your information for the particular purpose for which it was collected, unless an exception applies. Exceptions include:

- you have consented to a secondary use or disclosure;
- you would reasonably expect the use or disclosure, and that is related to the primary purpose of collection or, in the case of sensitive information, directly related to the primary purpose;
- the use disclosure of the personal information is required or authorised by or under an Australian law or a court/tribunal order;
- a permitted general situation exists in relation to the secondary use or disclosure of the personal information by the us;
- we reasonably believe that the use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Under APP 8.27, PM Capital may disclose personal information to an overseas recipient without complying with APP 8.1 where:

- we expressly inform you that if they consent to the disclosure, this principle will not apply, and
- you consent to the disclosure.

4. PROTECTING YOUR PERSONAL INFORMATION

PM Capital takes all reasonable steps to protect your personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure using both physical and electronic security measures.

By providing us with your personal information by email, over the Internet, you accept that such information will be transmitted at your own risk as the security of such information cannot be guaranteed.

5. RETENTION OF PERSONAL INFORMATION

As required by APP 11.2, we take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under the Privacy Act.

Despite this we are further obligated under the Corporations Act (2001) (Cwth) to keep financial records for at least 7 years after the transactions covered by the records are completed. Accordingly, client records are retained for the period required (being at least 7 years) to allow us to satisfy our obligations under the Corporations Act.

6. DATA BREACHES

A data breach is when personal information held by an entity is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach are when a device containing personal information of clients is lost or stolen, an entity's database containing personal information is hacked or an entity mistakenly provides personal information to the wrong person.

A 'data breach' may also constitute a breach of the Privacy Act, however this will depend on whether the circumstances giving rise to the data breach also constitute a breach of one or more of the APPs, a registered APP code or the Privacy (Credit Reporting) Code 2014 (CR code).

6.1 Response to data breaches

PM Capital will consider four key steps when responding to a breach (or suspected breach) being:
Step 1: Contain the breach and do a preliminary assessment
Step 2: Evaluate the risks associated with the breach
Step 3: Notification
Step 4: Prevent future breaches

STEP 1: Contain the breach and do a preliminary assessment

Once PM Capital has discovered or suspects that a data breach has occurred, it should take immediate steps to limit the breach. These may include the following:

<u>Contain the breach</u>

1. Take whatever steps possible to immediately contain the breach.
2. Assess whether steps can be taken to mitigate the harm an individual may suffer as a result of a breach.

Initiate a preliminary assessment

The Head of Compliance (or delegate) will commence an initial assessment. This assessment will consider the following preliminary questions:

- What personal information does the breach involve?
- What was the cause of the breach?
- What is the extent of the breach?
- What are the harms (to affected individuals) that could potentially be caused by the breach?
- How can the breach be contained?

Consider who needs to be notified immediately

Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage. In some cases it may be appropriate to notify the affected individuals immediately (for example, where there is a high level of risk of serious harm to affected individuals).

If the breach appears to involve theft or other criminal activity, it will generally be appropriate to notify the police. If the data breach is likely to involve a real risk of serious harm to individuals, or receive a high level of media attention, inform the OAIC.

STEP 2: Evaluate the risks associated with the breach

To determine what other steps are immediately necessary, PM Capital will assess the risks associated with the breach.

The following factors will be considered in assessing the risks:

(a) The type of personal information involved.
(b) The context of the affected information and the breach.
(c) The cause and extent of the breach.
(d) The risk of serious harm to the affected individuals.
(e) The risk of other harms.

STEP 3: Notification

PM Capital will consider the circumstances of the breach, and:

(a) decide whether to notify affected individuals, and, if so
(b) consider when and how notification should occur, who should make the notification, and who should be notified
(c) consider what information should be included in the notification, and
(d) consider who else (other than the affected individuals) should be notified.

In general, if a data breach creates a real risk of serious harm to the individual, the affected individuals should be notified.

Refer to **Section 7.2** (below).

STEP 4: Prevent future breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, PM Capital will investigate the cause and consider whether to review the existing prevention plan or, if there is no plan in place, develop one.

A prevention plan should suggest actions that are proportionate to the significance of the breach, and whether it was a systemic breach or an isolated event.

This plan may include:

- a security audit of both physical and technical security

- a review of policies and procedures and any changes to reflect the lessons learned from the investigation, and regular reviews after that (for example, security, record retention and collection policies)
- a review of employee selection and training practices, and
- a review of service delivery partners (for example, offsite data storage providers).

The plan may include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.

6.2 Notification of data breaches

The passage of the Privacy Amendment (Notifiable Data Breaches) Act 2017 established a Notifiable Data Breaches ('NDB') scheme in Australia. The NDB scheme will commence on 22 February 2018, and only applies to eligible data breaches that occur on, or after, that date.

Information relating to handling data breaches is available at:
https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/

The NDB scheme requires PM Capital to notify any individuals likely to be at risk of serious harm by a data breach. This notice must include recommendations about the steps that individuals should take in response to the data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified.

PM Capital will conduct quick assessments of suspected data breaches to determine if they are likely to result in serious harm.

6.2.1 What is a Notifiable Data Breach?

A Notifiable Data Breach is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. A data breach occurs when personal information held by PM Capital is lost or subjected to unauthorised access or disclosure.

Examples of a data breach include when:

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.

The threshold tests which trigger the notice obligations are based on an objective test of what a reasonable person would conclude. There are some important exceptions to notification, in particular where remediation taken by PM Capital has reduced the risk of serious harm.

Key exception

There are a number of exceptions to the definition of eligible data breach. Most critically the unauthorised loss, access or disclosure of the information will not be an eligible data breach where, as a result of remedial action taken by the relevant entity in relation to the breach, before it results in serious harm to any individual to whom the information relates, a reasonable person would conclude that the loss, access or disclosure of the information is unlikely to result in serious harm to any of those individuals.

Similarly, if such action were taken in respect of particular individuals prior to serious harm occurring and a reasonable person would conclude that, as a result the loss, access or disclosure would not be likely to result in serious harm to those particular individuals, the entity will not be required to notify those individuals of the loss, unauthorised access or unauthorised disclosure.

What is serious harm?

Serious harm is broadly construed. The explanatory memorandum accompanying the Bill explains that serious harm could include serious physical, psychological, emotional, economic and

financial harm as well as serious harm to reputation. The Bill sets out a non-exhaustive list of relevant matters to have regard to when determining whether access or disclosure would likely to result in serious harm:

- the kind and sensitivity of the information;
- whether the information is protected by security measures and the likelihood any such security measures would be overcome including the use of an encryption key to circumvent the encryption technology or methodology;
- the persons or kinds of persons who have or could obtain the information;
- the likelihood that any persons who have or could obtain the information could obtain information or knowledge or circumvent any security technology or methodology applied to the information with the intent to cause harm;
- the nature of the harm; and
- any other relevant matters.

6.2.2 Assessment of suspected eligible data breaches

PM Capital is required to carry out an assessment if it:

1. is aware that there are reasonable grounds to suspect that there may have been an eligible data breach; and
2. is not aware that there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach.

PM Capital will take reasonable steps to ensure that the assessment is completed within 30 days after becoming aware of the reasonable grounds of the suspicion. The assessment must be a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible breach of the entity.

If the eligible data breach applies to more than one group entity, only one entity needs to undertake an assessment for all entities to comply with this requirement.

6.2.2 How to Notify?

Where PM Capital becomes aware that there are reasonable grounds to believe an eligible data breach has occurred, we will notify individuals at risk of serious harm and the OAIC as soon as practicable.

This notification must set out:

- the identity and contact details of the organisation;
- a description of the data breach;
- the kinds of information concerned; and
- recommendations about the steps individuals should take in response to the data breach.

If PM Capital becomes aware (whether by assessment, if required, or by other means) that there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity, PM Capital must meet the following notification obligations as soon as practicable:

1. Prepare a statement that sets out:
    - the identity and contact details of the entity and, if the eligible data breach relates to more than one entity, it may set out the identity and contact details of those other entities;
    - a description of the eligible data breach that the entity has reasonable grounds to believe has happened;
    - the kind or kinds of information affected;
    - recommendations about the steps that individuals should take in response; and
    - If the statement is being made under a direction from the Commissioner (discussed below), any specified information from the Commissioner's direction.

2. Give a copy of this statement to the Commissioner.

3. If it is practicable, take such steps as are reasonable to notify the contents of the statement to:
   - each individual to whom the information relates;
   - each individual at risk from the eligible data breach; and
   - in the method the entity normally communicates with the individual (if any).

4. If individual notification is not practicable, the entity must:
   - publish a copy of the statement on the entity's website (if any); and
   - take reasonable steps to publicise the contents of the statement.

Exemptions

The exemptions to the statement and notification obligations are:

1. if the eligible data breach applies to more than one entity, only one entity needs to undertake the statement and notification for all entities to comply;
2. where it would be likely to prejudice enforcement related activity of an enforcement body;
3. where it is inconsistent with a secrecy provision; and
4. at the Commissioner's direction (see below).

Commissioner's direction

The Commissioner may act on their own initiative or upon the application by PM Capital, to declare that the statement and notification obligations do not apply, or to extend the time for compliance. The Commissioner also has the power to direct PM Capital to comply with the statement and notification requirements. For this direction, PM Capital must be invited to make a submission.

In exercising these powers, the Commissioner must be satisfied that the direction is reasonable in the circumstances, having regard to the public interest, any relevant advice of an enforcement body and any other matters the Commissioner considers relevant.

PM Capital is not required to comply with a Commissioner's direction to comply with the statement and notification requirements, if it would be likely to prejudice enforcement related activity of an enforcement body.

7. ACCESS, CORRECTION AND COMPLAINTS

You may contact PM Capital during normal business hours to request that we provide you with access to any of your personal information held by us. We will deal with your request to provide access to your personal information within 30 days as required by this Policy and law. You should promptly notify PM Capital if you become aware that any of your personal information held is inaccurate, out-of-date, incomplete, irrelevant or misleading.

If you have any concerns about whether PM Capital has complied with this Policy, or the Privacy Act, please contact us as follows:

Compliance Manager
PM Capital Limited

Address: Level 27, 420 George Street
Sydney NSW 2000

Email: PMCapital@PMCapital.com.au
Telephone: +612 8243 0888
Fax: +612 8243 0880

Our Compliance Manager will investigate your complaint and advise you of the outcome. If you are not satisfied with our response you can complain to the Office of the Australian Information Commissioner as follows:

The Privacy Commissioner
Office of the Australian Information Commissioner

Post: GPO Box 5218
Sydney NSW 2001

Email: enquiries@oaic.gov.au
Telephone: 1300 363 992 (within Australia only)
Fax: +61 2 9284 9666