Water Dragon Solutions Pte Ltd, the Compliance Practice of
Maroon Analytics Pte Ltd
Sentient House
16 Stanley Street
Singapore 068735
www.maroonanalytics.com

Frequently Asked Questions re Personal Data Protection Framework

1) What are the different templates for?

The templates provide you templates for your crucial documents regarding personal data protection, i.e. to meet the requirements of the Personal Data Protection Act ('PDPA'). Please read each template carefully and amend it to fit the specifics of your company.

- Personal Data Protection Policy ('PDP Policy'; file "Personal Data Protection Policy - AIAM Template"): The PDP Policy provides a template for your policy on personal data protection. You may implement this policy as a separate policy or integrate it into your existing policies, e.g. as a chapter of your compliance and operations manual.
- Consent to Our Processing of Your Personal Data (Annex to Asset Management Agreement re Personal Data Protection; 'PDP Annex') (file "PDP Annex - AIAM Template"): The PDP Annex provides you a template for the document to submit to your future clients together with your asset management agreement to obtain their necessary consent for your collection, use and disclosure of their personal data. Alternatively, you may integrate this template into your asset management agreement.
- Personal Data Protection Notification & Consent (Letter for Client Notification and Consent re Personal Data Protection) (file "Client Notification & Consent - AIAM Template"): The Personal Data Protection Notification & Consent provides you a template for the document to submit to your existing clients to inform them of the PDPA and your personal data protection policy and to obtain their necessary consent for your collection, use and disclosure of their personal data.
- Consent to Our Processing of Your Personal Data (Annex to Employment Agreement re Personal Data Protection; 'EPDP Annex') (file "EPDP Annex - AIAM Template"): The EPDP Annex provides you a template for the document to submit to your future employees together with your employment agreement to obtain their necessary consent for your collection, use and disclosure of their personal data. Alternatively, you may integrate this template into your employment agreement.
- Consent to Our Processing of Your Personal Data (Employee Consent to the Processing of Their Personal Data) (file "Employee Consent - AIAM Template"): The Consent to Our Processing of Your Personal Data provides you a template for the document to submit to your existing employees to inform them of the PDPA and your personal data protection policy and to obtain their necessary consent for your collection, use and disclosure of their personal data.
- Singapore Data Protection Notice (Public Notice on Personal Data Protection) (file "Public Notice - AIAM Template"): An organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available (para. 2.2(i) Introduction to the Guidelines). An organisation must at least make available to the public the business contact information of the personal data protection officer (sec. 11(5) PDPA). Upon request, the organisation must make information available: (i) its data protection policies and practices and (ii) its complaint process (sec. 12(d) PDPA). As a result of these openness obligations, many organisations provide information about their data protection policy on their websites. The Singapore Data Protection Notice provides you a template for the text or document you may wish to publish on your website or make otherwise available to the public to meet your openness obligations.
  Please note that the Singapore Data Protection Notice is aligned to the PDP Policy. If you introduce

amendments into the PDP Policy, you should ensure that these amendments are also reflected in the Singapore Data Protection Notice as required.

2) Do we have to adopt the entire PDP Policy template?

The PDP Policy aims at covering all your duties under the PDPA. At the same time, considering the small size of most independent asset managers ('IAMs'), the PDP Policy– and the templates in general – attempts to limit the obligations in the PDP Policy to the strict requirements. It is remains your duty and responsibility to ensure that the template is amended to fit your specific company. If you feel that specific duties or obligations do not apply to your company, go beyond what is commensurate with the nature, scale and complexity of your business or don't cover all your operations, you should amend the template accordingly e.g. you may omit the provisions with respect to CCTVs, if you do not operate any CCTV cameras.

Two areas in the PDP Policy are not explicitly required by the PDPA, but are advised in the guidance provided by the Personal Data Protection Commission ('PDPC') and provide useful tools for the management of personal data.

- Personal data inventory map: The personal data inventory map is not required in the PDPA, but is only indicated in the checklist for companies by the PDPC. The personal data inventory map is a useful tool for the IAM to be aware how it collects, stores and discloses personal data.
- Annual review: The annual review is not required in the PDPA, but only indicated in the checklist for companies by the PDPC. Only regular reviews will however ensure the consistent compliance with the personal data protection regulations.

3) Does the PDP Policy also apply to the collection, use and disclosure of personal data in other countries?

The PDPA determines how data collected in another jurisdiction may be used and disclosed in Singapore and how data collected in Singapore may be used or disclosed in another jurisdiction. You may be able to collect personal data without the individual's consent in several countries (although most, if not all European countries have laws similar to the PDPA in place), but you will not be able to use or disclose such information in Singapore without the respective consent. In general, it is advisable that you maintain the same standards of personal data protection and apply the same policy in all your dealings, in particular with all your clients, in all jurisdictions. Indications on the general collection, use and disclosure of personal data in other countries are provided in the PDP Policy template.

4) When the client signs the asset management agreement, does he not automatically give consent to our collection, use and disclosure of his personal data? Is he required to sign a designated consent form?

A client who signs an asset management agreement may be considered to give deemed consent to the collection, use and distribution of his personal data for connected purposes. Deemed consent however exposes you to increased risk of disputes, in particular since there are little indications to the extent of activities and operations covered by the deemed consent. Moreover, you may wish to properly inform your client about your collection, use and disclosure of his personal data.

5) When our employee signs the employment agreement, does he not automatically give consent to our collection, use and disclosure of his personal data? Is he required to sign a designated consent form?

An employee who signs an employment agreement may be considered to give deemed consent. In addition, the PDPA provides for some exemptions regarding employment issues. These exemptions however leave some space for the general PDPA obligations. In order to comply with your information obligations, the

EPDP Annex (or Consent to Our Processing of Your Personal Data respectively) aims at fully informing your employees and obtaining their full consent.

6) Is an email good enough for a notice or acknowledgement in writing?

All consent should preferably be obtained in writing. The purpose of this is to have clear documentation of the consent. This is also achieved by email.

The organisation must provide an applicant access to the applicant's personal data requested by providing the applicant a copy of the personal data and use and disclosure information in documentary form (reg. 4(2) PDPR). The aim appears to be that the information is clearly documented. This is also achieved by email.

If the organisation is unable to grant access to personal data within 30 days after receiving a request made, the organisation must within that time inform the applicant in writing of the time by which it will respond to the request (reg. 5 PDPR). The aim of this provision appears to be to provide clear, unambiguous information. This is also achieved by email.

7) Do we need to issue a PDPA notice informing every patron walking into our premises about our closed circuit television ('CCTV') cameras?

Under the PDPA, the organisation is held to obtain the individuals consent before collecting personal data, including CCTV footage. The guidelines suggest to place a notice in a clearly visible spot in the area where CCTV surveillance is taking place. For details please see the Advisory Guidelines On The Personal Data Protection Act For Selected Topics (http://www.pdpc.gov.sg/docs/default-source/advisory-guidelines---selected-topics/selected-topics-guidelines-15-may-2014.pdf?sfvrsn=2).

8) Do we really need to review all our personal data at the beginning of every year to ensure that it is accurate?

You are free to determine when you want to review the personal data you collect, use, retain and disclose to ensure that it is up to date. It is suggested that you perform this review at the same time that you perform your general client due diligence / know your customer review.

9) Do we really need to review our personal data within two months of the end of each year to determine if personal data should be kept or destroyed?

Under the PDPA, an organisation has the duty to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that (a) the purpose for which that personal data was collected is no longer being served by retention of the personal data and (b) retention is no longer necessary for legal or business purposes (sec. 25 PDPA). In order to comply with this duty and ensure that the personal data is timely destroyed or anonymised, the PDP Policy proposes an annual review by the compliance officer within two months of the end of each financial year. This time limit for this annual review can be extended, but it must be reasonable. In general, it is suggested that you destroy all data that is older than five years unless you are required to maintain the data (e.g. for purposes of anti-money laundering and countering the financing of terrorism or because of legal disputes).

10) Do we need to employ a Personal Data Protection Officer

All organisations are required to designate at least one person (a "personal data protection officer") to be responsible for ensuring that the organisation complies with the PDPA (Q12 FAQs for Organisations). In

order limit the burden of this requirement, the PDP Policy suggests to appoint the person currently in charge of your compliance[1] as the person in charge of personal data protection.

11) What is the personal data inventory map?

The personal data inventory map is encouraged in the Personal Data Protection Checklist of the PDPC (https://www.pdpc.gov.sg/docs/default-source/publications-edu-materials/pdpc-checklist-for-orgs-v1-0.pdf?sfvrsn=0).

The personal data inventory map is a simple document to trace the flow of personal data in the organisation.

- What personal data is collected and why?
- Who collects it?
- Where is it stored?
- Who is it disclosed to?

The personal data inventory map thus provides you with an overview of the personal data you manage and provides indications regarding your obligations. It will in particular assist you in finding personal data for requests and destruction or anonymisation of personal data as required.

12) Is it necessary that we publish the Singapore Data Protection Notice on our website?

An organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available (para. 2.2(i) Introduction to the Guidelines). An organisation must at least make available to the public the business contact information of the personal data protection officer (sec. 11(5) PDPA). Upon request, the organisation must make information available (i) its data protection policies and practices and (ii) its complaint process (sec. 12(d) PDPA). According to informal discussions, organisations will generally provide at least the basics of their data protection policies on their websites.

[1] Every licensed fund management company ('LFMC') and registered fund management company ('RFMC') is required to appoint a compliance officer for anti-money laundering and countering the financing of terrorism purposes (para. 10.8 SFA04-N02), i.e. have a compliance officer. See also para. 3.1.5 and Appendix 2 SFA 04-G05.