Association of Process Industry (ASPRI) / ASPRI Dormitory Pte Ltd (ADPL)

PERSONAL DATA PROTECTION ACT POLICY

At ASPRI/ADPL, we strive to protect and safeguard the personal data which we have collected. Every employee *including all our Associate trainers, temporary staff and vendors* are required to sign a Declaration to Secrecy and an Undertaking to comply with the Personal Data Protection Act (PDPA).

This PDPA Policy describes the types of personal data we collect from our operations. The Policy also sets forth how we use, disclose, store and protect your personal data, and who to contact if you have any questions or concerns.

This PDPA Policy covers the following areas:

1. Consent Obligation
2. Purpose Limitation Obligation
3. Notification Obligation
4. Access and Correction Obligation
5. Accuracy Obligation
6. Protection and Disposal Obligation
7. Retention Limitation Obligation
8. Right to Withdraw Consent
9. Transfer Limitation Obligation
10. Accountability Obligation
11. Data Breach Obligation
12. Exceptions and Exclusion of Liability
13. Business Contact Information of Data Protection Officers (DPOs)

1) Consent Obligation

ASPRI/ADPL may collect, use or disclose personal data after consent is obtained from the individual. ASPRI/ADPL can collect your personal data through written (i.e. physical / e-form), verbal (i.e. voice recording) or deemed consent.

2) Purpose Limitation Obligation

ASPRI/ADPL may collect, use or disclose the individual personal data for the following reasons (collectively "Purposes"):

a) Evaluating application for membership.
b) Evaluating application for employment and payroll purposes.
c) Evaluating application for council election.
d) Providing services, to process billing/payment transactions.
e) Administering participation in any programme/event/activity organised by ASPRI/ADPL.
f) For financial processing purposes (i.e. banking related processing)
g) For the maintenance and upkeep of internal records, filing and operations or meeting any legal or regulatory requirements relating to our provision of services and to make disclosure under the requirements of any applicable law, regulation, direction, court order, by-law, guideline, circular, code applicable to us or our affiliates.
h) For entering into the any agreements and/or contracts.
i) For handling the report for lost item, customer complaints and taking appropriate action relating to it.
j) For security and crime prevention purposes, risks management, safeguarding ASPRI/ADPL in the event of any claims or litigation suits.
k) For any other reasonably related purposes or reasons.

ASPRI/ADPL may use your personal data without your consent in any of following circumstances:

a) The use is necessary for any purpose which is clearly in the interests of the individual, if consent for its use cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent.
b) The use is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual.
c) The personal data is publicly available.
d) The use is necessary in the national interest.
e) The use is necessary for any investigation or proceedings.
f) The use is necessary for evaluative purposes.
g) The personal data is used for the organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation.
h) The use is necessary for the provision of legal services by the organisation to another person or for the organisation to obtain legal services.

i) Subject to the conditions, the personal data is used for a research purpose, including historical or statistical research.
j) The data was collected by the organisation and is used by organisation for purposes consistent with the purpose of that collection.

3) Notification Obligation

ASPRI/ADPL will notify the individual of the purposes before collecting, using or disclosing the personal data.

4) Access and Correction Obligation

Individual personal data and how their personal data is used or disclosed should be provided upon a reasonable request. However, ASPRI/ADPL will prohibit in providing the individual access if the provision of the personal data or other information could reasonably be expected to:

- Cause immediate or grave harm to his safety or physical or mental health.
- Threaten another individual safety, physical and mental health.
- Reveal another individual personal data.
- Reveal the identity of another individual who has provided the personal data, and the individual has not consented to the disclosure of his identity; or
- Contradict or threat to national interest.

If you wish to make an access request to a copy of the personal data which ASPRI/ADPL hold about you or information about the ways in which ASPRI/ADPL use or disclose your personal data, or a correction request to correct or update any of your personal data which we hold, please fill up the ASPRI Access Request Form **here**.

Please note that a fee of S$5 will be charged for an access request.

Upon receiving your access request, ASPRI/ADPL will respond to your access request within 30 calendar days. If ASPRI/ADPL are unable to provide access within 30 calendar days, ASPRI/ADPL will inform you as soon as possible of the time ASPRI/ADPL will be able to provide access.

ASPRI/ADPL is not required to provide access to the documents which do not comprise or contain the personal data in question.

ASPRI/ADPL shall correct any error or omission in your personal data upon your request. If ASPRI/ADPL is satisfied upon reasonable grounds that a correction should not be made, ASPRI/ADPL is required to annotate the correction that was requested but not made. ASPRI/ADPL may provide the explanation why the correction should not be made.

5) Accuracy Obligation

ASPRI/ADPL will make reasonable effort to ensure that personal data collected and recorded by or on behalf of the organisation is accurate, complete and current.

6) Protection and Disposal Obligation

ASPRI/ADPL shall make reasonable security arrangements to protect the personal data that ASPRI/ADPL possesses or controls to prevent unauthorised access, collection, use, disclosure, copying, modifying, disposal or similar risks.

Security arrangements may take various forms such as (i) administrative measures, (ii) physical measures, (iii) technical measures or a combination of these. In practice, ASPRI/ADPL would:

a) Design its security arrangements to fit the nature of the personal data and the possible harm that might result from a security breach.
b) Identify reliable and well-trained personnel responsible for ensuring information security.
c) Implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity.
d) Be prepared and able to respond to information security breaches promptly and effectively.

ASPRI/ADPL would undertake the following measures to protect the personal data in various forms:

	Types of Data	
	Soft copy / Online / Cloud	**Physical medium**
Measure to be taken	Encrypt the files so that only authorised personnel have access	Lock physical files in cabinet and only authorised personnel have the keys
	Install appropriate computer security software	Implement an appropriate level of security when sending out mails (i.e. opt for registered mail)

ASPRI/ADPL would undertake the following measures to dispose the personal data in various forms:

	Types of Data	
	Soft copy / Online / Cloud	**Physical medium**
Measure to be taken	Erase files / contents, including emptying the recycle bin	Erase contents from re-writable disc, USB, hard disk, memory stick
		Degauss hardwares where data could be stored

		Incinerate, shred and pulp hard copies and ensure data are not retrievable

7) Retention Limitation Obligation

ASPRI/ADPL must cease retention of personal data after 4 years when the purpose of retention is no longer necessary for any business or legal purposes associated with the individuals as soon as it is reasonable to assume that:

a) Purpose for which the personal data was collected is no longer being served by retention of the personal data.
b) Retention is no longer necessary for legal or business purposes.

Retention period may depend on the following:

a) The purpose(s) for which personal data was collected
   i) If one or more of the purposes for which it was collected remains valid.
   ii) Personal data should not be kept for "just in case".

b) Other legal or business purposes e.g. legal action, required under other applicable laws or regulations, needed for generating annual reports, or performance forecasts.

ASPRI/ADPL ceases to retain personal data when documents are:

a) Destroyed
b) Disposed of in an appropriate manner
c) Returned to the individual concerned
d) Transferred to another person on the instructions of the individual concerned; or
e) Anonymisation is the process of removing identifying information, such that the remaining data does not identify a specific individual

8) Right to Withdraw Consent

You may at any time withdraw your consent to ASPRI/ADPL. ASPRI/ADPL shall take all necessary measures to give effect to your withdrawal of consent, to the extent that such withdrawal does not conflict with any of our legal obligations. To withdraw, please fill up the ASPRI Withdrawal of Consent Form **here**.

Upon receipt of a notice of withdrawal of consent, ASPRI/ADPL must cease to collect, use or disclose the individual's personal data, and inform its data intermediaries and agents about the withdrawal and ensure that they cease collecting, using or disclosing the personal data for the various purposes.

Having received and verified your identification and documentation, ASPRI/ADPL shall endeavour to respond to your request within 10 business days.

However, by withdrawing your consent, ASPRI/ADPL might not be able to render adequate service to you or you might be disqualified for certain services/participation. Please note that there may be legal consequences which may arise from the withdrawal of your consent to the collection, use or disclosure of your personal data. ASPRI/ADPL shall inform you of any such consequences depending on the nature of the withdrawal of consent you are requesting.

9) Transfer Limitation Obligation

Should ASPRI/ADPL transfer personal data out of Singapore, ASPRI/ADPL must take steps to ensure compliance with the DP provisions. When transferring to a recipient or its subsidiaries out of Singapore, ASPRI/ADPL must ascertain and ensure that the recipient or its subsidiaries is bound by legally enforceable obligations that provide a standard protection that is at least comparable to the PDPA.

10) Accountability Obligation

ASPRI/ADPL shall be responsible for the personal data collected or obtained for processing or which ASPRI/ADPL has control over. ASPRI/ADPL will undertake the following measures to ensure obligations under the PDPA are met:

- Designate Data Protection Officers (DPO)
- Make available the Business Contact Information (BCI) of the DPOs
- Develop and implement relevant data protection policies and practices
- Develop a process to receive and respond complaints that may arise with respect to the application of the PDPA
- Make information available on request concerning ASPRI/ADPL's data protection policies and practices and complain process
- Communicate to ASPRI/ADPL's staff information on relevant policies and practices

11) Data Breach Obligation

If there is a data breach discovered by ASPRI/ADPL, the following measures will be taken:

1. Contain the data breach to prevent further compromise of data and implement mitigating action(s) to minimise potential harms from the breach after an initial appraisal has been conducted to determine the extent of the breach.

2. Assess the data breach to determine the root cause (where possible) and the effectiveness of containment action(s) taken thus far to contain the data breach. Where necessary, continuing efforts should be made to prevent further harm from the data breach.

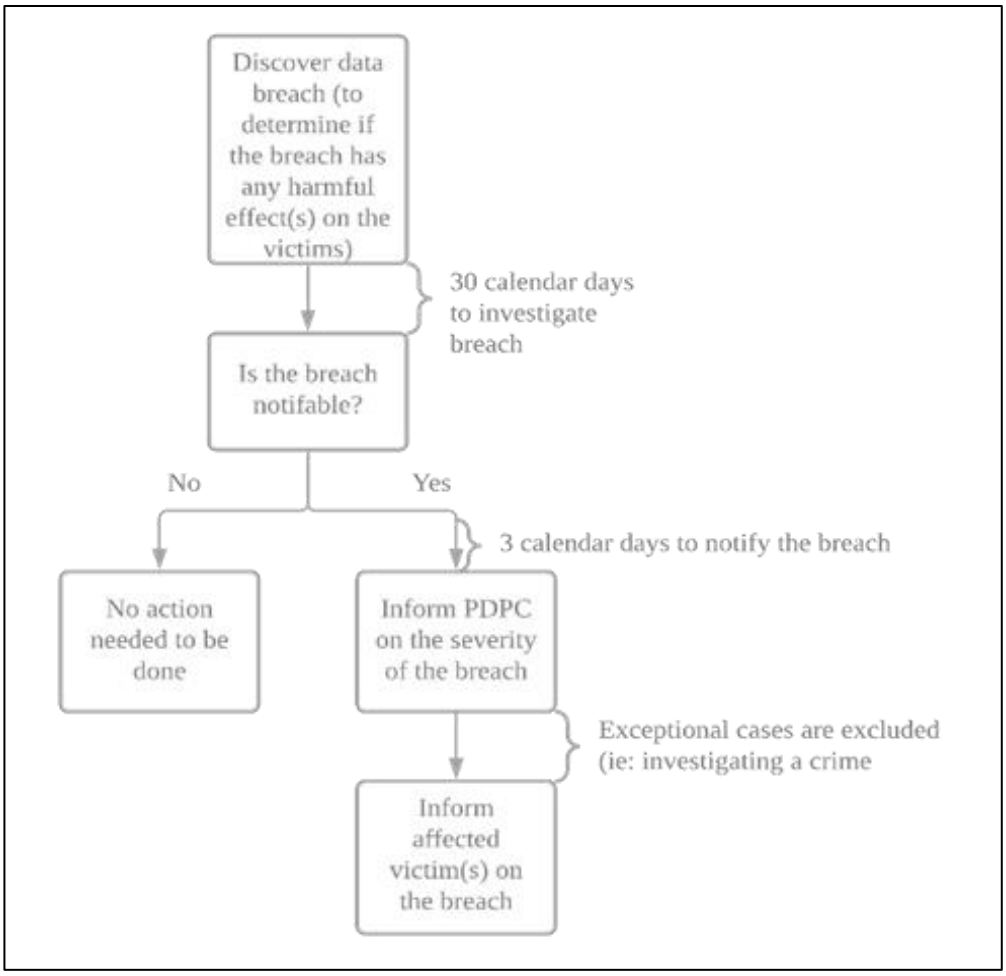
3. Report the data breach to:
    - The PDPC (mandatory if the breach is a notifiable data breach under the Personal Data Protection Act ("PDPA") no later than 3 calendar days.

Organisations may also inform PDPC of the data breach voluntarily); and/or

- The affected individuals (if required under the Data Breach Notification Obligation ("DBN Obligation")) as soon as practicable, at the same time or after notifying the PDPC.

4. Evaluate the organisation's response to the data breach and consider the actions that can be taken to prevent future data breaches. Where necessary, continuing efforts should be made to prevent further harm from the data breach.

Below is a timeline that ASPRI/ADPL will follow when there is a case of data breach:



12) Exceptions and Exclusion of Liability

ASPRI/ADPL reserves the right to refuse to process any request for withdrawal of consent, access or correction in the following circumstances:

- Where there is an insufficiency of information provided by any party making a request to enable ASPRI/ADPL to locate or identify the Personal Data in question.

- Where there is reasonable doubt surrounding the identity of the person making the request or where ASPRI/ADPL feels that the requesting party is not in fact the owner or the subject of the Personal Data in question and is not lawfully entitled to make any requests in relation to the Personal Data.

- Where permitting access or correction would be tantamount to a violation of an order of Court.

- In requests for access or for correction (excluding instances of withdrawal of consent):

    i. where the burden or expense of processing the request for access or correction is disproportionate to the privacy of the party making a request;
    ii. where compliance with the request would involve the unauthorised disclosure of Personal Data belonging to a third party;
    iii. where compliance would result in the disclosure of confidential commercial information; or
    iv. where access is regulated by another law

ASPRI/ADPL will not be liable for any purported violation, breach or non-compliance with any precepts of privacy or the protection of Personal Data in the following instances:

- Where an act of nature or event happened outside the control of ASPRI/ADPL resulted in the damage or malfunction or destruction in any equipment or technologies used to secure, store or process Personal Data;

- Where Personal Data is readily available or able to be found in the public domain; and

- Where despite ASPRI/ADPL best efforts, there is an unauthorised access, modification, alteration, misuse, tampering and abuse of Personal Data caused by the malicious, fraudulent, criminal acts and conduct of a third party not being under the control or direction of ASPRI/ADPL.

13) Business Contact Information of Data Protection Officers (DPOs)

<u>Chief DPO</u>
Name: Ms Chantal Quek
Contact Number: 6560 5051
Email Address: chantal@aspri.com.sg
Address: 9 Jurong Town Hall Road #04-11 Trade Association Hub S609431

<u>Assistant DPO (ASPRI Secretariat)</u>
Name: Mr Wong Jun Yuan
Contact Number: 6560 5051
Email Address: junyuan@aspri.com.sg
Address: 9 Jurong Town Hall Road #04-11 Trade Association Hub S609431

Assistant DPO (ADPL, Finance, HR)
Name: Mr Lung Sze Wynn
Contact Number: 6560 5051
Email Address: szewynn@aspri.com.sg
Address: 9 Jurong Town Hall Road #04-11 Trade Association Hub S609431

Assistant DPO (ASPRI-IPI)
Name: Ms Caphine Lee
Contact Number: 6795 5700
Email Address: caphine@ipi.org.sg
Address: 5 Jalan Papan Singapore 619421