SUNWAY®

SUNWAY GROUP OF COMPANIES
PERSONAL DATA DISCLOSURE POLICY

TABLE OF CONTENTS

Contents **Page**

1. Introduction

1.1 The employees of the Sunway Group of Companies ("**Sunway**") are required to refer to this policy when disclosing personal data of customers/tenants/vendors or any other individuals internally or to third parties, to ensure compliance with the Malaysian Personal Data Protection Act 2010 ("**PDPA**").

2. Personal Data & Sensitive Personal Data

2.1 Personal data means any information of individuals, for example name, IC/passport number, date of birth, contact details and bank details.

2.2 Under the PDPA, Sunway is required to exercise extra caution when disclosing sensitive personal data. Sensitive personal data means any information relating to physical or mental health or condition of an individual, his political opinions, his religious beliefs or other beliefs of a similar nature, commission of crime (alleged or otherwise).

2.3 The access to sensitive personal data within Sunway should be strictly limited to the relevant employees and access should be reviewed periodically; and

2.3 There should be no transfer or disclosure of sensitive personal data to third parties save where explicit consent is obtained.

3. Disclosure within Sunway

3.1 Any disclosure within Sunway should be on a "need to know" basis according to the job scope of the employees and functions of the units/departments.

3.2 The purposes of disclosure need to be taken into account and only information necessary to achieve the objectives should be shared with the relevant employees. Personal data should not be shared where the purposes of disclosure can be achieved without sharing the data or anonymising it.

Example 1:

The payroll division has access to the name and basic details of the employees including his bank details to process his salary. However, the payroll division should not have access to other unnecessary information such as the employees' health condition or their academic records.

4. Disclosure to Third Parties

The employees of Sunway should not disclose the personal data of any individual to any third party save where steps 1 to 4 stated in paragraphs 4.2 to 4.5 below are followed OR where there is an exceptional situation (refer to Section 5 below).

(a) Step 1 Authorisation

You should only disclose the personal data if you have the appropriate authorisation, where any of the followings applies:

(i) The individual has given consent for such disclosure. The consent needs to be in writing and submitted to the relevant department for records. Consent sent via email can be an acceptable form where it is sent from the individual's official email address (Sunway employees' email address) or an email address previously notified to Sunway; or
(ii) The purpose of disclosure is the purpose the personal data was to be disclosed at the time of its collection or directly related to that purpose and the third party falls within one of the classes of third parties stated in the written notice issued pursuant to section 7 of the PDPA; or
(iii) The individual is under the age of 18 and disclosure is made to his parents/guardians.

(b) Step 2 Information to be shared

You should only disclose information which is necessary to achieve the purposes of disclosure and does not exceed the scope of authorisation.

(c) Step 3 Mode of disclosure

(i) Correspondences in writing

The request by the third party and disclosure by Sunway should be **in writing** only. The authorisation to disclose (for example, consent is obtained/the purpose of disclosure) should be clearly stated in the cover email/letter to third parties.

(ii) Recipient

The personal data should only be disclosed to the right person. You should ensure that:

- the personal data is sent to the address/email address as provided in the individual's consent letter; and
- for disclosure to other organisations/companies, the personal data is sent to authorised personnel in the recipient company/organisation.

(iii) Secured transmission

You should ensure that the personal data is transmitted to the third party securely:

- Certified true copy of print/hard copy/photocopy of original document to be sent by courier/hand or to be made available for collection and in a sealed envelope (stamped confidential). Recipient confirmation is required; and
- Electronic file to be sent in a way to prevent interception/modification (e.g. PDF) with the subject title marked confidential. Electronic file to be password protected where possible. Acknowledgement of receipt is required.

(d) Step 4 Records

You should record the disclosure of personal data, including the following information:

(i) the type of personal data shared;
(ii) the authorisation/purpose of disclosure;
(iii) the recipient of the personal data; and
(iv) the date of disclosure.

Table 1 below provides guidance on type of authorisation required and information to be shared for third parties which SUNWAY may deal with regularly. Step 3 and 4 need to be strictly followed for all types of disclosure.

Please consult your Business Unit PDPA Officer if:

- the third party you are dealing with is not stated in the table below;
- the type of information required is excessive/ beyond the scope of authorisation/not for the purpose of disclosure; and/or
- you have any doubt on this step 1 to 4 stated above.

Table 1

No	Third party	Authorisation	Information to be shared
1.	Family members, parents, guardians (of any individual who is 18 or above)	The individual has given written consent for disclosure.	Depending on the scope of authorisation as stated in the consent letter.

No	Third party	Authorisation	Information to be shared
2.	Parents/guardians (of any individual who is under the age of 18)	No authorisation is required, request can be made via Data Access Request Form and Policy via the Group Human Resources Portal.	In accordance with the Data Access Request Policy.
3.	Banks	The individual has given written consent for disclosure.	Depending on the scope of authorisation as stated in the consent letter.
4.	Disclosure to media for marketing and other purposes	The individual has given written consent for disclosure.	Depending on the scope of authorisation as stated in the consent letter.
5.	Malaysian immigration department and other Embassies (or private companies representing Malaysian immigration department or embassies)	The individual has given written consent for disclosure.	Depending on the scope of authorisation as stated in the consent letter.
6.	Potential employers (release of health screening results)	The individual has given written consent for disclosure.	Strictly in accordance with the scope of authorisation as stated in the consent letter.
7.	External counterparts/institutions • Third party private hospitals or government hospitals where patients are transferred	The individual has given written consent for disclosure.	Strictly in accordance with the scope of authorisation as stated in the consent letter.

No	Third party	Authorisation	Information to be shared
8.	Accreditation bodies (Malaysian Society for Quality in Health)	Purpose of the disclosure is only to assist the hospital in acquiring accreditation.	Not excessive and only to the extent required to achieve the purpose of disclosure e.g. making available information only as is necessary for MSQH audit.
9.	Regulatory authority • Ministry of Health • Law enforcement agencies such as police • EPF • SOCSO • Income tax • Any other statutory bodies	Sunway is required by law or by the court order to disclose personal data	Not excessive and only to the extent required by law or by the court order e.g. infection control and HIV reporting obligations .
10.	Third party service providers* • Auditors • Company secretary • Mailing companies • Printing companies • Insurers • Telecommunications companies • Event Organisers	Purpose of disclosure is for the third party service providers to carry out the services.	Not excessive and only to the extent required to achieve the purpose of disclosure e.g. only customer email address provided to email blast service provider, only required financial information made available to auditors, etc.

No	Third party	Authorisation	Information to be shared
	• Travel agencies • Suppliers • Recruitment agents • Consultants *To ensure that third party service providers have given warranty and indemnity to SUNWAY to comply with the PDPA prior to the disclosure.		
11	Statutory bodies / business partners	Purpose of disclosure is for current / potential business partnering, licensing, tendering and/or relevant contractual obligation	Not excessive and only to the extent required to achieve the purpose of disclosure e.g. application/renewal of PKK license

5. Exceptional Circumstances

In the event of emergency, the staff of Sunway may disclose the personal data without complying with Section 3 & 4 above, provided ALWAYS that such disclosure has obtained the approval of the your Business Unit PDPA Officer or where the approval of the Business Unit PDPA Officer cannot be reasonably obtained, the approval of the Head of Department.

(a) Disclosure under emergency circumstances includes:
   (i) Disclosure necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations;
   (ii) Disclosure necessary where there is a serious and imminent risk to the welfare of the individual; and
   (iii) Disclosure required or authorised by or under any law or by the order of court.

6. Further Information

Please contact Group Human Resources Personal Data Protection (PDP) Officer on Level 14 for further information.

TABLE OF CONTENTS

Contents **Page**

1. Introduction

1.1 Sunway Group of Companies ("**Sunway**") processes and retains certain personal data in the course of its commercial transactions, including personal data of its students, customers, donors and employees.

1.2 This document intends to provide guidance to the staff of Sunway in relation to the retention and destruction of personal data.

2. Personal Data Retention and Destruction

2.1 Under the Personal Data Protection Act 2010, the personal data processed for any purpose should not be kept longer than is necessary for the fulfilment of that purpose. Sunway should therefore take all reasonable steps to ensure that all personal data processed by Sunway is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

2.2 Sunway reconciles the obligation stated in paragraph 2.1 with other statutory obligations or industry practices for the purposes of ensuring consistency throughout SUNWAY's retention procedure. For example:

the personal data may no longer be needed for a particular purpose but it may still be retained to fulfil obligations under the Income Tax Act 1967 or Employment Act 1955;

an action founded on contract expires after six (6) years from the date on which the cause of action accrued under the Limitation Act 1953 ("**Limitation Act**"). It is advisable for the personal data processed pursuant to contracts / agreements (between Sunway and employees / customers / suppliers / vendors / tenants) to be retained for a minimum period of 6 years as the information may be used as evidence in the event of civil action.

3. Personal Data Retention

3.1 The personal data retention schedule attached as Schedule 1 ("**Retention Schedule**") serves as guidance for Sunway staff in relation to the minimum retention period for different types of personal data.

3.2 The Personal Data Protection Officer should exercise his / her discretion to change the retention period where appropriate. For example, where there is an on-going / pending litigation / investigation or where there is a reasonable justification (as required by laws or external institutions).

3.3 The retention period is the number of years that a record should be retained in the relevant department / unit prior to destruction or deletion. Sunway may be required to keep certain personal data (such as basic records of previous employees) permanently for future references

4. Personal Data Destruction

4.1 The disposal of personal data in all format (including written documentation, electronic personal data, photographic data and any other medium used to store the personal data) should be carried out in a safe and secured manner after the minimum retention period, as follows:

Media	Disposal methods
Papers / Files	Shred
Laptop / USB / Computer / Shared Drive and other electronic platform	Delete and ensure that all the personal data is removed permanently using appropriate software.
CDs/tapes	Crush or cutting into pieces.

5 Further Information

5.1 Please contact Group Human Resources Personal Data Protection (PDP) Officer on Level 14 for further information.

Schedule 1: Personal Data Retention Schedule

	Type of Personal Data	Example	Retention Period	Reason
Customers				
1.	Marketing	• Survey forms • Enquiry forms • Marketing database	Retain for the period when the customers' are actively contacted for marketing purposes.	For marketing correspondences. The customers' personal data should be removed from marketing database immediately if requested by the customers or no longer used by Sunway for this purpose.
2.	Providing services	• Registration forms • Application forms	Retain for 7 years after the provision of services ceases.	Limitation Act, potential litigation.
3.	Finance	• Customer bills • Invoices	Retain for at least 7 years after the provision of services ceases or from the end of the year of tax assessment (whichever is longer).	Limitation Act, potential litigation. Tax & Audit purposes.
4.	Security	• Access, visitors information, sign in book • CCTV • Incident reports	Retain for 7 years after the date of records.	Limitation Act, potential litigation.
Suppliers, vendors, tenants				
1.	Suppliers Vendors Tenants	• Agreements/ contracts • Relevant database	Retain for 7 years after the expiration/ termination of contract.	Limitation Act, potential litigation
2.	Finance	• Invoices • Purchase orders	Retain for at least 7 years after the expiration/ termination of contract or from the end of the year of tax	Limitation Act, potential litigation. Tax & Audit purposes

	Type of Personal Data	Example	Retention Period	Reason
			assessment (whichever is longer).	
Human Resources				
1.	Recruitment	• Application for employment • References • Supporting documents and qualifications • Offer letter / rejection letter	Retain for 1 year for unsuccessful applicants. Retain for 7 years after termination of employment for successful applicants.	Limitation Act, potential litigation.
2.	Administration during the term of employment	• Employees' personal data and family members' personal data • Leave authorisation form • Staff performance ratings • Salary • Employee benefits • Training and development	Retain for 7 years after termination of employment.	Limitation Act, potential litigation.
3.	Misconduct	Complaints against an employee, investigations, hearing process, correspondences, interviews.	Retain for 7 years after termination of employment or such longer period as required.	Limitation Act, potential litigation.
4.	Records after the term of employment	Core files containing a summary of staff's basic information, position, salary, duration of employment	Retain permanently.	To provide references to the employees.
5	Payroll document	• EA forms • Contribution forms • Salary master	Retain for at least 7 years after the termination of employment or from the end of the year of tax assessment (whichever is longer).	Limitation Act, potential litigation. Tax & Audit purposes

History Log (Last Page)

Date	Details of Reviews	PIC