HL MANAGEMENT CO SDN BHD

PERSONAL DATA PROTECTION POLICY

1. INTRODUCTION

1.1 The Personal Data Protection Act 2010 (**"PDPA"**) is a legislation with ramifications for any company that processes personal data. The PDPA affects how personal data of customers, employees and any other individual is processed.

1.2 The purpose of the PDPA is to protect personal data. It aims to regulate the activities of all Data Controllers who process personal data, including the collecting, recording, holding, storing, use, disposal or disclosure of personal data.

2. SCOPE

2.1 Besides HL Management Co Sdn Bhd ("**HLMC**"), this Personal Data Protection Policy ("**PDP Policy**") shall also be adopted by:

(i) Hong Leong Share Registration Services Sdn Bhd ("**HLSRS**"); and
(ii) Hong Leong Healthcare Group Sdn Bhd ("**HLHG**").

(each of HLMC, HLSRS and HLHG shall respectively be referred to as the "**Company**", collectively the "**Group**")

2.2 This PDP Policy applies to all employees of the Company and any person performing work or services for and on behalf of the Company such as contract staff, interns, vendors, contractors, agents or representatives.

2.3 The categories of personal data processed by the Group are primarily the following:

(i) Employees' personal data (existing, leavers and prospective);
(ii) Directors' personal data;
(iii) Customers or clients' personal data (for customer-facing companies); and
(iv) Scholarship applicants' and recipients' personal data.

3. POLICY STATEMENT

3.1 This PDP Policy sets out the Company's approach to ensure compliance with the PDPA Laws, and in particular, the 7 data protection principles described below.

4. DATA PROTECTION PRINCIPLES ("DPPs")

4.1 Each Company shall comply with the 7 DPPs set out in the PDPA for processing of all personal data as summarised below: -

DPP1 General Principle
Personal data can only be processed with the consent of the Data Subject, save where PDPA Laws provide otherwise. Further, the personal data collected should not be excessive in relation to the stated purposes.

DPP2 Notice and Choice Principle
This provides that written notice ("**Privacy Notice**") must be provided to Data Subjects about the Data Controller's policies and practices in relation to processing of personal data, the kinds of personal data they hold and the purposes for which personal data are used, and the Data Subject shall be provided with the means to exercise his choice on matters comprised in the Privacy Notice.

DPP3 Disclosure Principle
This provides that unless the Data Subject gives consent (including pursuant to a Privacy Notice), or where consent is not required by PDPA Laws, or where the disclosure is required for compliance with law, or for the purpose of preventing or detecting a crime, or for the purpose of investigations, personal data should only be disclosed (1) for the purpose (a) for which the personal data was to be disclosed at the time of collection of the personal data, or (b) for a purpose directly related to the purpose referred to in (a), or (2) to a third party or a class or category of third parties mentioned in the Privacy Notice for the purpose referred to in (1).

DPP4 Security Principle
This requires appropriate security measures to be applied to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

DPP5 Retention Principle
This provides that personal data shall not be kept longer than necessary.

DPP6 Data Integrity Principle
This provides that reasonable steps should be taken to ensure that the personal data is accurate, complete, not misleading and kept up-to-date.

DPP7 Access Principle
This provides for Data Subjects to have rights of access to and correction of their personal data.

5. PRINCIPLES

5.1 Appointment of Data Protection Officer ("DPO")

A data protection officer shall be appointed in a Company where the processing of personal data involves:

(i) personal data exceeding 20,000 Data Subjects;
(ii) sensitive personal data including financial information data exceeding 10,000 Data Subjects; or
(iii) involves activities that require regular and systematic monitoring of personal data.

More than one DPO may be appointed from different divisions or functions in a Company, as required, depending on the Company's operations, structure and size. A DPO may have duties and responsibilities under another function provided that it does not conflict with his/her task and function as a DPO.

The appointed DPO shall have sufficient training, skills and competency to carry out its duties as a DPO and must be proficient in both English and Malay language.

Appointment of a DPO and the DPO's business contact information must be promptly notified to the Commissioner no later than twenty-one (21) days from the date of appointment. Any change to the DPO or business contact information of the DPO must be notified to the Commissioner no later than fourteen (14) days from the effective date of the new appointment.

The appointed DPO must have a separate and dedicated official business email account ("**Designated Email Account**") for all communication with the Commissioner and Data Subjects. Additionally, the DPO's business contact information must be made publicly available on the Company's website, personal data protection notices or security policies and guidelines.

On cessation or termination of the appointment of the DPO (where he/she is the sole DPO of the Company):

(a) a new DPO must be appointed within one (1) month from the cessation/termination of the previous DPO; and
(b) an interim DPO must be appointed to monitor communications from the Designated Email Account (hlmc-dpo@hongleong.com) until the new DPO is appointed.

5.2 PDP Committee for HLMC ("Committee")

A Committee shall be established to support the DPO in implementing data protection measures and overseeing all data privacy matters.

The Committee shall comprise the DPO and representatives from key departments, including:
(a) Legal department;
(b) Human Resources department; and
(c) IT department.

5.3 Appointment of Department PDP Representative

A Department PDP Representative shall be appointed for each department in a Company. More than one Department PDP Representative may be appointed in a department for different functional or operational sections in a department.

The Responsible Party shall appoint the Department PDP Representative for their respective department.

5.4 **Responsibilities**

(a) **Data Protection Officer**

Key responsibilities of DPO, with the assistance and support of the Committee, the Responsible Party and Department PDP Representatives, are as follows: -

(i) Inform and advice the Company and Senior Management on matters related to processing of personal data in the Company, including any risks that may arise or have arisen with regards to the same;

(ii) Support the Company in complying with the PDPA law including staying informed of data processing risks affecting the Company;

(iii) Support the carrying out of data protection impact assessments (where applicable);

(iv) Monitor the personal data compliance of the Company;

(v) Ensure proper personal data breach and security incident management by facilitating investigation of personal data breach incidents and assisting the Company to prepare, process and submit reports and other documents required by the Commissioner in respect of personal data breaches;

(vi) Act as the facilitator and point of contact between Data Subjects and the Company regarding the processing of the Data Subject's personal data and their rights;

(vii) Act as the liaison officer and the main point of reference between the Company and the Commissioner;

(viii) Alert Senior Management of any personal data breach in the incidents that he/she is aware of;

(ix) Involvement in all matter concerning personal data protection starting from the earliest stage of data processing lifecycle i.e. from policy formulation to collection, storage and deletion or destruction of personal data; and

(x) Provide PDPA related training/seminars to Department PDP Representatives and the employees of the Company.

(b) **Responsible Party**

Key responsibilities of the Responsible Party are as follows:

(i) Draw up the required standard operating procedures (where required) to ensure full and correct implementation of the requirements under PDPA Laws and this PDP Policy in respect of processing of personal data within their department; and

(ii) Alert the DPO of any personal data breaches or to any risks that might arise or have arisen with regard to personal data processing in their department.

(c) **Department PDP Representative**

The Department PDP Representative serves as the first line of defence for PDPA compliance and matters within their department. The primary responsibility of each Department PDP Representative is to raise awareness of PDPA requirements to promote compliance of PDPA Laws and this PDP Policy within their department. Key responsibilities of Department PDP Representative are as follows:

(i) Department PDP Representatives should have a good understanding of the requirements of the PDPA (including the 7 DPPs), the related Codes of Practice and Guidelines, and this PDP Policy;

(ii) Support and provide advice on PDPA matters referred by personnel in the department;

(iii) Consult the DPO or where there is no DPO, the Legal department on queries / complaints in relation to compliance with PDPA Laws;

(iv) Update the relevant Responsible Party on any matters affecting the processing of personal data in their department.

6. PROCESSES FOR PROCESSING OF PERSONAL DATA

The processing of personal data shall comply with the following:

6.1 Monitor Data Collection

(a) Before a Data Subject is first asked to provide personal data or before any personal data is first collected (whichever is the earlier), all Data Subjects must be given the Company's Privacy Notice or given the opportunity to obtain a copy of, view or access the Privacy Notice.

(b) Ensure that Data Subject's consent is obtained prior to collection of personal data, and is recorded and maintained by the Data Controller.

(c) All personal data collection processes must comply with PDPA Laws.

(d) Common personal data collection points will include:

- Data Subject/prospective Data Subject application forms and correspondence from Data Subjects. Obtaining ID card numbers and ID card copies;
- telephone conversations;
- third party sources (e.g. from a credit reference agency or a third party providing personal or credit references) or a mailing list supplier;
- employment applications;
- via electronic means (e.g. emails, websites, social media platforms, service applications, whatsapp);
- new hires forms; and
- Company's online site(s) or application(s) which collect personal data.

(e) Data collected must be limited to what is required or relevant for the intended purpose and Data Controller must justify the collection of each category of personal data.

6.2 **Monitor Use of Data**

(a) The purposes for which the personal data is used must be identified, e.g. (non-exhaustive list):

(i) internal marketing activities;
(ii) credit risk or other analysis, referral to credit reference agencies;
(iii) transfer or referral outside the Company, including:
- to other companies within the Hong Leong Group (e.g. for cross-marketing purposes or employment referrals); and
- to third-parties, such as regulators and service providers;

(iv) provision of services;
(v) employment purposes and employee background checks; and
(vi) customer/vendor/supplier due diligence.

(b) Data Controller must consider if these purposes are reasonable in the circumstances and covered by the Privacy Notice. Department PDP Representatives shall consult the DPO if the intended purposes are not covered by the Privacy Notice or if in any doubt.

(c) Unless the Data Subject gives consent (including pursuant to a Privacy Notice), or where consent is exempted by law, or the disclosure is required for compliance with law, or for the purpose of preventing or detecting a crime, or for the purpose of investigations, personal data should only be disclosed:

(1) for the purpose (a) for which the personal data was to be disclosed at the time of collection of the personal data, or (b) for a purpose directly related to the purpose referred to in (a), or
(2) to a third party or a class or category of third parties identified in the Privacy Notice for the purpose referred to in (1).

(d) Sensitive Personal Data must be processed in accordance with the requirements of PDPA Laws.

6.3 **Monitor Cross Border Personal Data Transfers**

(a) Transfers of any personal data to a place outside Malaysia must be done in compliance with the requirements of PDPA Laws.

(b) Personal data may be transferred outside Malaysia if the Data Subject has provided express consent, or if the transfer satisfies any of the conditions or exceptions permitted under the PDPA Laws.

6.4 **Monitor Security/Ensure confidentiality**

(a) Personal data is confidential. All employees must understand the need to safeguard the confidentiality of personal data at <u>all</u> times. Personal data must be protected against any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or

destruction or other unauthorised use. Systems to protect confidentiality must be developed and maintained including procedures for secure storage and disposal of personal data and records.

(b) The IT department plays a crucial role in maintaining the technical measures and infrastructure necessary to ensure security of personal data. All employees shall comply with all relevant IT standard operating procedures, including any email guidelines, security warnings, access protocols, and incident reporting procedures.

6.5 **Retention period for personal data**

A retention schedule for personal data held by a department must be drawn up, taking into account the following:

(a) The PDPA prohibits retention "longer than is necessary for the fulfillment of that purpose".

(b) The retention period of documents shall take into account the retention period specified in any law/regulations or recommended by the Legal Department. In the event of inconsistency, the retention period reflected in the law/regulations shall prevail.

Reasonable steps are to be taken to ensure the destruction or permanent deletion of personal data (including any paper and digital data), including mode of destruction and at appropriate times pursuant to the retention schedule, which must be set out in relevant standard operating procedures.

6.6 **Monitor Data Integrity, Access and Correction Requests**

(a) Reasonable steps must be taken to ensure that the personal data is accurate, complete, not misleading and kept up-to-date.

(b) Data Subject shall be provided with the means to exercise his choice on matters comprised in the Privacy Notice.

(c) Requests by Data Subjects for access to their personal data or correction of inaccurate, incomplete, misleading or outdated personal data must be monitored, complied with or corrected within applicable timelines set out under PDPA Laws.

6.7 **Data Processor**

Where processing of personal data is carried out by a Data Processor on behalf of a Company, the Company shall require the Data Processor (through legally binding documentation) to:

(a) Take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction;

(b) Provide sufficient guarantees in respect of the technical and organisational security measures in place prior to any personal data processing being carried out;

(c) Take reasonable steps to ensure compliance with the measures specified in sub-paragraph (b) above;

(d) To have an appointed DPO throughout the period it is processing personal data of the Company; and

(e) Notify the Company of any personal data breaches in relation to the personal data of the Company and provide all reasonable and necessary assistance, cooperation and information to enable the Company to fulfill the Company's data breach notification obligation under the PDPA.

6.8 **Other implementation considerations**

(a) The proper handling of, and escalation procedures for, queries and complaints regarding personal data use and policy must be established and maintained.

(b) Companies shall comply with the registration and display of registration/ licence requirement including renewal of the registration under the PDPA Act 2010 (if required).

7. PRIVACY NOTICE

7.1 At the initial point of collection of personal data, the Company shall by a Privacy Notice inform a Data Subject:

(a) that personal data of the Data Subject is being processed by or on behalf of the Company, and provide the Data Subject with a description of the personal data being processed by the Company, including Sensitive Personal Data;

(b) the purposes for which the personal data is being or is to be collected and processed;

(c) of any information available to the Company as to the source from where the personal data is collected;

(d) of the Data Subject's right to request access to and to request correction of the personal data, how to do so and how to contact the Company with any inquiries or complaints in respect of the personal data;

(e) of the class of third parties to whom the Company discloses or may disclose the personal data;

(f) of the choices and means the Company offers the Data Subject for limiting the processing of their personal data, including personal data relating to other persons who may be identified from that personal data; and

(g) whether it is compulsory or voluntary for the Data Subject to supply the personal data and if compulsory, to specify the consequences of failing to provide such personal data.

7.2 The Privacy Notice shall be drawn up and maintained by the Data Controller. It shall be in Bahasa Malaysia and English. The Data Controller shall review the Privacy Notice periodically to reflect changes or updates in business, operational, legal or regulatory requirements, and shall keep a record of the effective date of each updated Privacy Notice. Privacy Notices must be approved by the DPO prior to its publication or issuance.

8. DATA BREACH NOTIFICATION

8.1 The Company shall vide the DPO[1] notify the Commissioner of a Data Breach as soon as practicable but no later than 72 hours after the occurrence of the Data Breach. The DPO[1] shall be the main point of contact with regards to all correspondences with the Commissioner in relation to the Data Breach.

8.2 The notification to the Commissioner shall be made by completing the data breach notification form prescribed in the GDBN or applicable PDPA Laws.

8.3 The Company shall notify the Data Breach to the affected Data Subject no later than seven (7) days after the initial Data Breach notification is made to the Commissioner.

8.4 A Personal Data Breach Notification Standard Operating Procedures shall be established and maintained by the Company to ensure a coordinated and effective approach to managing Data Breaches.

9. RECORD KEEPING

9.1 The Company shall keep a record of all documentation and records of data processing activities and in relation to the requirements of this PDP Policy (including related policies and standard operating procedures), for a minimum period of seven (7) years calculated from the date of document, date of cessation of use of personal data which is related to such document or date of closure of accounts, whichever is later. This includes Privacy Notice, records of consent, records of request to access or correction of personal data by Data Subject and training records.

9.2 The Company shall keep records and maintain a register detailing personal data breaches for a minimum period of seven (7) years from the date of notification to the Commissioner, which records shall be made available to the Commissioner upon request.

10. DEFINITIONS

Biometric Data	any personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a person
Commissioner	the Personal Data Protection Commissioner appointed under the PDPA
Company	each of HLMC, HLHG and HLSRS as applicable
Data Breach	breach of personal data, loss of personal data, misuse of personal data or unauthorised access of personal data that causes or is likely to cause Significant Harm or is of Significant Scale

[1] Manager designated by Senior Management, where no DPO is appointed.

Data Controller	any person who, either alone or jointly or in common with other persons, processes personal data or has control over or authorises the processing of personal data, but excluding a Data Processor. The Company is a Data Controller
Data Processor	any person, other than an employee of the Data Controller, who processes the personal data solely on behalf of the Data Controller, and does not process the personal data for any of his own purposes, for example, payroll companies and cloud providers
Data Protection Officer / DPO	such person appointed pursuant to paragraph 5.1
Data Subject	the individual who is the subject of the personal data
Department PDP Representative	has the meaning set out in paragraph 5.3
Designated Email Account	hlmc-dpo@hongleong.com
DPP	Data Protection Principles
GCBPDT	Guidelines on Cross Border Personal Data Transfer issued on 29 April 2025
GDBN	Guidelines on Data Breach Notification issued on 25 February 2025
GDPO	Guidelines on Appointment of Data Protection Officer issued on 25 February 2025
Group	HLMC, HLHG and HLSRS
HLHG	Hong Leong Healthcare Group Sdn Bhd
HLMC	HL Management Co Sdn Bhd
HLSRS	Hong Leong Share Registration Services Sdn Bhd
Hong Leong Group	Hong Leong Company (Malaysia) Berhad, GuoLine Capital Assets Limited and their subsidiaries, direct and indirect
PDPA	Personal Data Protection Act 2010 and Personal Data Protection (Amendment) Act 2024 and as amended from time to time
PDPA Laws	the PDPA, Personal Data Protection Regulations 2013 ("**PDPR**"), Personal Data Protection Standards 2015, GCBPDT, GDBN, GDPO and any other standards, guidelines or directives issued by the Commissioner or pursuant to the PDPA or PDPR from time to time, as

	applicable to the relevant Company
personal data	any information in respect of commercial transactions that relates directly or indirectly to a Data Subject who is identified or identifiable from that information or from that and other information in the possession of a Data Controller, including any sensitive personal data and expression of opinion about the Data Subject Examples include: (a) name, address, e-mail address, telephone number, national registration identity card number, passport number; (b) name of family members and personal information about them (e.g. para (a) items); (c) employment details, academic qualifications; and (d) bank accounts, credit card accounts, financial position, transaction details and other information where the Data Subject can be identified
Privacy Notice	written notice issued to Data Subjects
processing	collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including: (a) the organization, adaptation or alteration of personal data; (b) the retrieval, consultation or use of personal data; (c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or (d) the alignment, combination, correction, erasure or destruction of personal data
Responsible Party	the heads of departments of the Company
Senior Management	(i) in respect of HLMC, the Managing Director, Finance & Treasury Director, and General Counsel; and (ii) in respect of other Companies, the most senior members of its management team
Sensitive Personal Data	any personal data that includes information related to a Data Subject's physical or mental health or condition, political opinions, religious or similar beliefs, the commission or alleged commission of any offence, Biometric Data, or any other personal data as may be determined by the Minister by order published in a government gazette
Significant Harm	a personal data breach that:- (a) may result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property; (b) may be misused for illegal purposes; (c) consists of sensitive personal data; or (d) consist of personal data and other personal information which, when combined, could potentially enable identity fraud

Significant Scale	a personal data breach that affected more than one thousand (1,000) Data Subjects