


<b>POLICY OWNER</b>	: Corporate Secretarial & Legal			
<b>TITLE</b>	: <b>IMU HEALTH GROUP PERSONAL DATA PROTECTION POLICY ("IMUH PDP POLICY")</b>			
Reference No.	: IMU/POL/CSL/02	Edition		: 1
Approval Body	: Board of Directors – IMU Health Sdn Bhd Management Committee	Approval Date		: 17 May 2021
Effective Date	: 1 June 2021	Pages		: 21



# IMU HEALTH GROUP PERSONAL DATA PROTECTION POLICY



## Contents

1	Overview .....	3
1.1	Foreword .....	3
1.2	Objectives .....	3
1.3	Application .....	3
1.4	Personal Data .....	4
1.5	Data Protection Notice .....	4
1.6	Data Protection Personnel .....	5
2	Data Protection Principles & Standards .....	6
2.1	Principles .....	5
2.2	Standards .....	6
2.2.1	Consent .....	6
2.2.2	Accuracy, Correction & Relevance .....	7
2.2.3	Protection & Storage .....	7
2.2.4	Access .....	8
2.2.5	Retention, Erasure & Cessation .....	8
2.2.6	Transfer .....	8
2.2.7	Incident Reporting .....	10
2.2.8	Data Portability .....	12
2.2.9	Documentation & Records .....	12
2.2.10	Training .....	12
2.2.11	Request, Complaint, Notification & Inquiries .....	13
2.2.12	Sensitive Personal Data & Vulnerable Persons .....	13
2.2.13	Profiling or Monitoring of Persons .....	14
3	Risk Assessment & Management .....	14
3.1	Data Protection Impact Assessment .....	14
3.2	Third-Party Dealings .....	15
4	Applicable Laws & Regulations .....	15
4.1	Relevant Laws & Regulations .....	15
4.2	Multijurisdictional Law .....	16
4.3	Register of Data Protection-Related Laws & Regulations .....	16
5	National Registrations .....	16
5.1	Registration Requirements .....	16
6	Contracting .....	16
6.1	Standard Contractual Clauses .....	16
7	Policy Review & Audit .....	17
7.1	Periodic Assessment .....	17
8	Group Policies .....	17
8.1	IHH Personal Data Protection Governance Framework .....	17
8.2	Relevant Group Policies .....	17
9	Glossary .....	18
9.1	Terminologies .....	18
10	External References .....	19
10.1	National Laws, Regulations, Advisories & Guidelines .....	19
10.2	Other Laws, Regulations, Advisories & Guidelines .....	21



## **IMU HEALTH SDN BHD Personal Data Protection Policy**

### **1. Overview**

#### **1.1. Foreword**

- 1.1.1 Globally, legislations have been established to regulate how information from which a person could be identified (“personal data” – which shall also mean “personal information”) is dealt with to ensure the protection of personal data.
- 1.1.2 This policy document (“Policy”) aims to establish how the IMU Health Sdn Bhd group of companies (collectively, “Group”) will comply with applicable laws and regulations pertaining the protection of personal data (“data protection”). A subsidiary, related corporation, affiliate, division, centre, department, unit and/ or school of the Group shall be referred to in this Policy as an “entity”.
- 1.1.3 The Policy supports the Group’s intention to leverage and process data to improve its operational, institutional and clinical performance and pursue business opportunities.
- 1.1.4 For the purposes of this Policy, reference to “protection” is equivalent to the safeguarding of “privacy” (i.e. “data protection” shall mean “data privacy”).

#### **1.2. Objectives**

- 1.2.1 This Policy outlines the basic requirements and considerations that the Group needs to take into account to safeguard the proper use, disclosure and storage of personal data in the Group’s possession, so that we comply with the applicable laws and regulations.
- 1.2.2 Noting sub-section 1.6, an entity may, for the purposes of implementing this Policy, develop its own data protection policies or procedures necessary to ensure compliance with applicable laws and regulations.
- 1.2.3 This Policy serves as the Group’s intra-group personal data sharing agreement and organisation rules for dealing with personal data. Where necessary and appropriate, this Policy shall serve as the basis for the Group to establish “Binding Corporate Rules” or other intra-group data protection protocols evidencing comparable standards of data protection within the Group in compliance with applicable laws and regulations.

#### **1.3. Application**

- 1.3.1 This Policy is a document internal to the Group and shall only be internally accessed and used by the Group.
- 1.3.2 This Policy supplements any measure required for an entity’s compliance with applicable laws and regulations and other Group policies (such as in relation to retention of medical records). Where this Policy is inconsistent with any such applicable laws and regulations, such inconsistency shall be resolved in compliance with such applicable laws and regulations.



## **1.4. Personal Data**

1.4.1 In relation to a person, types of personal data may include:

- a) Full name, fingerprint, national identification number, date of birth, residential address, personal email address, mobile device number, and vehicle number.
- b) Biometric and genetic data, and medical records, sexual life and orientation, and other health-related data.
- c) Education data, and financial data (including bank account, credit card, debit card, or other payment instrument details).
- d) Criminal records and data about sanctions and other punitive measures levied.
- e) Family or legal representation data.
- f) Photography or videography image.
- g) Passwords.
- h) Location data.
- i) Internet Protocol (IP) address and “cookie ID”.
- j) Data in character, number, symbol and/or other code representation that uniquely identifies a person.
- k) Data about racial and ethnic origins, caste or tribe, political opinions, and religious and philosophical beliefs.
- l) Data about memberships of unions, associations, and foundations.

1.4.2 Business contact information made publicly known for business purposes may not necessarily be deemed personal data.

1.4.3 Certain information may not in itself and on its own afford identification of a person and would not constitute personal data.

1.4.4 Where an entity is in doubt as to whether information is personal data, the entity shall consult the DPO. Where in respect of the foregoing the DPO is in doubt, the DPO shall consult the IHH GDPO (“GDPO”).

## **1.5. Data Protection Notice**

1.5.1 The DPO shall, in consultation with the GDPO, develop a data protection notice (“Data Protection Notice”) in accordance with this Policy and applicable laws and regulations for communication to the general public. A Data Protection Notice shall be approved by an entity’s Chief Executive Officer or equivalent.



- 1.5.2 The Data Protection Notice shall provide a definition and description of the terms “personal data” or “personal information” (as the case may be), describe an entity’s personal data usage purposes, data protection practices, and provide contact details of the DPO for the receipt of information, inquiries, requests, complaints, and feedback.
- 1.5.3 A Data Protection Notice may be legally construed to regulate legal relations between an entity and the general public. Where applicable, an entity may develop a Data Protection Notice that can be legally relied on to evidence the procuring of “implied” consent.
- 1.5.4 A Data Protection Notice shall be comprehensible and made available to the general public by such means and manner necessary for legally “effective” notice, including through digital (e.g. websites) and physical (e.g. business operations sites) avenues managed by an entity.

## **1.6. Data Protection Personnel**

- 1.6.1 The Group shall maintain an appointment of a Data Protection Officer (DPO). Subject to and in accordance with other Group policies, the DPO may delegate duties or appoint personnel to deputise for the DPO appointment. The DPO appointment shall be assumed by Head, Compliance Unit, Group Risk Management, unless otherwise appointed.
- 1.6.2 An entity shall maintain appointments of Deputy Data Protection Officer (DyDPO). Subject to and in accordance with other Group policies, the DyDPO may delegate duties or appoint personnel to deputise for the DyDPO appointment.
- 1.6.3 The DPO shall be the overall custodian of this Policy for the Group. Requests for disclosure of this Policy to third parties shall be directed to the DPO. The DPO shall be the contact point for data protection matters concerning or impacting more than one country jurisdiction, including contracting matters.
- 1.6.4 The DPO shall be the custodian of an entity’s Data Protection Notice. The DPO shall be the contact point for data protection matters concerning or impacting the entity, including contracting matters.
- 1.6.5 A person shall report non-compliance with this Policy or a Data Protection Notice to the DPO, if not to an entity’s Chief Executive Officer or equivalent. Where not appropriate or possible to do so, such person shall report such non-compliance to the DPO. Where reporting to the DPO is not appropriate or possible, such person shall do so by means of other relevant Group policies.
- 1.6.6 An entity shall raise any inconsistency between this Policy/Data Protection Notice and applicable laws and regulations/other Group policies to the DyDPO. Where in doubt about such inconsistency, the DyDPO shall consult the DPO.



1.6.7 Subject to paragraph 1.3.2 of this Policy, inconsistency between the Data Protection Notice and applicable laws and regulations/other Group policies, shall be jointly decided on by the relevant entity head and the DPO. Where in doubt regarding such decision, the DPO shall consult the GDPO.

1.6.8 Subject to paragraph 1.3.2 of this Policy, inconsistency between this Policy and applicable laws and regulations/other Group policies shall be jointly decided on by the relevant entity head and the DPO.

## **2. Data Protection Principles & Standards**

### **2.1. Principles**

2.1.1 Data protection shall constitute the core of the Group's conduct of business (i.e. data protection considerations shall apply by default to the Group's conduct of business).

2.1.2 The Group shall use reasonable best efforts to take data protection into consideration in the designing of business processes.

2.1.3 The Group shall collect, store, and use personal data only to such extent relevant and necessary for the intended purposes for which personal data is to be used.

### **2.2. Standards**

#### **2.2.1 Consent**

2.2.1.1 Before dealing with personal data, an entity shall ensure adequate consent has been secured from persons able to provide such consent, unless exempted or waived by applicable law and regulations.

2.2.1.2 An entity shall before or at the time of personal data collection or receipt, establish and document the following:

- a) "Effective" notice, with reference to relevant legal standards, of intended purposes (internal and external to the entity, including for commercial purposes) for such proposed collection has been provided.
- b) "Effective" notice, with reference to relevant legal standards, of the intended uses (internal and external to the entity, including for commercial uses) of personal data proposed to be collected has been provided.
- c) In accordance with applicable laws and regulations, "explicit" or "implied" consent for such proposed collection on the bases of such intended purposes and uses, taking into consideration reference in relevant legal standards to "informed" consent, has been secured.
- d) In accordance with applicable laws and regulations, mechanisms to opt in (for "explicit" consent) or opt out (for consent other than "explicit" or "implied") of providing consent, have been provided.



- 2.2.1.3 Unless otherwise provided for by applicable laws and regulations, where applicable laws and regulations neither stipulate “explicit” consent nor specifically provide for “implied” consent, “opt-out” consent shall be secured.
- 2.2.1.4 A Data Protection Notice shall reasonably allow for the receipt of legal requests for the withdrawal of consent in accordance with applicable laws and regulations. An entity shall establish mechanisms to effect the withdrawal of consent.

## **2.2.2 Accuracy, Correction & Relevance**

- 2.2.2.1 An entity shall upon being made aware maintain the accuracy, completeness, currency, and clarity of personal data in its possession, to the extent technically feasible.
- 2.2.2.2 A Data Protection Notice shall reasonably allow for the receipt of legal requests for personal data to be corrected or updated in accordance with applicable laws and regulations. An entity shall establish mechanisms for the correction or updating of personal data upon request.

## **2.2.3 Protection & Storage**

- 2.2.3.1 An entity shall comply with other relevant Group policies to avoid and prevent accidental or unauthorised loss, access, collection, processing, use, disclosure, transfer, replication, alteration, disposal, erasure, destruction, or similar risks, to the extent feasible.
- 2.2.3.2 An entity shall establish appropriate security measures including physical, technical, administrative, management, operational, procedural, legal, regulatory, and compliance controls.
- 2.2.3.3 An entity shall, to the extent technically feasible, ensure secure physical and digital storage of personal data, including in relation to physical forms, files, letters, and other physical documentation handled by frontline operations and medical record offices.
- 2.2.3.4 In relation to personal data stored digitally, to the extent technically feasible, an entity shall ensure the use of, among others:
  - a) Encryption
  - b) Masking
  - c) Tokenization
  - d) Other obfuscation techniques, access restriction techniques, and data backup and recovery techniques.
- 2.2.3.5 Third-party and overseas storage of personal data shall be in accordance with applicable laws and regulations and Group policies.



## **2.2.4 Access**

- 2.2.4.1 An entity shall, to the extent technically feasible, provide access to and supply personal data to parties as provided for by applicable laws and regulations.
- 2.2.4.2 A Data Protection Notice shall reasonably allow for the receipt of legal requests for access to and copies of personal data in accordance with applicable laws and regulations.
- 2.2.4.3 Such personal data access and reproduction may include providing information about the circumstances and ways in which personal data has or may have been dealt with, the type of personal data dealt with, and the parties involved in such dealings.

## **2.2.5 Retention, Erasure & Cessation**

- 2.2.5.1 Subject to legal requirements of retention, availability, storage, processing, and disposal, an entity shall, to the extent technically feasible:
  - a) Retain personal data and maintain association of personal data with persons to the extent relevant and necessary for the purposes for which the personal data was collected and processed.
  - b) Cease to retain personal data or associate personal data with persons, as soon as such retention or association is no longer relevant and necessary for the purposes for which the personal data was collected and processed, and such retention or association is no longer relevant and necessary for other legal or business purposes.
- 2.2.5.2 In accordance with applicable laws and regulations, a Data Protection Notice shall reasonably allow for the receipt of legal requests for the following: destruction, permanent and complete erasure/deletion, anonymisation, pseudonymisation, or cessation of use of personal data.
- 2.2.5.3 Subject to applicable laws and regulations and technical feasibility, an entity shall establish mechanisms to destroy, permanently and completely erase/delete, anonymise, or pseudonymise, as the case may be, all personal data in respect of which retention or association with persons is to cease, and shall document and maintain records of all such actions.

## **2.2.6 Transfer**

- 2.2.6.1 Unless prohibited, exempted, waived, or otherwise required by applicable laws and regulations, transfer of personal data shall be subject to one or more of the following conditions ("Transfer Conditions"):
  - a) Transferee is bound by data protection contractual obligations, which shall be drafted in accordance with standard contractual clauses provided by applicable laws and regulations where applicable.
  - b) Consent for transfer of personal data has been secured.





- c) Laws and regulations that the transferee is subject to provide comparable standards of data protection.
- d) Transfer is necessary for the performance of a contract.

2.2.6.2 Cross-border transfer of personal data by an entity is prohibited unless one of the following scenarios applies:

- a) Where provided for by applicable laws and regulations, government approval of such transfer to the location or transferee is secured, regardless of whether the Transfer Conditions are satisfied.
- b) Where provided for by applicable laws and regulations, relevant regulatory authorities have approved the Group's or the entity's submissions of "Binding Corporate Rules" or other intra-group protocols the approvals of which permit such transfer.
- c) Where applicable laws and regulations provide that such transfer is permitted where either one or all the Transfer Conditions are satisfied.
- d) Where applicable laws and regulations provide that such transfer is permitted regardless of whether the Transfer Conditions are satisfied.
- e) Where personal data has been "deidentified" such that it is no longer deemed personal data by applicable laws and regulations.
- f) Applicable laws and regulations obligate such transfer.

2.2.6.3 Transfer of personal data within the Group shall be in accordance with paragraphs 2.2.6.1 and 2.2.6.2. An entity shall comply with any stipulation by applicable laws and regulations to adopt standard contractual clauses to contractually govern transfer of personal data.

2.2.6.4 The DyDPO shall consult the DPO in respect of any cross-border transfer of personal data.

2.2.6.5 Where applicable laws and regulations require the use of but do not stipulate contractual terms for the transfer of personal data, this Policy may serve as such contractual terms between an entity and the Group.

2.2.6.6 Unless otherwise intended, compliance with this Policy evidences the application of comparable standards of data protection within the Group.

2.2.6.7 The DyDPO shall work with the DPO to make a submission where an entity is legally required to submit "Binding Corporate Rules" or other intra-group protocols for approval by regulatory authorities to permit transfer of personal data within the Group.



2.2.6.8 A Data Protection Notice shall provide notification of potential transfer of personal data overseas where applicable laws and regulations deem reasonable. Such notification shall include information on the intended purposes of such transfers and the identities of such transferees.

## **2.2.7 Incident Reporting**

2.2.7.1 An entity shall develop incident response plans (“Incident Response Plans”) in consultation with the DPO to be implemented in the event of awareness of an actual or suspected compromise of data protection (“Incident”) including in relation to personal data, accidental or unauthorised loss, access, collection, processing, use, disclosure, transfer, replication, alteration, disposal, erasure, or destruction.

2.2.7.2 An entity shall maintain reasonably detailed, complete, and communicable documentation on an Incident. Such documentation may include details on the personal data compromised or potentially compromised, logs of identities of persons notified and actions taken, and current timelines of events.

2.2.7.3 Incident Response Plans shall align reporting and notification requirements internal and external to an entity.

2.2.7.4 Incident Response Plans shall include the following protocols for communication internal and external to an entity:

### **a) Internal Communication**

- i. A person shall without undue delay notify the relevant entity department head(s) of an Incident. Where a person is in doubt as to whether an Incident has or may occur, the person shall without undue delay notify the relevant entity department head(s).
- ii. Where the relevant entity department head(s) deem(s) a notified Incident to be of significant or potentially significant detriment, graveness, severity, magnitude, or impact, the relevant entity department head(s) shall without undue delay notify the DyDPO. Where in doubt about such significance or potential significance, the relevant entity department head(s) shall without undue delay notify the DyDPO.
- iii. Where the DyDPO deems a notified Incident to be of significant or potentially significant detriment, graveness, severity, magnitude, or impact, the DyDPO shall without undue delay notify the DPO. Where in doubt about such significance or potential significance, the DyDPO shall without undue delay notify the DPO.

Without undue delay, person notifies the relevant entity department head(s) of Incident

Incident of significant or potentially significant detriment, graveness, severity, magnitude, or impact

Without undue delay, relevant entity department head(s) notify/notifyes the DyDPO of Incident

Incident of significant or potentially significant detriment, graveness, severity, magnitude, or impact

Without undue delay, DyDPO notifies the DPO of Incident

- iv. An entity shall maintain records of Incidents not deemed necessary for notification to the DyDPO at time of occurrence.

b) External Communication

- i. In accordance with applicable laws and regulations, an entity shall establish mechanisms and timelines for the timely reporting of an Incident to regulatory authorities, and if necessary, timely notification of affected persons.
- ii. An entity shall take into account circumstances on the bases of which applicable laws and regulations prohibit, exempt, or waive such regulatory reporting or notification.
- iii. Where, in accordance with applicable laws and regulations, the DPO deems that regulatory reporting or notification is not to be carried out, the entity shall maintain reasonably detailed, complete, and communicable documentation justifying so.



- iv. The DyDPO shall notify the DPO before reporting an Incident to regulatory authorities or notifying affected persons.
- v. The DyDPO shall notify the DPO as soon as the DyDPO anticipates not being able to meet regulatory reporting or notification requirements.
- vi. Where the DyDPO anticipates not being able to meet reporting or notification requirements in accordance with applicable laws and regulations, the entity shall maintain reasonably detailed, complete, and communicable documentation justifying so.
- vii. Where the DyDPO is in doubt as to whether an Incident requires regulatory reporting or notification, the DyDPO shall consult the DPO.

### **2.2.8 Data Portability**

- 2.2.8.1 An entity shall, to the extent technically feasible, establish mechanisms to receive and respond to data porting requests where required by applicable laws and regulations. Personal data provided pursuant to such requests should be in reasonably structured, commonly used, and machine-readable format.
- 2.2.8.2 A Data Protection Notice shall reasonably allow for the receipt of legal requests for data porting in accordance with applicable laws and regulations.

### **2.2.9 Documentation & Records**

- 2.2.9.1 An entity shall maintain reasonably detailed, complete, and communicable documentation in compliance with this Policy, other relevant Group policies, and applicable laws and regulations.
- 2.2.9.2 An entity shall endeavour to adopt relevant Group or entity document repositories and knowledge management and information access platforms.
- 2.2.9.3 Where there are requests from outside an entity to access to this Policy, the entity shall make reference to the entity's Data Protection Notice. Where an entity's Data Protection Notice is not sufficient to meet such requests, the entity shall consult the DyDPO. Where the DyDPO deems that access external to the entity may be necessary, the DyDPO shall consult the DPO.

### **2.2.10 Training**

- 2.2.10.1 An entity shall ensure communication of this Policy internal to the entity and shall conduct training initiatives in relation to this Policy.
- 2.2.10.2 An entity shall conduct training initiatives in relation to the entity's Data Protection Notice.



### **2.2.11 Request, Complaint, Notification & Inquiries**

- 2.2.11.1 An entity shall without undue delay notify the DyDPO when it receives requests, complaints, notifications, or inquiries that are of significant or potentially significant detriment, graveness, severity, magnitude, or impact to the entity.
- 2.2.11.2 The DyDPO shall without undue delay notify the DPO when such requests, complaints, notifications, or inquiries to be of significant or potentially significant detriment, graveness, severity, magnitude, or impact to the Group or more than one country jurisdiction, the DyDPO shall immediately notify the DPO.
- 2.2.11.3 An entity shall maintain records of such requests, complaints, notifications, or inquiries not deemed necessary for notification to the DyDPO at the time of occurrence.

### **2.2.12 Sensitive Personal Data & Vulnerable Persons**

- 2.2.12.1 An entity shall take into account certain types of personal data that are either specified as or deemed “sensitive” by applicable laws and regulations (“Sensitive Personal Data”) and thus requiring more robust standards of protection. Notwithstanding the foregoing, an entity shall endeavour to ensure similar standards of protection to personal data not so specified or deemed.
- 2.2.12.2 An entity shall establish measures to ensure protection of the personal data of certain groups of persons deemed more vulnerable by applicable laws and regulations (“Vulnerable Persons”) such as, but not limited to, juveniles, the elderly, persons with disabilities, and persons with diminished mental capacity.
- 2.2.12.3 An entity shall ensure the establishing of:
  - a) the capacity and ability of a person to provide consent for such person’s personal data to be dealt with on such person’s own behalf and such person’s understanding of the nature and consequences of providing consent.
  - b) in relation to a person under the age of 16, mechanisms for age verification and, unless prevented by applicable laws and regulations and other Group policies, parental, guardianship or other legal representation consent for such person’s personal data to be dealt with.
  - c) in relation to persons with disabilities or diminished mental capacity, mechanisms for, unless prevented by applicable laws and regulations and other Group policies, next-of-kin, guardianship or other legal representation consent for such person’s personal data to be dealt with.
- 2.2.12.4 An entity shall have the discretion to deem that a person of at least 18 years of age has the capacity and ability to provide consent and the understanding of providing consent, unless otherwise required by applicable laws and regulations or other Group policies (such as in relation to the general age of majority of 18), and provided an entity has no reason to believe otherwise.



2.2.12.5 An entity shall secure consent from a person's parent, guardian or other legal representative for such person's personal data to be dealt with where there is reason to believe that a person regardless of age may not have the capacity and ability to and the understanding of providing consent, subject to applicable laws and regulations and other Group policies.

2.2.12.6 Where an entity is in doubt as to whether personal data is Sensitive Personal Data or whether persons are Vulnerable Persons, the entity shall consult the DyDPO. Where in doubt, the DyDPO shall consult the DPO.

### **2.2.13 Profiling or Monitoring of Persons**

2.2.13.1 An entity shall consult the DyDPO before carrying out any activity in relation to the profiling of persons or monitoring of persons' behaviours based on automatic processing of personal data and/or automated decision-taking in the absence of human intervention.

## **3. Risk Assessment & Management**

### **3.1. Data Protection Impact Assessment**

3.1.1 Where dealing with personal data may result in significant or novel risk to data protection, an entity shall conduct a Data Protection Impact Assessment (DPIA) to identify, assess and address any data protection risk, and where necessary, implement technical and/or organisational measures to safeguard against such risk to ensure compliance with applicable laws and regulations. The conduct of a DPIA shall be done in consultation with the DyDPO, and where necessary, the DPO.

3.1.2 Scenarios warranting a DPIA may include when a system, process, or physical setup is new and in the process of being designed, or when a system, process, or physical setup is in the process of undergoing major change.

3.1.3 Scenarios requiring a DPIA may include:

- a) Introduction of new technology or technological techniques.
- b) Dealing with Sensitive Personal Data.
- c) Dealing with personal data of Vulnerable Persons.
- d) Dealing with personal data in respect of which if data protection is compromised would result in physical harm.
- e) Profiling of persons.
- f) Monitoring of persons' behaviours.
- g) Significant or large-scale tracking of persons' locations or behaviours.
- h) Significant or large-scale monitoring of publicly accessible places.



i) Significant or large-scale automated decision-making.

3.1.4 The entity shall consult the DPO where there is in doubt as to whether a DPIA is required. Where the DyDPO is in doubt, the DPO shall be consulted.

3.1.5 The DyDPO shall be consulted on any data protection concern or matter pertaining to data protection even where a DPIA is assessed not to be required.

### **3.2. Third-Party Dealings**

3.2.1 An entity shall establish measures to manage third-party dealings involving personal data to ensure compliance with this Policy, and to ensure third-party compliance with applicable laws and regulations.

3.2.2 An entity shall ensure that a contract with a third party clearly:

a) Identifies the parties (referred to in some jurisdictions as “controller”, “user”, “fiduciary”, “organisation”, or “individual”) that either instruct, authorise and/or control the processing of personal data by other parties (referred to in some jurisdictions as “processor”, “intermediary”, “person”, or “entity”) or are entitled to do so, including by way of determining the intended purposes, means and/or manner of such processing.

b) Specify any data protection obligations on the third parties, which shall at minimum include all obligations prescribed under applicable laws and regulations.

c) Stipulates reporting, as between the parties, and rectification of and recourse for any breach of third-party data protection obligations.

d) Identifies the regulatory authority/authorities with jurisdiction over data protection regulatory aspects of such contracts.

3.2.3 Where possible, an entity shall ensure that a contract with a third party provides for an entity’s right to audit the third party for compliance with applicable laws and regulations and in relation to this Policy.

3.2.4 A Data Protection Notice shall provide reasonable notification of potential transfer of personal data to third parties to the extent subject to any provision of reasonableness in applicable laws and regulations. Such notification shall include information on the intended purposes of such transfers and the identities of such transferees.

## **4. Applicable Laws & Regulations**

### **4.1. Relevant Laws & Regulations**

4.1.1 Forms of applicable laws and regulations shall include international and national legal and quasi-legal instruments, government and regulatory pronouncements, regulatory and industry standards, and decisions, statements, guidelines, advisories and opinions of regulatory authorities and authoritative bodies.



- 4.1.2 Subject matters of applicable laws and regulations shall include data protection, health, labour, commerce, information technology and security, cybersecurity, digital technology, national identification number, tax, consumer rights, constitutional rights, civil code rights, and human rights.

#### **4.2. Multijurisdictional Law**

- 4.2.1 The DyDPO shall, in consultation with the DPO, determine the application of international, regional, extraterritorial, or cross-border laws, regulations, or standards (“Multijurisdictional Law”) to an entity on a case-by-case basis.
- 4.2.2 An entity shall not bind itself, any other entity or the Group to Multijurisdictional Law. An entity must, through the DyDPO, obtain the DPO's approval before agreeing to bind itself, any other entity or the Group to Multijurisdictional Law.
- 4.2.3 An entity shall consult the DyDPO on data protection matters pertaining to Multijurisdictional Law. Where in doubt about data protection matters pertaining to Multijurisdictional Law, the DyDPO shall consult the DPO.

#### **4.3. Register of Data Protection-Related Laws & Regulations**

- 4.3.1 An entity shall maintain a register of data protection-related laws and regulations detailing obligations and requirements.

### **5. National Registrations**

#### **5.1. Registration Requirements**

- 5.1.1 Where applicable, an entity shall maintain national registrations of the entity, data protection personnel appointments, and/or activities in relation to the dealing with of personal data.

### **6. Contracting**

#### **6.1. Standard Contractual Clauses**

- 6.1.1 The DPO shall develop standard contractual clauses for data protection (“Group Clauses”) to be used for the Group’s contracting purposes.
- 6.1.2 The DyDPO may, in consultation with the DPO, reasonably customise the Group Clauses to develop standard contractual clauses for the entity’s contracting purposes (“Entity Clauses”) in place of the Group clauses.
- 6.1.3 An entity shall consult the DyDPO on matters pertaining to the Group Clauses or any Entity Clauses. Where in doubt about the Group Clauses, the DyDPO shall consult the DPO.
- 6.1.4 Where an entity decides that contractual clauses provided by a third party is to be used as bases for contracting, such contractual clauses shall be comparable to the Group Clauses or any Entity Clauses.



## 7. Policy Review & Audit

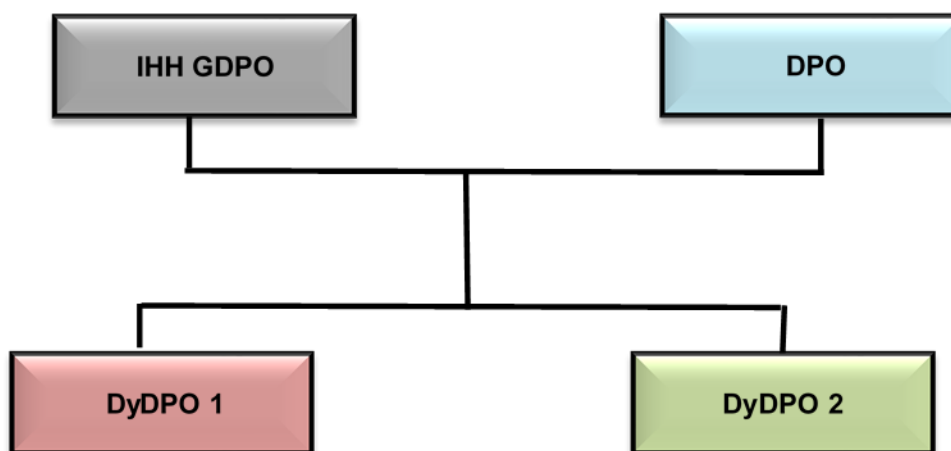
### 7.1. Periodic Assessment

7.1.1 This Policy shall be reviewed for relevance on an annual basis or as and when required, such as when an initiative involves a significant amount of personal data and may be done so in conjunction with an audit of compliance with this Policy.

## 8. Group Policies

### 8.1. IMUH Personal Data Protection Governance Framework

#### Reporting Structure Reporting Structure



#### Legend

IHH GDPO: IHH Group Data Protection Office

DPO: IMUH Group Data Protection Officer

DyDPO: Deputy Data Protection Officer

### 8.2. Relevant Group Policies

8.2.1 Minimally, the other Group policies that shall be taken in account to ensure compliance with this Policy are as follows:

- a) Compliance
  - i. IHH Third Party Code of Conduct
  - ii. IMUH Group Third Party Code of Conduct
- b) Finance
  - i. IHH Limits of Authority
  - ii. IMU Education Sdn Bhd's Limits of Authority
- c) Human Resource
  - i. IHH Whistleblowing Policy
  - ii. IHH Employees Code of Conduct Policy



- iii. Employee Conflict of Interest Declaration
- iv. Employee Confidentiality Agreement
- v. IMU Education Sdn Bhd's Whistleblowing Policy
- vi. IMU Education Sdn Bhd's Employees Code of Conduct Policy
- vii. Employee Conflict of Interest Declaration
- viii. Employee Confidentiality Agreement

d) Information Technology & Information Security

IHH:

- i. SOP\_PIT\_004 - Information Security Policy
- ii. SOP\_PIT\_005 - Data Integrity
- iii. SOP\_PIT\_006 Cyber Security
- iv. SOP\_PIT\_008 Reporting of Information Security Problems
- v. SOP\_PIT\_015 Information Classification and Handling
- vi. SOP\_PIT\_018 Information Access Control
- vii. SOP\_PIT\_022 Information Asset Management
- viii. SOP\_PIT\_001\_Acceptable\_Use\_of\_Information\_and\_IT\_Assets
- ix. SOP\_PIT\_021\_Compliance\_Management
- x. SOP\_PIT\_109\_Encryption Policy

IMU:

- xix. IMU-POL-ITS-06 - IT Security Policy
- xx. IMU-POL-ITS-06 - IT Security Policy
- xxi. IMU/POL/ITS/14 - Network Communication Security Policy
- xxii. IMU/POL/ITS/15 – Cybersecurity Incident Handling Policy
- xxiii. IMU-POL-ITS-05 - System Access Control Policy
- xxiv. IMU-POL-ITS-13 Information Technology Asset Management Policy
- xxv. IMU-POL-ITS-02 - Email Policy for All Authorized User
- xxvi. Draft Information Classification Policy

e) Legal

Contracting guidelines or other guidelines/policies/standards issued by IMU's Legal

## 9. Glossary

### 9.1. Terminologies

- a) “affiliate” – Means any entity that controls, is controlled by, or is under common control, in each case either directly or indirectly with either a subsidiary or related corporation of the Group, where “control” means the ownership or more than 50% of the voting stock, shares or interests of the entity.
- b) “applicable laws and regulations” – As described in sub-section 4.1.
- c) “Binding Corporate Rules” – As referenced in the General Data Protection Regulation, are data protection policies adhered to by companies established in the European Union for transfers of personal data outside the European Union within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They must be legally binding and enforced by every member concerned of the group.
- d) “data porting” – Refers to the act of data migration which is the process of transferring data from a source system to a target system.
- e) “deidentified” – In relation to a dataset, refers to the state of having identifying



information removed from the dataset so that individual data cannot be linked with specific individuals.

- f) “Data Protection Impact Assessment” – Refers to a data protection-related impact assessment tool which objective is to identify and analyse how data protection may be affected by actions or activities.
- g) “Data Protection Notice” – A notice to inform stakeholders on how their personal data is managed.
- h) “effective” – In the context of providing notice, refers to a notice being effectively delivered or brought to the attention of, and reasonably comprehensible to, its target audience.
- i) “explicit” – In the context of consent, is synonymous with “express” consent.
- j) “implied” – In the context of consent, is synonymous with “implicit” and “deemed” consent.
- k) “informed” – For the purposes of this Policy, in the context of consent, refers to consent provided on the basis of having reasonably understood the implication of providing such consent.
- l) “opt-out” – In the context of consent, refers to providing consent by not declining to provide consent where such option to decline consent is provided.

## **10. External references**

### **10.1. National Laws, Regulations, Advisories & Guidelines**

- a) Malaysia
  - i. Personal Data Protection Act 2010
  - ii. Personal Data Protection (Class of Data Users) Order 2013
  - iii. Personal Data Protection (Registration of Data User) Regulations 2013
  - iv. Personal Data Protection (Fees) Regulations 2013
  - v. Personal Data Protection (Compounding of Offences) Regulations 2016
  - vi. Personal Data Protection (Class of Data Users) (Amendment) Order 2016
  - vii. Personal Data Protection Standard (2015)
  - viii. Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010 ('pc01/2020') (dated 14 February 2020)