**Version 29.05.2024**

# GOLDEN LAND BERHAD

[Registration No. 199401012688 (298367-A)]
[Incorporated in Malaysia]

---

# PERSONAL DATA PROTECTION POLICY

---

# TABLE OF CONTENTS

## 1. PURPOSE

Golden Land Berhad ("**GLB**") and its subsidiaries (each, the "**Company**" and collectively, the "**Group**") are committed to complying with the Personal Data Protection Act 2010 of Malaysia ("**PDPA**"). This Personal Data Protection Policy ("**Policy**") contains the policies and practices of the Group to comply with the PDPA.

## 2. REQUIREMENTS

2.1 The requirements of the Company under the PDPA are as follows:

(a) develop and implement policies and practices necessary for the Company to meet its obligations under the PDPA;

(b) develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA;

(c) communicate to its employees information about this Policy;

(d) make information available on request about the Policy and the complaint process referred to in paragraph (b) above; and

(e) (i) appoint one or more data protection officers. These are the persons responsible for ensuring that the Company complies with the PDPA ("**Data Protection Officers**" or "**DPO**") and (ii) make available to the public the business contact information of at least one of the Data Protection Officers.

2.2 GLB has implemented this Policy and certain personal data protection internal practices ("**PDP Internal Practices**") attached hereto as Annexure A for the Group to meet the requirements under the PDPA.

## 3. PRIMARY DATA PROTECTION RULES

The Company must comply with the following rules when collecting, using or disclosing Personal Data of any individual:

| | **Rules** |
|---|---|
| (a) | Obtain the consent of the individual or, if consent is not obtained, ensure that the collection, use or disclosure is permitted under Malaysia law |
| (b) | Ensure that the individual is informed of the purpose of such collection, use or disclosure |
| (c) | Ensure that the Personal Data is only collected, used or disclosed for such purpose, and no other purpose |
| (d) | Ensure that the Personal Data is properly retained, protected and disposed of in accordance with the PDP Internal Practices |

## 4. WHAT IS PERSONAL DATA

4.1 Personal Data is data (whether true or not) about an individual who can be identified:

(a) from such data alone; or
(b) from such data and other information that the organisation has or is likely to have access.

4.2 Non-exhaustive examples of an individual's Personal Data:

(a) Personal contact information, including name, personal address, personal email address and telephone number, bank account and tax details;
(b) NRIC, passport or other equivalent identification number; and
(c) Other information where the individual can be identified from such information.

Personal Data does NOT cover an individual's "business contact information" such as his/her position, title, business address, business email/ fax number.

4.3 The PDPA deals with only with the Personal Data of individuals (i.e. natural persons), and does not extend to data of companies or corporations.

## 5. PURPOSES OF COLLECTION, USE AND/OR DISCLOSURE OF PERSONAL DATA

5.1 Examples of some situations where the Company collects, uses and/or discloses Personal Data, and the purposes of such are set out below:

| | Person | Personal Data Collected | Purposes |
|---|---|---|---|
| (a) | Job applicants | • Information in job applicant's curriculum vitae or the job application forms (e.g. personal email, telephone number, address, educational history and background, salary at current/previous place of employment). | • To evaluate the applicant and to attend to all administrative work to process the job application. |
| (b) | Employees | • Personal Data of its employees (e.g. information in (a) above, bank account details, information relating to their salary, tax etc.);<br><br>• Personal Data of employees within the | • For legal, audit and other compliance purposes, managing the employment relationship, including filings with or disclosure to authorities and bankers. |

| | | | |
|---|---|---|---|
| | | Group and related corporations of the Group. | |
| (c) | Directors and other officers | • Personal Data of its directors and other officers (e.g. information in (a) above, bank account details, information relating to their fee, tax etc.);<br><br>• Personal Data of directors and other officers within the Group and related corporations of the Group. | • For legal, audit and other compliance purposes, managing the employment relationship, including filings with or disclosure to authorities and bankers. |
| (d) | Shareholders and investors | • Personal Data of shareholders/investors of GLB when they write to GLB to raise queries or when they submit forms to GLB (e.g. relating to proxy forms/ dividends/ general meetings);<br><br>• Personal Data of shareholders/investors of GLB with their shareholding interests (e.g.: CDS account holders in dealings with Bursa Depository for Malaysian securities (e.g.: stock listed on Bursa Malaysia) and other regulatory bodies). | • To implement or undertake corporate actions such as dividend payments, general meetings (e.g. processing of proxy forms);<br><br>• To respond and deal with enquiries/ feedback and for other shareholder or investor. |
| (e) | Third parties Including contracting parties | • When an individual interacts with the employees and officers of the Company, for example, via telephone calls, correspondence and face-to-face meetings (including at shareholder meetings);<br><br>• When an individual visits the Company's premises where CCTV may be deployed for security purposes;<br><br>• When a party transacts or contracts with the | • To respond, deal with, manage and/or for other legitimate purposes for the business and operations of the Group. |

| | | | |
|---|---|---|---|
| | | Company, it may provide Personal Data of its directors and employees;<br><br>• When an individual approach, sign, subscribe, engage, transact and/or dealing with the Company. | |

5.2 The Group collects Personal Data primarily from the persons identified in the table set out above. Unless permitted by laws, the collection, use and/or disclosure of Personal Data should be limited to that which is necessary for the identified purposes in the table above.

## 6. PERSONAL BEHAVIOUR AND CONDUCT IN GLB

6.1 Before collecting, using or disclosing Personal Data, the consent of the individual consent must be obtained. There are two types of consent:

(a) actual consent; and
(b) deemed consent under the PDPA.

Generally, the Company should seek **actual consent**. When seeking consent, the purpose for which the consent is sought must be notified to the individual.

6.2 The Company may collect, use or disclose an individual's Personal Data without his/her consent in the following circumstances:

(a) the collection, use or disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;
(b) the Personal Data is publicly available;
(c) the collection, use or disclosure is necessary for any purpose which is clearly in the interests of the individual, if consent for its collection, use or disclosure cannot be obtained in a timely way;
(d) the collection, use or disclosure is necessary for any investigation or proceedings;
(e) the collection, use or disclosure is necessary for evaluative purposes; and/or
(f) in any other circumstances set out in the PDPA.

## 7. WITHDRAWAL OF CONSENT / CORRECTION AND ACCESS TO PERSONAL DATA

7.1 An individual who has provided the Company with Personal Data is entitled under the PDPA to withdraw his/her consent, request for corrections to be made and for access to such Personal Data. In such cases, the Company must comply with the following:

| Circumstance | |
|---|---|
| Withdrawal of Consent | An individual is entitled at any time to withdraw his/her consent to the continued collection, use and disclosure of the Personal Data. Such withdrawal shall be made formally in writing to the office of the DPO. The Company must not prohibit an individual from withdrawing his/her consent. |
| Correction of Personal Data | Upon request by the individual concerned, the Company must, in accordance with the PDPA, correct or complete any Personal Data found to be inaccurate or incomplete as soon as practicable unless the Company is satisfied that on reasonable grounds that the correction should not be made. |
| Access to Personal Data | Upon request by an individual, the Company is required under the PDPA to provide the individual with:<br>(a) his/her Personal Data which is in the possession or under the control of the Company; and<br>(b) information about the ways in which the Personal Data has been or may have been used or disclosed during the past 1 year. Such request shall be made in accordance with the practices set out in the PDP Internal Practices.<br><br>There are some exceptions to the obligation to provide the above. Please see the PDP Internal Practices (para 4(a)). |

## 8. RETENTION PROTECTION AND DISPOSAL OF PERSONAL DATA

The PDPA regulates how Personal Data in the Company's possession is to be protected or dealt with. Some of the basic obligations and the corresponding required practices and policies of the Company are set out below and must be complied with at all times:

| Action | Policies/Practices |
|---|---|
| Protection of Personal Data | The Company shall protect Personal Data in its possession or under its control against risk of unauthorised access, collection, use, disclosure, copying, modification or disposal through reasonable security measures. These measures are dealt with in the PDP Internal Practices. |
| Retention and Disposal of Personal Data | The Company must cease to retain documents containing Personal Data or remove the means by which the Personal Data can be associated with particular individuals as soon as it is reasonable to assume that: (i) the purpose for which the Personal Data was collected is no longer being served by the retention of such Personal Data; and (ii) retention is no longer necessary for legal or business purposes. In such event, the Company must ensure that the Personal Data is |

| | |
|---|---|
| | properly disposed of in accordance with the PDP Internal Practices. |
| Transfer of Personal Data | The Company shall not transfer any Personal Data of an individual to a recipient outside Malaysia unless the standard of protection to Personal Data in the foreign country is comparable to the protection under the PDPA. |

## 9. POWERS OF PDPC AND CONSEQUENCES OF NON-COMPLIANCE WITH PDPA

9.1 The Personal Data Protection Commission ("**PDPC**") may, upon receiving a complaint or of its own motion, conduct an investigation to determine whether an organisation is in compliance with the PDPA. For the purposes of an investigation, the PDPC's powers include, amongst others, requiring documents or information which relates to any matter relevant to the investigation to be produced by the organisation.

9.2 It is important for the Company to ensure that its employees comply with the requirements of the PDPA as non-compliance can affect the Company. It is to be noted that enforcement decisions of the PDPC are made public, and the PDPC may issue warnings to the organisation. Amongst others, the PDPC may:

(a) if it is satisfied that an organisation is in breach, impose a financial penalty of up to RM500,000.00 and/or jail imprisonment up to 3 years;
(b) give directions for the destruction of Personal Data collected or for that the organisation ceases to collect or use Personal Data in breach of the PDPA;
(c) review any complaint by an individual against an organisation for refusal to provide access to his/her Personal Data; and
(d) give such directions as it thinks fit to ensure compliance with the PDPA.

## 10. GENERAL

10.1 If you are in any doubt or unclear as to the policies or practices set out in this Policy, please contact the DPO for assistance.

10.2 GLB may revise or amend or supplement this Policy or PDP Internal Practices at its discretion from time to time. Employees of the Company are encouraged to check periodically to ensure that they are aware of any such changes.

10.3 Further information on the PDPA can be found at https://www.pdp.gov.my/.

++++++++++++++++++End++++++++++++++++++

## ANNEXURE A – PDP INTERNAL PRACTICES

### 1. DATA PROTECTION OFFICER(S)

The department or office of the DPO has been set up to oversee the Group's compliance with the PDPA. Other employees within the Group may be delegated to act on behalf of the DPO or to take responsibility for the day-to-day collection and processing of Personal Data. The DPO may be contacted at:

**Golden Land Berhad**
A-09-03, Empire Tower
Empire Subang
Jalan SS16/1, 47500 Subang Jaya
Selangor Darul Ehsan.

**Attention: Ms. Lai Wern Ching, Legal Manager**

Tel: 03-5611 8844
Email: lai.wernching@glbhd.com

### 2. CONSENT FOR COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

(a) Employee must OBTAIN THE CONSENT of an individual BEFORE the: (i) collection; (ii) use; and/or (iii) disclosure of an individual's Personal Data.

(b) All consents must be obtained IN WRITING. This is to mitigate against disputes.

(c) When seeking such consent, employee must:

(i) notify the individual IN WRITING of the PURPOSE(S) for which the Company intends to collect, use or disclose his/her Personal Data. The purpose should be clearly set out.

(ii) obtain the individual's WRITTEN confirmation that the Personal Data provided is accurate and complete.

(d) If consent is obtained, the Personal Data must only be collected, used or disclosed by the Company for the purposes for which the consent was obtained, and not for any other purpose.

(e) The individual is entitled to WITHDRAW CONSENT given, on giving reasonable notice to the Company. In such event:

(i) Employee should direct the individual to submit their notice of withdrawal in writing to the DPO;

(ii) On receipt of withdrawal notice, the DPO shall inform the individual of the likely consequences of withdrawing the consent; and

(iii) Upon withdrawal, the Company MUST CEASE to collect, use or disclose the Personal Data of such individual (as the case may be).

## 3. PROTECTION, RETENTION AND DISPOSAL OF PERSONAL DATA

(a) Employee must keep all documents containing any Personal Data and confidential
information secure and locked at all times.

(b) Employee must activate the self-locking mechanism for his/her computer if the computer is left unattended for a certain period.

(c) Employee must encrypt all electronic documents containing Personal Data.

(d) Documents containing Personal Data should be removed or disposed of once the purposes for which the Personal Data was collected are no longer being served by the retention of the Personal Data and the retention is no longer necessary for legal or business purposes.

(e) Recycling of paper is encouraged but employee shall ensure that papers or documents containing Personal Data are SHREDDED BEFORE recycling.

(f) Employee must delete the electronic files containing Personal Data PRIOR to the disposal of IT devices in which the Personal Data was kept or stored.

(g) Copying of Personal Data to removable storage devices or transmitting such data via email is strictly prohibited unless prior approval of the DPO is obtained.

## 4. ACCESS TO, CORRECTION AND ACCURACY OF PERSONAL DATA

(a) Upon request by an individual, the Company must provide him/her with:

(i) his/her Personal Data which is in the possession or under the control of the Company; and

(ii) information about the ways in which the Personal Data has been or may have been used or disclosed during the past 1 year.

There are some **exceptions** to the above obligations:

- opinion data kept solely for an evaluative purpose;
- Personal Data which is subject to legal privilege;
- Personal Data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation; or
- any request for information that does not exist or cannot be found.

Personal Data and information must NOT be provided where it could be reasonably be expected to:

- threaten the safety or physical or mental health of an individual, other than the individual who made the request;
- cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request; or
- reveal Personal Data about another individual.

(b) To assess the information set out above in 4(a), individual is required to submit his/her request.

*Note: When processing an access request, it is important for employee to establish and verify the identity of the individual making the request.*

(c) In order to comply with an access request made by an individual as set out above in 4(a)(ii), employee who is managing or handling the relevant Personal Data must maintain a disclosure list.

(d) An individual is entitled to request that an error in his/her Personal Data be corrected. Upon receipt of such a request, employee shall correct the Personal Data as soon as practicable and send the corrected personal data to every other organisation to which the Personal Data was disclosed by the Company within 1 year before the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

(e) Employee should make reasonable efforts to ensure that Personal Data collected from an individual is correct, accurate and complete. This should be done at the stage when consent is first obtained or when the correction to the Personal Data is made.

## 5. TRANSFER OF PERSONAL DATA

Employee transferring Personal Data of an individual to a recipient outside Malaysia must ascertain and ensure that the recipient is bound by legally enforceable obligations that provide a standard of protection to the Personal Data that is comparable to the protection under the PDPA. If in doubt, please check with the DPO.

Legally enforceable obligations include any law, contracts, binding corporate rules or any other legally binding instrument.

## 6. DATA BREACHES

(a) Data breaches can occur for various reasons. These may be caused by employees, external parties or computer system errors. The following are some possible ways in which a data breach may occur. The list is not meant to be exhaustive.

| | |
|---|---|
| Malicious activities | • Hacking incidents/ illegal access to databases containing Personal Data<br>• Theft of computer notebooks, data storage devices or paper records containing Personal Data<br>• Scams that trick organisations into releasing Personal Data of individuals |
| Human error | • Loss of computer notebooks, data storage devices or paper records containing Personal Data<br>• Sending Personal Data to a wrong e-mail or physical address, or disclosing data to a wrong recipient<br>• Unauthorised access or disclosure of Personal Data by employee<br>• Mistakes in the printing process which may lead to the exposure of Personal Data<br>• Improper disposal of Personal Data (e.g. hard disk, storage media or paper documents sold or discarded before Personal Data is properly deleted) |
| Computer system error | • Errors or bugs in the programming code of websites, databases and other software which may be exploited to gain access to Personal Data stored on computer systems |

(b) When data breach occurs or is likely to occur, employee must comply with the following:

| | |
|---|---|
| Containing the breach | Where applicable,<br>• Notify IT Department immediately<br>• Shut down and isolate the compromised system that lead to the data breach<br>• IT Department shall establish whether steps can be taken to recover lost data and limit any damage caused by the breach<br>• Reset password<br>• Address lapses in processes that led to the data breach<br>• Put a stop to practices that led to the data breach |

| | |
|---|---|
| Reporting the incident | • Employee and IT Department to immediately report matter to DPO with details on how and when the data breach occurred, types of Personal Data involved in the data breach<br><br>• DPO to report to the management of the Company to consider whether to notify the police if criminal activity is suspected and preserve evidence for investigation<br><br>• DPO to notify the affected individuals and/or PDPC taking into account the prevailing PDPC's guidelines |

## 7. COMPLAINT HANDLING PROCESS

| Stages | Steps to be taken | Person In Charge |
|---|---|---|
| Initial handling of complaints | Upon receipt of a complaint,<br><br>• Employee must inform the DPO of all information relating to the complaint<br><br>• Employee or (where appropriate) DPO to send an acknowledgement reply to the complainant<br><br>• A data protection complaint register will be maintained by the DPO to keep track of the status of the complaint DPO/ Employee | DPO/Employee |
| Assessing the complaints | • DPO to follow up and assess the validity of the complaint<br><br>• If the complaint is valid, to determine which data protection provisions has the Company not complied with, and to assess the impact and severity of the complaint<br><br>• Assess the timeframe needed to achieve closure for the complaint and inform complainant accordingly | DPO (or such person delegated to act on behalf of the DPO) |
| Investigating/ Reporting the complaints | • Determine what caused the non-compliance to take place, who were involve, how and why it happened<br><br>• Provide interim updates to the complainant and find out from the complainant how he/she might want his/her complaint to be resolved | |

| | | |
|---|---|---|
| | • Submit investigation report to appropriate level of management of the Company, including findings made and recommendations on remedial actions to be taken to achieve resolution of the complaint<br><br>• If need be, report to inform the relevant authorities such as police and PDPC | |
| Responding to complaints | • Inform complainant about the results of the investigation and the remedial actions to be taken<br>• If complainant disagrees with the remedial actions, this could be escalated to the management of the Company or independent third party for resolution | |
| Taking corrective actions | • Analyse current and past complaints to determine if there are systemic issues that might cause such complaints to be lodged in the first place<br><br>• Once these systemic issues are identified, recommend specific actions such as fine-tuning of specific data protection policies and processes and employee's training to prevent future recurrences | |