Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

# Generali Life Assurance (Thailand) Plc.

# PERSONAL DATA PROTECTION POLICY

Compliance Function

**LOCAL POLICY**

*For internal purposes only*

generali.co.th

| Approved by Board of Directors of Generali Life Assurance (Thailand) Plc. | |
|---|---|
| Meeting No./Year | 01/2025 |
| Date of Meeting | 31 March 2025 |
| Signed by | DocuSigned by: E7CED1F428C44F1... Mr. Arsh Kaumi (Chief Executive Officer) |

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

## Control Version

| Version | Date of issuance | Document code | Reason of Changes |
|---|---|---|---|
| 3 | 2025-03-31 | GTL-2025/023 | Amended the requirements to comply with Thailand Personal Data Protection Laws and the practices of Thai Businesses on followings points<br>- Amended Roles and Responsibility of the Data Controller and the Data Processor.<br>- Added the new roles “Data Protection Committee”<br>- Amended criteria to perform the DPIA.<br>- Added the new data subject right.<br>- Amended the conditions of data transfers outside Thailand and more. |
| 2 | 2023-03-29 | GTL-2023/013 | Added definition of “Privacy Notice.”<br>Revised the relevant Function to be aligned with current organization. |
| 1 | 2020-03-27 | GTL-2020/022 | Initial version to be complied with PDPA enforcement. |

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

## EXECUTIVE SUMMARY

The Personal Data Protection Policy (hereinafter "the Policy") is aimed at supporting the implementation of the Personal Data Protection Act B.E.2562 ("PDPA") sets the minimum requirements that Generali Life Assurance (Thailand) Plc. (hereinafter "GTL") must implement when Processing Personal Data. To this purpose, the Policy provides:

- the principles that must inspire the Processing of Personal Data (→ 3);
- the requirements to be implemented whenever acting as Data Controller, Data Processor or Joint Controller in respect of specific Personal Data Processing (→4);
- the role and the responsibilities of the Data Protection Officer (→ 5);
- the rules for the identification of the Lead Data Protection Supervisory Authority (→ 6);
- the cooperation with Data Protection Supervisory Authority (→ 7);
- the roles and the responsibilities defined in the Policy (→ 8).

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

# INDEX

**1 Glossary and Definitions ..... 3**

**2 Introduction ..... 4**

2.1 Objectives 4
2.2 Approval and Review 4
2.3 Effective Date 4

**3 Key Principles governing Personal Data Processing ..... 5**

**4 Key Requirements ..... 5**

4.1 KEY REQUIREMENTS FOR THE DATA CONTROLLER 5
4.2 KEY REQUIREMENTS FOR THE DATA PROCESSOR 10
4.3 KEY REQUIREMENTS FOR JOINT CONTROLLERS 10

**5 Data Protection Officer ..... 10**

5.1 APPOINTMENT OF THE DPO 10
5.2 FIT & PROPER REQUIREMENTS 10
5.3 RESPONSIBILITIES OF THE DPO 11

**6 Cooperation with Data Protection Supervisory Authority ..... 11**

**7 Roles and Responsibilities ..... 11**

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

# 1 Glossary and Definitions

| Acronym/Term | Explanation/Definition |
|---|---|
| Data Controller | The natural or legal person that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. |
| Date of Issuance | Date on the Policy is approved. |
| Effective Date | Date on the Policy must be effective. |
| Data Processing (or Processing) | Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| Data Processor | The natural or legal person that processes the Personal Data on behalf of the Data Controller. |
| Data Protection Impact Assessment (or DPIA) | An assessment of the impact of the envisaged Processing operations on the protection of Personal Data. It must be carried out by the Data Controller when a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of the Processing and the use of new technologies. |
| Data Protection Officer (or DPO) | The Data Protection Officer is the role described under section 5. |
| Data Subject | An identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| Generali Group (or Group) | The Generali Group whose ultimate parent Company is Assicurazioni Generali S.p.A. |
| Joint Controllers | Two or more Data Controllers that jointly determine the purposes and means of the Processing of Personal Data. |
| Joint Venture | Legal Entities established on the basis of specific shareholder agreements defined with partners. |
| Personal Data | Any information directly or indirectly relating to an identified or identifiable natural person (i.e., Data Subject). |
| Personal Data Breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. |
| Privacy Notice | Statement provided to the Data Subject with the aim of explaining how and for what purposes the Personal Data collected by the Group Legal Entity will be used. |
| Sensitive Personal Data | Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, Personal Data concerning health or concerning a natural person's sex life or sexual orientation. |
| Supervisory Authority (or Data Protection Supervisory Authority) | Personal Data Protection Commissioner or Personal Data Protection Committee. |

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

# 2 Introduction

## 2.1 OBJECTIVES

GTL the safeguarding of Personal Data as a priority to protect the fundamental rights and freedoms of customers, employees and all other stakeholders.

The purpose of the Personal Data Protection Policy is to set the key principles and requirements to be followed when Processing Personal Data, in compliance with the provisions of the Personal Data Protection Act, any personal data protection laws related thereto ("Personal Data Protection Laws")

This Policy also defines the key roles to be involved to manage the risks associated with the Processing of Personal Data.

## 2.2 APPROVAL AND REVIEW

The Policy was approved by the GTL Board of Directors ("BoD").

It shall be promptly reviewed, and in any case at least every three years to include developments in legislation, market and/or best practices. GTL strategy and organisation.

## 2.3 EFFECTIVE DATE

The Policy is effective as of 31 March 2025 and shall be immediately implemented.

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

# 3 Key Principles governing Personal Data Processing

The following key principles must always be applied to Personal Data Processing:

- **lawfulness**, **fairness** and **transparency**:
  - *lawfulness* → Processing is lawful if it is based on one of the valid grounds (please refer to par. 4.1.1 below for further information).
  - *Fairness* → "common sense" principle which requires that the Processing must not be carried out in a way that might be misleading, detrimental or unexpected for the Data Subject.
  - *Transparency* → The Data Subject must be provided with information about the Processing (i.e., a proper Privacy Notice; please refer to par. 4.1.2 below for further information).
- **Purpose limitation**: Personal Data should be collected and processed only for specified, explicit and legitimate purposes, as described in the Privacy Notice. Further Processing, incompatible with those purposes, is not allowed.
- **Minimization**: process only Personal Data that are adequate, relevant and limited to what is necessary in relation to the purposes described in the Privacy Notice provided to the Data Subject.
- **Accuracy**: do not process inaccurate Personal Data and, where necessary, keep them updated; when the inaccuracy of Personal Data is discovered, in respect of the purposes for which they are processed, GTL must take reasonable steps to correct or erase them without delay.
- **Storage limitation**: keep Personal Data for no longer than necessary for the purposes for which they are processed; define a retention period (i.e., how long a particular type of personal data can be stored for a particular purpose). The duration of the retention period is set on the basis of the purposes of the Processing to the extent that it does not conflict with other applicable laws and regulations.
- **Integrity and confidentiality**: ensure that appropriate organizational and technical measures are in place to protect Personal Data, so to avoid unauthorized or unlawful Processing, accidental loss, destruction or damage. Such measures are always necessary whenever Personal Data are being processed; however, in certain specific cases (i.e., when the related risk is higher), a higher standard may apply.
- **Accountability**: the Data Controller is responsible for the compliance with the principles above and must be able to demonstrate at all times through the adoption of appropriate internal regulations, processes, and other measures which include, at least: i) the keeping of a record of Processing activities (see par. 4.1.5 below), ii) the performance of a DPIA (see par. 4.1.8 below), iii) the performance of controls to verify the status of implementation of the Personal Data protection principles and requirements.

# 4 Key Requirements

Considering the above principles, different key requirements need to be implemented depending on whether Personal Data are being processed by GTL acting as Data Controller, as Data Processor or as Joint Controller. The Data Controller and the Data Processor must provide the personnel who process Personal Data with appropriate instructions and training in order to ensure that Personal Data are processed in compliance with this Policy and the personal data protection laws.

## 4.1 KEY REQUIREMENTS FOR THE DATA CONTROLLER

Whenever, as regards to a specific Processing of Personal Data, GTL act as Data Controller, the activities listed under this section must be carried out. The Data Controller must ensure that the Data Protection Officer, where appointed, is involved, properly and in a timely manner (from the earliest stage possible), in all issues which relate to the protection of Personal Data.

### 4.1.1 Process Personal Data based on lawful grounds

The Data Controller must identify the lawful basis of each Data Processing and before the Data Processing is initiated.

The identification of the correct lawful basis depends on the purpose and the nature of the relationship with the Data Subjects concerned (i.e. employees, customers, other stakeholders) and the nature of Personal Data, in particular whether Sensitive Personal Data are processed.

Processing of Personal Data is lawful when it is:

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

- based on consent given by the Data Subject for one or more specific purposes; or
- necessary for the performance of: (i) a contract to which the Data Subject is party or (ii) pre-contractual activities after the request of the Data Subject; or
- necessary for compliance with a legal obligation, to which the Data Controller is subject; or
- necessary for the purposes of a legitimate interest pursued by the Data Controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data. To assess that such interests aren't overridden by the interests or fundamental rights and freedoms of the Data Subject whose data are processed it's necessary perform a Legitimate Interest Assessment (LIA).

Save in exceptional cases where strictly required for the provision of their services, GTL shall refrain from using the following two further legal grounds to process personal data:

- necessary to protect the vital interests of the Data Subject or of another natural person; or
- necessary for the performance of a task carried out in the public interest or in the exercise of an official authority.

Processing of Sensitive Personal Data is prohibited, except when one of the following applies:

- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by applicable law.
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
- Processing relates to Personal Data which are manifestly made public with explicit consent from the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of applicable laws and regulations or pursuant to contract with a health professional and subject to the following conditions and safeguards referred: those Personal Data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under applicable laws and regulations or by another person also subject to an obligation of secrecy under applicable laws and regulations.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- Performed in accordance with applicable laws and regulations, including further conditions and limitations with regard to the processing of Sensitive Personal Data.

### 4.1.2 Provide the Data Subjects with the proper information related to the Processing of Personal Data

The Data Controller must provide (free of charge) Data Subjects with adequate and clear information in the Privacy Notice relating to the Processing of their Personal Data. This information shall also include, if applicable, the existence of automated decision-making (e.g., profiling) and meaningful information about the logic involved, as well as the significance and the envisaged consequences for the Data Subject.

The Privacy Notice shall be concise, transparent, easily accessible and intelligible. It shall be written in an easily understandable form, using clear and plain language.

The Data Controller, prior to implementing or rolling-out a new Privacy Notice, or amending an existing one, must consult the relevant DPO on the proposed new or modified Privacy Notice prior to its finalization. The DPO must check that its content is accurate and corresponds to the information contained in the Record of Processing Activities and that all the relevant Personal Data Processing activities undertaken by GTL are included.

### 4.1.3 Facilitate the exercise of Data Subjects' rights

As a rule, and subject to certain circumstances defined by the applicable regulations, the Data Controller must allow each Data Subject to exercise the following rights:

a) **Right of access**: right to obtain confirmation as to whether or not Data Subjects' Personal Data are being processed and, where that is the case, access to the Personal Data without undue delay.
b) **Right to rectification**: right to obtain, without undue delay, the rectification of inaccurate Personal Data or the completion of incomplete Personal Data.
c) **Right to erasure (right to be forgotten)**: right to obtain the deletion of Data Subjects' Personal Data from wherever they are stored without undue delay.
d) **Right to restriction**: right to obtain the limitation of the Processing activities on Data Subjects' Personal Data. Once restricted, Personal Data can only be stored, unless specific exemptions apply.

e) **Right to portability**: right of the Data Subjects to receive their Personal Data in a structured, commonly used, and machine-readable format and have those Personal Data transmitted to another Data Controller (if a direct transfer is technically possible).
f) **Right to object**: the right to oppose, on grounds relating to their specific situation, at any time to the Processing of Data Subjects' Personal Data. Once the right to object has been exercised, Personal Data must no longer be processed unless the existence of legitimate grounds that override the interests, rights and freedom of the Data Subjects, or the need to establish, exercise or defend legal claims is demonstrated. In any case, if the Data Subjects objects to Processing for direct marketing purposes, Personal Data must no longer be processed for such purposes.
g) **Right to be informed**: right to be informed ensures that data subjects are aware of how their personal data is being collected, used, and disclosed.
h) **Right to withdraw consent**: right to withdraw consent for the processing of personal data at any time.
i) **Right to lodge the complaint:** right to file complaints to the Supervisory Authority in the event of the violation.

In particular, the Data Controller must:

- define processes to allow the easy exercise of Data Subjects' rights and to promptly take any subsequent actions;
- provide Data Subjects with information on any actions taken;
- make Data Subjects aware of the modalities for exercising such rights.

Unless exceptional circumstances occur, all actions and communications to the Data Subjects must be free of charge for the Data Subjects.

### 4.1.4 Privacy by Design and by Default

The Data Controller must ensure that Personal Data protection is granted by design and by default.

The Data Controller must identify and implement appropriate technical and organizational measures in order to meet the requirements of the data protection laws and protect the rights and freedoms of Data Subjects; such activity must be performed at the time of the determination of the means and purpose of any system, service, product or process and at the time of the Processing itself, in order to comply with privacy and data protection principles right from the start (**privacy by design**).

For the identification of the appropriate technical and organizational measures, the Data Controller must take into consideration at least the following:

- the technical and technological solutions available on the market at the time,
- the cost of implementation,
- the nature, scope, context and purposes of the Personal Data Processing,
- the impacts of the Personal Data Processing on the rights and freedoms of the Data Subjects.

By default, the Data Controller must ensure that Personal Data are processed with the highest privacy protection, meaning that appropriate technical and organizational measures must be implemented in order to ensure that only Personal Data which are necessary for each specific purpose of the Processing are processed, the same with reference to the amount of Personal Data collected, the extent of their Processing, their retention period and their accessibility (**privacy by default**).

GTL must apply the IT and physical security measures.

### 4.1.5 Keep records of the Personal Data Processing activities performed under its responsibilities

The Data Controller must keep a **Record of Processing Activities** ("RoPA") under its responsibility, which is a document with inventory and analysis purposes that must reflect the reality of the Personal Data processing carried out by the Data Controller or Data Processor and allows to identify, among others:

- the actors involved (controller, processors, representative, joint controller, etc.);
- the categories of data processed;
- the purpose of the processing, who has access and who are the recipients of the personal data;
- for how long Personal Data are retained;
- the technical and organizational measures implemented.

The RoPA shall be made available to the Supervisory Authorities on request.

Also, the Data Processor shall maintain a record of all categories of processing activities carried out on behalf of a Data Controller.

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

### 4.1.6 Implement adequate technical and organizational measures to ensure a level of security appropriate to the risk

The Data Controller must implement adequate technical and organizational measures to ensure an adequate level of security of Personal Data.

A risk-based approach must be followed when identifying these measures. The risk-based approach must consider, among others, the state of the art of technologies, the nature, scope, context and purpose of the Processing and the likelihood and severity of the risks on rights and freedoms of Data Subjects posed by the Processing.

Without prejudice to the involvement of any other functions in relation to their area of responsibility, the Data Controller shall follow the "privacy by design and by default" approach (please refer to the above par. 4.1.4) and implement the appropriate technical and organizational measures, asking for the DPO's advice on such measures when appropriate.

### 4.1.7 Notify to the supervisory authority and communicate to the Data Subjects a Personal Data Breach

The Data Controller must implement an adequate process in order to ensure the proper management of Personal Data Breaches.

The process must:

- include the involvement of the DPO;
- define how to detect and promptly circumstantiate a Personal Data Breach;
- indicate a methodology to assess the risk to individuals;
- give guidance to determine whether it is necessary to notify the competent Data Protection Supervisory Authority (not later than 72 hours after having become aware of the Breach) and to communicate the Breach to the Data Subjects concerned.

Personal Data Breaches must be managed following the principles and provisions set out in the internal regulation governing the management of Personal Data Breaches.

### 4.1.8 Carry out an assessment of the Processing impact on the protection of Personal Data (Data Protection Impact Assessment – DPIA)

When the processing of personal data in new initiatives, project, or enhancements to existing system/processes meets certain criteria defined by DPIA framework, the Data Controller shall, prior to the processing, carry out a DPIA, which is an important assessment to demonstrate that appropriate measures have been taken to ensure compliance with the personal data protection laws. The Data Controller shall ask the advice of the Data Protection Officer, when carrying out a Data Protection Impact Assessment.

### 4.1.9 Adopt adequate safeguards and additional measures for transfers of Personal Data outside Thailand

The Data Controller must ensure that any transfer of Personal Data outside Thailand is performed only if necessary and after having adopted at least one of the recommended safeguards and the supplementary measures appropriate to ensure that the Personal Data transferred receive, in the foreign country, a level of protection essentially equivalent to the one provided in Thailand.

Transfers of Personal Data outside Thailand may take place on the basis of an adequacy decision of the Personal Data Protection Committee assessing that the foreign country ensures an adequate level of Personal Data protection.

In the absence of an adequacy decision, the transfer may take place on the basis of appropriate safeguards are:

- Standard Contractual Clauses ("SCCs") adopted by Personal Data Protection Commissioner, ASEAN Model Contractual Clause, or the contractual clause for the transfer of personal data to third parties in the General Data Protection Regulation ("GDPR"), which must be executed and can be complied with foreign country.
- standard data protection certification for collecting, using, and disclosing of the data controller or the data processor that relates to cross-border transfers ensuring that appropriate personal data protection safeguards are in place, in accordance with accepted standards
- Binding Corporate Rules ("BCRs"), which are approved by the Personal Data Protection Committee and help ensure an adequate level of protection for Personal Data exchanged within a group of companies located both inside and outside Thailand,

When the transfer to foreign country is based on an appropriate safeguard the Data Controller has to assess whether they are effective in light of all circumstances of the transfer and, if not, the Data Controller must adopt additional measures (e.g. encryption in transit and at rest, end-to-end encryption, anonymization, pseudonymization) to ensure that the Personal Data transferred are

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

afforded in the third country a level of protection essentially equivalent to that guaranteed in the Thailand.

In the absence of either an adequacy decision or appropriate safeguards, transfers of Personal Data to a non-adequate Country are allowed where one of the following conditions is applicable:

- the Data Subject has explicitly consented to the proposed transfer; or
- the transfer is necessary for the performance of a contract between the Data Controller and the Data Subject or for the implementation of pre-contractual measures taken at the Data Subject's request; or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person; or
- the transfer is necessary for important reasons of public interest; or
- the transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent;

As a residual case, where no adequacy decisions, derogations or appropriate safeguards are applicable, Personal Data can be transferred to foreign country only if the following points are met:

- the transfer is not repetitive, concerns only a limited number of Data Subjects and is necessary for the purposes of compelling legitimate interests pursued by the Data Controller which are not overridden by the interests or rights and freedoms of the Data Subject.
- all the circumstances surrounding the transfer have been assessed and based on that assessment, suitable safeguards with regard to the protection of Personal Data have been implemented.
- the relevant Supervisory Authority of the transfer and the Data Subjects have been preliminary informed.

If none of the above options is feasible (including if no additional measure appears to be effective to ensure that the Personal Data transferred receive, in foreign country, a level of protection essentially equivalent to the one provided within Thailand), or whenever in doubt, the Data Controller must refrain from transferring Personal Data.

The Personal Data transfer provisions apply to transfers of Personal Data within the Generali Group and outside the Generali Group (e.g., to suppliers, vendors).

### 4.1.10 Data Processors

When the Data Controller delegates the Data Processing to a third party (outside or within the Generali Group), the Data Controller must appoint a Data Processor in writing form. The appointment must be formalised also when it occurs in the context of an outsourcing agreement, in accordance with the Third Parties Management and Outsourcing Policy.

Before a Data Processor is appointed, the Data Controller must ensure that the Data Processor has in place appropriate technical and organizational measures capable to grant the compliance with the Personal Data principles and requirements as well as the exercise of Data Subjects' rights. The Data Controller must authorize any appointment by the Data Processors of sub-Data Processors. The prior written authorization can be general or specific.

In case an authorized sub-Data Processor processes Personal Data outside Thailand, the Data Controller shall verify that the Data Processor assesses and implements appropriate safeguards to guarantee a level of protection essentially equivalent

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

## 4.2 KEY REQUIREMENTS FOR THE DATA PROCESSOR

Whenever, as regards to a specific Processing of Personal Data, GTL acts as **Data Processor**, it must:

- process the Personal Data in accordance with the principles set out under par. 3 of this Policy, the applicable Personal Data protection laws and regulations and only according to the documented instructions of the Data Controller, unless otherwise required by the applicable laws.
- Ensure that persons authorized to process the Personal Data have committed to confidentiality or are under an appropriate obligation of confidentiality.
- Maintain a record of the RoPA, with a dedicated record for each Data Controller on behalf of which is acting.

## 4.3 KEY REQUIREMENTS FOR JOINT CONTROLLERS

When two or more Data Controllers act as Joint Controllers (either within the Generali Group or outside the Generali Group), GTL that will become part of the joint controllership agreement, before its execution, must:

- assess that all the other Joint Controller(s) have in place appropriate technical and organizational measures to ensure compliance with the applicable Personal Data internal and external regulation.
- Draft a contractual arrangement that, as minimum, determines the respective responsibilities for compliance with the Personal Data Protection regulation, particularly in respect of:
    - primary responsibility for complying with internal and external applicable regulation;
    - purpose and duration of processing
    - transparency obligations;
    - individuals' rights, DPIA, records and Personal Data Breach management;
    - contact point for Data Subjects;
    - Personal Data transfers (if any).
    - Security measures

The arrangement must be formalized in writing and the essence shall be made available to Data Subjects.

# 5 Data Protection Officer

## 5.1 APPOINTMENT OF THE DPO

Whenever acting as Data Controller or Data Processor or Joint Controller, GTL must appoint a Data Protection Officer at least when they perform the following activities:

- The activities of the Data Controller or the Data Processor in the collection, use, or disclosure of the Personal Data require a regular monitoring of the personal data or the system, by the reason of having a large number of personal data as prescribed and announced by the Supervisory Authority.
- The core activity of the Data Controller or the Data Processor is the collection, use, or disclosure of the sensitive personal data.

The appointment of the DPO is made by the BoD and must be incorporated in the minutes of the relevant meeting. GTL must publish and communicate to the relevant Supervisory Authority the DPO's contact details.

The DPO can be outsourced to other entities or to third parties. Also, the DPO may be able to perform other duties or tasks but the Data Controller or the Data Processor must warrant to the Supervisory Authority that such duties or tasks are not against or contrary to the performance of the duties.

The DPO must report to the BoD.

## 5.2 FIT & PROPER REQUIREMENTS

The DPO must possess an expert knowledge of:

- the Data protection laws and practices,
- the Personal Data Processing operations carried out by GTL,
- the administrative rules and procedures of the GTL,
- the business sector in which the relevant GTL operates.

A higher level of expertise may be requested if the activities performed by GTL is particularly complex or involve a large amount of Personal Data or the latter are systematically transferred outside Thailand.

The Fit & Proper Policy applies.

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

### 5.3 RESPONSIBILITIES OF THE DPO

The Data Protection Officer of the GTL plays a key role in fostering the implementation of the applicable laws and regulations on Personal Data protection and in facilitating the compliance with them, even if it is the responsibility of the Data Controller to act and demonstrate that each specific Processing operation is carried out in accordance with the applicable provisions.

The DPO is in charge to:

- Ensure that adequate internal regulations on personal data protection topic are adopted.
- Inform and advise the BoD, Senior Management and personnel of their obligations related to the Processing of Personal Data pursuant to the Personal Data protection laws and regulations.
- Design personal data protection training content and ensure, in collaboration with the other GTL's functions responsible for training, its delivery.
- Monitor compliance with data protection laws, other local applicable laws and regulations and the internal policies in relation to the protection of Personal Data, including assignment of responsibilities, awareness and training initiatives of staff involved in Processing operations, and perform controls on their implementation.
- Provide advice, where requested, as regards the Data Protection Impact Assessment and monitor the implementation of the relevant measures to protect the Data Subjects.
- Act as contact point for the Data Subjects in case, for example, of exercise of rights.
- Act as contact point for the Supervisory Authority on issues relating to the Personal Data Processing.
- Inform the BoD on the activities carried out in the execution of his/her duties, for example, the overall data privacy management program or any regular reports (If any).

The Data Controller or the Data Processor must involve, inform and consult the DPO properly and in a timely manner, to ensure privacy by design approach and compliance with applicable laws and regulations. It must also be informed, without delay. of any potential data breach occurred once detected by any employees.

# 6 Cooperation with Data Protection Supervisory Authority

GTL, acting as Data Controller or Data Processor or Joint Controller, must cooperate, with the Supervisory Authority in the performance of tasks.

# 7 Roles and Responsibilities

| Role | Responsibility |
|---|---|
| BoD | • Appoint the DPO and Data Protection Committee<br>• Approve, validate, or certify data privacy matters as required by personal data protection laws or applicable laws. |
| Data Protection Committee | • Sponsor a data protection culture across GTL and ensure that data privacy is integrated into GTL's strategy and daily routine operations.<br>• Review and verify personal data protection-related policies. Also, monitor compliance with applicable Personal Data Protection Laws.<br>• Monitor and review the major projects, that related to the personal data.<br>• Oversee the handling of privacy incidents and data breaches<br>• Consider and approve activities if potential situations of Conflict of Interest are identified for the DPO.<br>• Support the role and responsibility of DPO in executing his/her responsibilities. |
| Data Controller | • Process Personal Data on the basis of lawful grounds<br>• Provide the Data Subjects with the proper information related to the processing of Personal Data<br>• Facilitate the exercise of Data Subjects' rights<br>• Ensure that Personal Data protection is granted by design and by default<br>• Keep a record of the Personal Data Processing activities performed under its responsibilities and make it ready and available to the Supervisory Authorities on request<br>• Implement adequate technical and organizational measures to ensure a level of security appropriate to the risk<br>• Notify to the supervisory authority and communicate to the Data Subjects a Personal Data breach<br>• Carry out an assessment of the Processing impact on the protection of Personal Data (DPIA)<br>• Adopt adequate safeguards for transfers of Personal Data outside Thailand<br>• Comply with the rules regarding the appointment of Data Processors |

Docusign Envelope ID: 96A5492A-BDD8-48AA-A769-257880266C4B

| Role | Responsibility |
|---|---|
| Data Processor | • Process Personal Data in accordance with the principles of this Policy, the applicable Personal Data protection laws and regulations and the documented instructions of the Data Controller, unless otherwise required by the applicable laws<br>• Ensure that persons authorized to process the Personal Data have committed to confidentiality or are under an appropriate obligation of confidentiality<br>• Maintain a record of the RoPA; with a dedicated record for each Data Controller on behalf of which is acting |
| Joint Controller | • Assess that all the other Joint Controller(s) have in place appropriate technical and organizational measures to ensure compliance with the applicable Personal Data internal and external regulation<br>• Enter into a joint controllership arrangement that, as minimum, determines the respective responsibilities for compliance with the Personal Data Protection law and regulation |
| Data Protection Officer | • Ensure that adequate internal regulations on personal data protection topic are adopted.<br>• Inform and advise the BoD, Senior Management and GTL personnel of their obligations related to the Processing of Personal Data pursuant to the applicable Personal Data protection laws and regulations<br>• Design personal data protection training content and ensure, in collaboration with the other GTL's functions responsible for training, its delivery<br>• Monitor compliance with the applicable Personal Data protection laws and regulations and the internal policies in relation to the protection of Personal Data, including assignment of responsibilities, awareness and training initiatives of staff involved in Processing operations, and perform controls on their implementation<br>• Provide advice, where requested, as regards the DPIA and monitor its performance<br>• Act as contact point for the Data Subjects in case, for example, of exercise of rights<br>• Act as contact point for the Supervisory Authority on issues relating to Personal Data Processing<br>• Inform the BoD on the activities carried out in the execution of his/her duties |