Generali Life Assurance (Thailand) Plc.

PERSONAL DATA PROTECTION POLICY

Compliance Department

Reference No: GTL-CP 2023/013

LOCAL POLICY

For Internal purposes only

www.generali.co.th

Approved by Board of Directors of Generali Life Assurance (Thailand) Plc.	
Meeting No./Year	**02/2023**
Date of Meeting	**29 March 2023**
Signed by	 Mr. Arsh Kaumi (Chief Executive Officer)

Control version

No.	Date of Approval	Ref. No.	Revise and/or summary of reason	Owner
2	29 March 2023	GTL-2023/013	Added definition of "Privacy Notice." Revised the relevant Function to be aligned with current organization.	Compliance
1	27 March 2020	GTL-2020/022	Initial version to be complied with PDPA enforcement	Compliance

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, this policy provides:

- Paragraph 2 deals with the principles that must inspire the Processing of Personal Data;
- Paragraph 3 introduces the key requirements to be implemented in the Personal Data Processing;
- Paragraphs 4 and 5 set the requirements to be implemented whenever acting as Data Controller or Data Processor in respect of specific Personal Data Processing;
- Paragraph 6 sets the requirements to be followed for the appointment of the Data Protection Officer;
- Paragraph 7 sets the rules for the identification of the Lead Data Protection Supervisory Authority.

Glossary and definitions

Acronym/Term	Explanation/Definition
GTL BOD	Board of Directors of Generali Life Assurance (Thailand) Plc.
Data Controller	The natural or legal person that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data 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 to be carried out by the Data Controller when a type of Processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the Processing, is likely to result in a high risk to the rights and freedoms of natural persons.
Data Subject	An identifiable natural person is one 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.
Judicial Data	Personal Data relating to criminal convictions and offences or related security measures relating to a natural person.
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.
Senior Management	The CEO and the Head of those functions that carry out management supervision duties including, at least, the first reporting line of the CEO.
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.

1. Introduction

1.1 Objectives

GTL considers Personal Data as a core asset to be safeguarded. Processing Personal Data according to the best practices is an essential part of the GTL strategies towards customers, employees and all other stakeholders.

The purpose of this Policy is to set the key requirements to be followed when Processing Personal Data keeping into account the provisions of the PDPA.

1.2 Issuers and Approval

The Personal Data Protection Policy (hereinafter "the Policy") has been approved by the Board of Directors of Generali Life Assurance (Thailand) Plc ("GTL BOD") proposal of Compliance Department.

The Data Protection Officer and Chief Compliance Officer are delegated to provide common standards and more detailed guidance in order to support an effective implementation of this Policy.

1.3 Effective Date and review

The Policy is effective as of 29 March 2023.

The Policy shall be reviewed at least every three years and/or any time it will be needed to include developments in legislation, market and/or best practices, GTL strategy and organisation.

2. Key Principles governing Personal Data Processing

When Processing Personal Data, the following principles will be always applied. Personal Data must be:

a) Processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (**"lawfulness, fairness and transparency" principle**). Processing of Personal Data is lawful when Personal Data are processed on the basis of a legitimate ground. The Processing is fair and transparent when Data Subjects are provided with a proper privacy notice at the point of Personal Data collection. The way that is unduly detrimental, unexpected or misleading to the Data Subjects concerned is not allowed;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes (**"purpose limitation" principle**). The purposes for which Personal Data are to be processed must be provided to Data Subjects in a privacy notice provided at the point of Personal Data collection in clear and plain language. Personal Data must be processed only for those reasons indicated to the Data Subjects and must not be processed in a way which is incompatible with those purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**"data minimization" principle**). Only Personal Data strictly necessary to pursue the communicated purposes must be collected and processed;
d) Accurate and, where necessary, kept up to date (**"accuracy" principle**). GTL should keep contact with their Data Subjects and periodically review their Personal Data. Personal Data that are inaccurate, having regard to the purposes for which they are processed, must be erased or rectified without delay;
e) Kept in a form which permits identification of Data Subjects for no longer than necessary for the purposes for which the Personal Data are processed (**"storage limitation" principle**). After having reached the purposes of the Processing, the Personal Data can be retained only in a form which does not permit the identification of the Data Subjects. Measures to de-identify Personal Data include deletion, obfuscation, redaction and anonymization, to the extent that these measures do not conflict with other local applicable laws and regulations;
f) Processed in a manner that ensures appropriate security of the Personal Data, using appropriate technical or organizational measures (**"integrity and confidentiality" principle**). Appropriate security measures to protect the Personal Data must be adopted.

The compliance with the above principles must be easily demonstrated at all times (**"accountability" principle**) through the adoption of appropriate internal regulations, processes and other measures which can include, for example, the keeping of a record of Processing operations (see par. 3.1.5 below), the performance of a DPIA (see par. 3.1.8 below), the performance of controls to verify the status of implementation of the Personal Data protections principles and requirement.

3. 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 or Data Processor.

Both 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 relevant regulations.

Whenever, as regards to a specific Processing of Personal Data, GTL acts 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. Process Key Requirements for the Data Controller

Whenever, as regards to a specific Processing of Personal Data, Group Legal Entities 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 on the basis of 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 special categories of Personal Data are processed.

Processing of Personal Data is lawful when it is:

a) based on consent given by the Data Subject for one or more specific purposes; or

b) necessary for the performance of: (i) a contract to which the Data Subject is party or (ii) pre-contractual activities; or

c) necessary for compliance with a legal obligation to which GTL is subject; or

d) necessary in order to protect the vital interests of the Data Subject or of another natural person; or

e) necessary for the performance of a task carried out in the public interest or in the exercise of an official authority; or

f) necessary for the purposes of a legitimate Interest pursued by GTL, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data.

g) it is for the achievement of the purpose relating to the preparation of the historical documents or for the purpose relating to research or statistics, in which the suitable measures to safeguard the data subject's rights and freedoms are put in place.

4.1.2 Provide the Data Subjects with proper information relating to the Processing of Personal 4.1.3 Facilitate the exercise of Data Subjects' rights

As a general rule and subject to certain circumstances defined by the applicable regulations, 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 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 Data Subjects' 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 data 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;
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 not to be subject to a decision based only on automated processing:** the right of the Data Subject not to be subject to a decision based only on automated processing, including profiling, which produces legal effects concerning him/her or significantly affects him/her.

In particular, the Data Controller must:

- processes to allow the easy exercise of Data Subjects' rights and to promptly take any subsequent actions must be defined;
- Data Subjects must be provided with information on any actions taken;
- Data Subjects must be aware of the modalities for exercising such rights;
- unless exceptional circumstances occur, all actions and communications to Data Subjects must be free of charge for the Data Subjects.

4.1.3 Ensure that Data Protection is granted by design and by default

Appropriate technical and organizational measures to implement the above listed principles and requirements must be adopted in an effective manner.

When new operations or transactions are foreseen, these must be evaluated in a documented manner also from a Personal Data protection perspective in order to ensure that all the appropriate measures are identified and consequently implemented once the operations or the transactions will be executed (**privacy by design**).

Appropriate technical and organizational measures for ensuring that, by default, only Personal Data necessary for each specific purpose of the Processing are processed (**privacy by default**) must be adopted. Privacy by default applies also to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. In particular, such measures shall ensure that, by default, Personal Data are not made accessible without the personnel's intervention to an indefinite number of natural persons.

In particular, whenever developing, designing, selecting and using applications, services and products that imply the Processing of Personal Data, the Data Protection related topics (*e.g.*, the principles listed in par. 2 above) must be taken into account.

4.1.4 Keep records of the Personal Data Processing activities performed under its responsibilities.

A record of Personal Data Processing activities must be kept by GTL acting as Data Controller and/or Data Processor and made available to the Supervisory Authorities.

When acting on behalf of Data Controllers, the Data Processor must establish and maintain a dedicated record for each of the Data Controllers.

4.1.5 Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk

Appropriate technical and organisational measures must be implemented in order to ensure an appropriate 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 likelihood and severity for the rights and freedoms of Data Subjects as well as the state of the art of technologies and the related implementing costs.

4.1.6 Notify to the Supervisory Authority and communicate to the Data Subjects a Personal Data Breach

Adequate processes must be put in place in order to ensure the proper management of any Personal Data Breaches, including the prompt notification not later than 72 hours after having become aware of them to the relevant Supervisory Authority and, where relevant, the communication to the affected Data Subjects.

4.1.7 Carry out an assessment of the Processing impact on the protection of Personal Data (Data Protection Impact Assessment - DPIA)

At the occurrence of specific triggers, a Data Protection Impact Assessment must be carried out. The DPIA is aimed at:

- describing the Processing of Personal Data,
- assessing the necessity and proportionality of such processes with regards to the relevant purposes; and
- helping managing the risks for the rights and freedoms of Data Subjects that may arise in connection with such Processing.

4.1.8 adopt adequate safeguards and additional measures for transfers of Personal Data to a foreign country.

It must be ensured that any transfer of Personal Data to foreign country is performed only after having adopted the following recommended safeguards.

Preference must be given to the safeguards in the following order:

- the destination country ensures an adequate level of Personal Data protection as assessed by the Supervisory Authority; or
- standard Personal Data protection clauses adopted by the Supervisory Authority are signed; or
- transfer is necessary for the performance of a contract between Data Controller and Data Subject; or
- transfer is necessary for the establishment, exercise or defense in a legal claim; or
- Data Subject explicitly consents to the specific Personal Data transfer; or
- as a residual case, i.e. where the transfer is not repetitive and concerns only a limited number of Data Subjects, it is necessary for the purposes of compelling legitimate interest pursued by GTL, provided that: all circumstances have been assessed and the Data Controller has adopted all necessary safeguards for the Processing and the Supervisory Authority has been duly informed about the transfer.

GTL must be aware that the cross-border Personal Data transfer provisions apply not only to transfers of Personal Data outside the Group Generali (*e.g.*, to suppliers, vendors) but also within the Group Generali.

4.1.9 Appoint Data Processors

Before a Data Processor is appointed, it must be ensured that the Data Processor has in place appropriate technical and organizational measures capable to ensure the compliance with the Personal Data principles and requirements as well as the exercise of Data Subjects' rights.

Whenever an external provider is selected to perform activities that include the Personal Data Processing, the written appointment of this external provider as Data Processor is required.

The provisions of the GTL Outsourcing Policy will apply.

5. 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 and the applicable Personal Data protection laws and regulations;
- ensure that individuals authorized to process the Personal Data have committed to confidentiality or are under an appropriate obligation of confidentiality;
- process Personal Data only according to the instructions of the Data Controller, unless otherwise required by the applicable laws;
- maintain a record of all the Processing activities;
- implement appropriate technical and organizational measures to protect the Personal Data Processing;
- appoint a Data Protection Officer, if required;
- in case of transfer of Personal Data to a foreign country, apply the safeguards as described under par. 4.9 of this Policy;
- sign a contract or other legal act ruling the relationship with the Data Controller;
- refrain from appointing another Data Processor without the prior specific authorization of the Data Controller. In case the Data Processor has received a general written authorization to engage other Data Processors, it shall timely inform the Data Controller of any intended changes concerning the addition or the replacement of other Data Processors in order to give to the Data Controller the opportunity to object to such changes;
- whenever the Data Processor engages other Data Processors for carrying out the specific Processing activities on behalf of the Data Controller, sign a contract with this new Data Processor to impose on it the same Data Protection obligations set out in the contract with the Data Controller;
- assist the Data Controller in meeting its obligations with respect to the responding of requests related to the rights of Data Subjects (as listed under par. 4.3 above);
- assists the Data Controller in meetings its obligations by co-operating in a timely manner with any DPIA undertaken by the Data Controller and in fulfilling any obligations to engage in prior consultation with the relevant Supervisory Authority;
- provide immediate notification to the Data Controller in relation to any Personal Data Breach or incident impacting the Personal Data being processed on behalf of the Data Controller;
- after the termination of the provision of services, delete existing copies of Personal Data, at the request of the Data Controller, unless Union or Member State law requires storage of the Personal Data and
- make available to the Data Controller all information necessary to demonstrate compliance with its legal obligations as Data Processor and allow for and co-operate with audits, including inspections, conducted by the Data Controller or another auditor appointed by the Data Controller.

6. Data Protection Officer

6.1 Appointment of the Data protection officer

Whenever acting as Data Controller or Data Processor, GTL must appoint a Data Protection Officer (hereinafter "DPO") at least when they perform the following activities:

- operations which require regular and systematic monitoring of Data Subjects on large scale as core activity; or

- Processing of large scale of special categories of Personal Data (*e.g.*, Sensitive Personal Data) or Judicial Data as core activity.

The evaluation on the need or the opportunity to appoint the DPO is made by GTL BOD and must be incorporated in the minutes of the relevant meeting. Compliance Function of GTL must publish and communicate to the relevant Supervisory Authority the DPO's contact details.

The DPO can be outsourced to third parties. The outsourcing of the DPO activities must be considered as "critical" according to the provisions of the GTL Outsourcing Policy.

To be effective, the DPO must have a clearly defined mandate and be positioned and perceived throughout the organisation as an independent function and essential part of the internal control system.

The DPO must report to BOD and shall not hold a position that leads him to determine the purposes and the means of the Processing of Personal Data.

Any conflicts between task of DPO and requirements in this Policy shall be proposed to Data Protection Committee ("DPC") to consider and approve the conflicts.

The roles and responsible including members of Personal Data Protection Committee is subjected to Data Protection Committee Charter.

6.2 Mission

The Data Protection Officer 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 up to the management to act and demonstrate that each specific Processing operation is carried out in accordance with the applicable provisions.

The DPO's mission is to:

- inform and advise the GTL BOD on compliance with the Personal Data protection laws, regulations and administrative provisions,
- monitor the internal compliance with the Personal Data protection laws, regulations and administrative provisions, also adopting a risk-based approach that allows DPO to prioritize the activities, including assignment of responsibilities, awareness-raising and training of staff involved in Processing operations, and the related audits, to be carried out and to focus the efforts on issues that present the higher Personal Data protection risks,
- provide advice to the Senior Management where requested as regards the DPIA (on whether or not to carry out a DPIA, what methodology shall be followed, whether to carry out a DPIA internally or outsource it, what safeguards shall be applied to mitigate any risks to the rights and freedoms of the Data Subjects) and monitor its performance (whether or not the DPIA is correctly carried out, whether the Personal Data Processing activities can be carried out meanwhile and what safeguards should be adopted and whether its conclusions are in compliance with data protection laws and regulations); and
- act as contact point for the Data Subjects and the Supervisory Authority on issues relating to Processing, including prior consultation in relation to DPIAs indicating that the Processing would result in a high risk in the absence of measures taken by GTL to mitigate the risk.

To perform the above mission, it has to be ensured that the DPO is properly and in a timely manner involved in all the operations and transactions which relate to the protection of Personal Data. Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the applicable regulations and ensure privacy by design-approach; this should therefore be standard procedure within GTL's organization.

6.3 Independence of DPO

GTL BOD ensures that the DPO is independent.

In order to preserve his/her independence, the DPO:

- cannot receive any instructions regarding the exercise of his/her tasks;
- cannot be dismissed or penalized for the performance or his/her tasks;
- cannot be instructed how to deal with a matter, what results should be achieved, how to investigate a complaint or whether to consult the Supervisory Authority, or to take a certain view of any issue related to Personal Data protection law, or a particular interpretation of the law;

- is allowed to make its dissenting opinion clear in case of business decisions that are incompatible with the Personal Data protection law and/or his/her advice; in case Senior Management disagrees with the advice of the DPO, the reasons for not following the DPO's advice must be duly documented.

6.4 Responsibilities of the DPO

The Data Protection Officer 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 up to 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, at least, to:

- provides guidelines and operating procedures for the implementation of Personal Data related policies;
- defines methodologies to be used (where required) in respect of Personal Data Processing operations;
- steers with GTL BOD, if provided by legislation, on site assessment on Personal Data protection-related topics;
- is systematically involved at the earliest stage possible in all issues relating to Personal Data protection and all relevant information are passed on to the DPO in a timely manner in order to allow him/her to provide adequate advice;
- is promptly consulted once a Personal Data Breach or another incident occurs;
- provides advice whenever a DPIA is carried out;

- acts as contact point for the Supervisory Authority on issues relating to Processing, including the prior consultation (in case of DPIA) and to consult, where appropriate, with regard to any other matter; acts as contact point for the Data Subjects in case, for example, of exercise of rights.

6.5 Fit & proper requirements.

The DPO must possess an expert knowledge of:
- the Data protection laws and regulations and also practices,
- the Personal Data Processing operations carried out by GTL,
- the administrative rules and procedures of GTL,
- the business sector in which 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 to foreign country.

The Fit & Proper Policy applies.

7. Lead Data Protection Supervisory Authority

If a Lead Supervisory Authority needs to be identified, this must be evaluated jointly with the DPC.