Generali Group

PERSONAL DATA PROTECTION GROUP POLICY

Public version

generali.com

EXECUTIVE SUMMARY

The Personal Data Protection Group Policy (hereinafter, also the "Group Policy") defines the principles of the implementation of the European Union privacy laws (including the GDPR - as defined hereinafter -, the national laws implementing GDPR provisions and the guidelines issued by the European Data Protection Board) across the Group and sets the minimum requirements that each Group Legal Entity must implement when Processing Personal Data.

To this purpose, the Group Policy provides:

- the principles that must inspire the Processing of Personal Data;
- the requirements to be implemented whenever acting as Data Controller, Data Processor or Joint Controller in respect of specific Personal Data Processing,
- the role and the responsibilities of the Data Protection Officer.

INDEX

1 Introduction

1.1 OBJECTIVES

The Generali Group considers 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 Group Policy is to set the key principles and requirements to be followed when Processing Personal Data, keeping into account the provisions of the GDPR.

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

2 Key Principles governing Personal Data Processing

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

- **lawfulness, fairness and transparency**: identify valid grounds (known as a 'lawful basis') for the Processing and provide Data Subjects with a proper Privacy Notice. Processing Personal Data in a way that is unduly detrimental, unexpected or misleading to the Data Subjects concerned is not allowed;
- **purpose limitation**: collect Personal Data 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 strictly necessary to pursue the purposes described in the Privacy Notice;
- **accuracy**: do not process inaccurate Personal Data and, where necessary, keep them updated; when it is discovered that Personal Data are inaccurate, in respect for the purposes for which they are processed, Group Legal Entities 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. 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 local applicable laws and regulations. Following the expiration of the retention period, Personal Data can be retained only in a form which does not permit the identification of the Data Subjects. To implement this principle, technical measures to irreversibly de-identify Personal Data, which include deletion, obfuscation, redaction, anonymization, must be adopted;
- **integrity and confidentiality**: ensure that appropriate organizational and technical measures are in place to protect Personal Data, so to avoid un-authorized or unlawful Processing, accidental loss, destruction or damage.

The Data Controller is responsible for the compliance with the principles above and must be able to demonstrate at all times ("**accountability**" principle). This is pursued through the adoption of appropriate internal regulations, processes and other measures which can include, at least, the keeping of a record of processing operations, the performance of a Data Protection Impact Assessment, 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 a Group Legal Entity 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 Group Policy and the applicable regulations.

3.1 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 (see below), where appointed, is involved properly and in a timely manner (from the earliest stage possible) in every issue related to the protection of Personal Data.

3.1.1 Process Personal Data on the basis of lawful grounds

The Data Controller must identify the lawful basis of each Data Processing 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:

- 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 Group Legal Entity is subject; or
- necessary in order 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; or
- necessary for the purposes of a legitimate interest pursued by the Group Legal Entity, unless there are interests or fundamental rights and freedoms of the Data Subject that prevail.

Processing of Special Categories of Personal Data is prohibited, except when it is:

- based on the explicit consent given by the Data Subject for one or more specific purposes except where applicable laws and regulations provide a prohibition that cannot be lifted by the Data Subject;
- 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 authorized by applicable law;
- 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;
- necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- 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;
- 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 Special Categories of Personal Data.

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

The Data Controller must provide Data Subjects with an adequate and clear Privacy Notice relating to the Processing of their Personal Data.

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

The Data Controller, prior to implementing or rolling-out a new Privacy Notice, or amending an existing one, must consult the DPO on the proposed new or modified Privacy Notice prior to its finalization. The DPO must check that its content is accurate and corresponds with the record of Personal Data Processing activity and that all of the relevant Personal Data Processing activities undertaken by the Group Legal Entity are included.

3.1.3 Facilitate the exercise of Data Subjects' rights

As a general 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 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 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:

- 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.

3.1.4 Ensure that Personal Data protection is granted 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 GDPR 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 (**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.

Appropriate technical and organizational measures must ensure, by default, 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**).

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

The Data Controller must keep a record of Personal Data Processing activities and make it ready and available to the Supervisory Authorities.

3.1.6 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 in order 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 for the rights and freedoms of Data Subjects posed by the Processing.

The Data Controller, with a "privacy by design and by default" approach, shall ask for advice to the DPO on the appropriate technical and organizational measures to implement without prejudice to the involvement of any other functions in relation to their area of responsibility.

3.1.7 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, where appointed, as well as the prompt notification of any Personal Data Breaches to the relevant Supervisory Authority not later than 72 hours after having become aware of them, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons and, where relevant, the communication to the affected Data Subjects.

3.1.8 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, the Data Controller performs a Data Protection Impact Assessment ("DPIA").

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.

The Data Controller shall ask the advice of the Data Protection Officer, where appointed, when carrying out a Data Protection Impact Assessment.

3.1.9 Adopt adequate safeguards and additional measures for transfers of Personal Data outside the EEA

The Data Controller must ensure that any transfers of Personal Data outside the European Economic Area (EEA) is performed only if necessary and after having adopted at least one of the following recommended safeguards and the supplementary measures appropriate to ensure that the Personal Data transferred receive, in the non-EEA country of destination, a level of protection essentially equivalent to the one provided in the EEA. Preference is to be given to Processing taking place only inside EEA.

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

- the non-EEA country ensures an adequate level of Personal Data protection as assessed by the European Commission; or
- transfer is necessary for the performance of a contract between the Data Controller and the Data Subject; or

- transfer is necessary for the establishment, exercise or defence of a legal claim; or
- Data Subject explicitly consents to the specific Personal Data transfer; or
- standard Personal Data protection clauses adopted by the European Commission are executed and can be complied with (in light of the laws and practices of the non-EEA country of destination of the Personal Data); 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 the Group Legal Entity, 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.

When the transfer to a non-EEA country is based on standard Personal Data protection clauses adopted by the European Commission, 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 afforded in the third country a level of protection essentially equivalent to that guaranteed in the European Union.

If no safeguard is applicable and/or if no additional measure appears to be effective to ensure that the Personal Data transferred receive, in the third country of destination, a level of protection essentially equivalent to that guaranteed in the European Union, 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 Group and outside the Group (e.g., to suppliers, vendors).

3.1.10 Appoint Data Processors

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

3.2 KEY REQUIREMENTS FOR THE DATA PROCESSOR

Whenever, as regards to a specific Processing of Personal Data, the Group Legal Entity acts as **Data Processor**, it must:

- process the Personal Data in accordance with the principles set out under this Group Policy, the applicable Personal Data protection laws and regulations and only according to the 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 all categories of the Processing activities; with a dedicated record of each Data Controller;
- implement appropriate technical and organizational measures to protect the Personal Data Processing;
- in case of transfer of Personal Data outside EEA, ensure application of the safeguards and measures as described under this Group Policy;
- sign a contract or other legal act ruling the relationship with the Data Controller;
- refrain from appointing another sub-Data Processor without the prior authorization of the Data Controller. In case the Data Processor has received a general written authorization to engage other sub-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;
- 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 the European 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.

3.3 KEY REQUIREMENTS FOR JOINT CONTROLLERS

When two or more Data Controllers act as Joint Controllers (either within the Group or outside the Group), the Group Legal Entities 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 an 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,
    - transparency obligations,
    - individuals' rights, DPIA, records and Personal Data Breach management,
    - contact point for Data Subjects,
    - Personal Data transfers (if any).

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

4. Key Requirements for The Data Protection Officer

Personal data protection is an identified and constantly managed risk within the operational risk management framework of the Group. The risk is therefore assessed and monitored by 3 level lines of defense: Operational, Risk and Compliance\DPO, and Audit.

When a Group Legal Entity appoints a Data Protection Officer (DPO) must grant that DPO is a subject matter expert, subject to Fit & Proper requirements and independent.

DPO is in charge, at least, to:

- inform and advise Group Legal Entity, Senior Management and personnel of their obligations related to the Processing of Personal Data pursuant to the GDPR and any other applicable law;
- monitor compliance with the GDPR, other national applicable Personal Data protection laws and the Legal Entity policies on the subject matter, 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 its performance;
- 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;
- advise Group Legal Entity in personal data breach management and support it in notifying and communicating the breach to the Authority and\or to the Data Subjects (when required).

Each Group Legal Entity must involve, inform and consult its DPO properly and in a timely manner, in order to ensure a privacy by design approach and compliance with applicable provisions.

In particular DPO, whenever appointed, with the support of Compliance staff, regularly plans and executes controls activities, quarterly collects Key Risk Indicators in order to monitor the personal data protection risk exposure and involves all relevant risk owners in a comprehensive risk assessment, at least once a year, in order to highlight any needed mitigation action to the Board of Directors.

What above to the extent that it does not conflict with other Country's applicable laws and regulations or requirements.