Generali Real Estate S.p.A. SGR

PERSONAL DATA PROTECTION POLICY

Assets & Wealth Management Compliance Function

POLICY

For internal purposes only

Generalirealestate.com

ABSTRACT

EXECUTIVE SUMMARY

The Personal Data Protection Policy (hereinafter, also the "**Policy**") defines the principles for 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 and sets the minimum requirements that Generali Real Estate S.p.A. SGR (hereinafter, also "**GRE SGR**" or the "**Company**") must implement when Processing Personal Data.

1. KEY PRINCIPLES GOVERNING PERSONAL DATA PROCESSING

Personal Data processing shall be carried out in compliance with the Relevant Data Protection Regulation and this Policy; specifically, it shall be based on the following key principles:

- **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, the Data Controller 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 must be adopted to irreversibly de-identify Personal Data, which include deletion, obfuscation, redaction, anonymization;
- **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.

The Data Controller is responsible for the compliance with the principles above and must be able to demonstrate it at all times ("**accountability**" principle) 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 DPIA, the performance of controls to verify the status of implementation of the Personal Data protection principles and requirements.

2. KEY REQUIREMENTS

Considering the above principles, different key requirements need to be implemented depending on whether Personal Data are being processed by GRE SGR 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 Relevant Data Protection Regulation.

[…]