Group Privacy Policy

Objective

As a business with a large global footprint, Prudential must navigate several different privacy laws. The Group Privacy Policy sets out the standard of privacy expected to be achieved across our global offices, in order to ensure that Prudential handles personal data in compliance with regulatory requirements and in line with customer and employee expectations while meeting the demands of a competitive commercial organisation.

Group Privacy Policy established the requirements for ensuring processing activities concerning personal data of our customers, staff members, agents and stakeholders embedded with 'Privacy-by-Design' principle. This supports Prudential's trustworthiness with customers and stakeholders, where they can let us process their personal data without concerning their data will be misused.

These minimum standards take into account the legal requirements of the EU General Data Protection Regulation, the OECD's Privacy Principles, and APEC Privacy Framework.

Principles and Policy Summary

Group Privacy Policy follows 'Privacy-by-Design' principles and the key principles of the privacy policy consist of:

- **Lawfulness** – to ensure we collect, use, disclose and retain personal data with a lawful ground.
- **Transparency** – to ensure we provide sufficient transparency to the individuals, whom their data will be processed by us, regarding what data, why and how we collect, use, disclose and retain their data.
- **Purpose Limitation** – to ensure we only use, disclose and retain personal data for the specific purposes as defined when the data was collected.
- **Data Minimisation** – to ensure we are not collecting, using, disclosing and retaining irrelevant personal data in accordance with the purposes of processing.
- **Security** – to ensure sufficient technical and organisational measures are in place to protect personal information during collection, use, disclosure and storage.
- **Data Transfer** – to ensure the data transfers (including cross-border transfers) are being supported with sufficient legal basis and records.
- **Storage Limitation** – to ensure we will not keep personal data longer than is necessary for the purposes of collection and use or any legal requirements.
- **Breach Handling** – to ensure personal data breach will be handled and reported in accordance to the regulatory requirements.
- **Data Subject Rights** – to ensure the compliance with Data Subject Rights to the extent of the applicable data privacy regulations.
- **Privacy Risk Assessment** – to ensure privacy risk/impact assessment will be completed when introducing new or significant changes to technology, systems, applications and/ or processes concerning the processing of personal data.