Our approach to

Personal Data Management

Based on the Personal Data Management Standard, version 2.6, approved by the Board of Directors on August 27th, 2024

INTRODUCTION

Data protection and privacy are of paramount importance to Ageas. As Ageas processes various categories of data, including personal data, the company applies a set of overarching principles to ensure **responsible and secure data management.** These principles cover **ethical** data handling, data **quality**, and data **security**.

SCOPE

Ageas Information Security Policy applies to **ageas SA/NV and all its Subsidiaries** and to their Staff.

For the **Subsidiaries**, should compliance with Information Security Policy result in non-compliance with local legislation or regulations, the latter must take precedence. The Group Policy owner must be informed and consulted immediately in such circumstances.

For the **Affiliates** it is recognised that the requirements of the local law, the local regulator and the majority shareholder's policy applies. However, Ageas will advise similar principles with reasonable effort.

AGEAS APPROACH TO DATA PROTECTION

FRAMEWORK

Ageas has established a robust Personal Data Management Framework supported by clear policies, processes, procedures, and governance mechanisms to ensure that the rights of data subjects are respected throughout all personal data processing activities. In line with the GDPR and other applicable regulations, Ageas ensures that personal data is **appropriately protected**, used **only** for the **purpose** for which it was **ultimate accountability** for, processed subject to the required **consent where applicable**, and **retained no longer than necessary** in accordance with data retention procedures. This approach is part of broader governance framework and contributes directly to sustainability obligations.

This framework sets out the rules and principles governing the processing and protection of personal data across Ageas and its entities. It grants data subjects a **clear set of rights**, defines **formal obligations** for Ageas when processing personal data, ensures that relevant processes are documented and consistently applied, enhances **transparency** - including information on **data transfers** outside the EEA - and strengthens the **protection of interest** of customers, staff, and other stakeholders. These measures support Ageas's commitment to responsible **business conduct**, **ethical** data use and the **mitigation** of data protection **risks** that may have double-materiality impacts

PRINCIPLES

Information about Ageas' data processing practices is shared with data subjects through dedicated **Privacy Notices** published on ageas SA/NV and its European subsidiaries websites and is included in product documentation.

AWARENESS & TRAINING

Ageas invests continuously in raising **awareness** and offering **mandatory training** for individuals involved in personal data processing. These activities ensure that staff understand their accountabilities and responsibilities regarding data protection, contributing to effective internal control systems and reinforcing governance and risk management practices.

EXTERNAL REVIEW

Ageas operating companies are ISO 27001:2022 certified. To maintain this certification, **yearly external assessments** are carried out by accredited ISO Certification Authorities, covering various aspects of information and data security, including personal data protection. This certification further reinforces Ageas's governance, security controls and resilience measures.

Next to that Ageas conducts **annual assessments** to evaluate its maturity in Data Protection. The results of this assessment are part of the annual DPO report to the Ageas Board of Directors, focusing on key risks and compliance status as well as key areas of improvement.

GOVERNANCE

Data Protection roles and responsibilities are clearly defined and assigned at all levels of organisation. This includes Board of Directors and Executive Committee responsibilities:

The **Board of Directors** of Ageas is **ultimate accountability** for the design and oversight of the implementation and correct operation of the controls related to the Personal Data Management as well as for the appointment of the DPO where required.

The **Executive Committee** of Ageas is **responsible for implementation**, maintenance and continuous improvement of the rules and principles with regards to data protection in accordance with applicable laws and regulations. This includes:

- Complying with all relevant EU and local laws related to the protection of personal data
- Protecting the rights and freedoms of individuals whose personal data are processed
- Ensuring compliance with data protection principles such as lawfulness, fairness, transparency, data minimisation, integrity and confidentiality, purpose limitation, storage limitation and data retention
- Making sure that data protection is incorporated in the Data Management Governance Framework and is part of Information Security implementation

Ageas has **appointed Data Protection Officers** (DPO's) at its head office and within its operating companies. The DPO function operates independently and performs following tasks:

- Provides **advises** and information to management and employees on GDPR compliance
- **Monitors** implementation of the Personal Data Management Framework to ensure adherence to data protection obligations
- **Advises** on Data Protection Impact Assessments (DPIAs).
- Performs **analysis** of security, privacy, and data protection risks.
- Ensures adequate **oversight** and reporting to the Board of Directors.
- Organises educational initiatives to **reinforce understanding** and compliance.
- Contributes to Ageas's overall governance structure and **supports** its **disclosure** obligations regarding internal control and risk management systems.

The **DPO** also acts as a point of **contact** for supervisory **authorities**. This includes:

- Providing **guidance** and **assistance** to management when a DPIA identifies high risks to individuals that cannot be mitigated, and Data Protection Authority (DPA) must be consulted
- **Supporting** data breach **notifications**
- **Facilitating communication** between the supervisory authority and the Ageas organisation.