Our approach to Personal Data Management

Based on the Personal Data Management, version 2.0, approved by the Board of Directors on August 6, 2019

INTRODUCTION

Data protection and privacy is of paramount importance to Ageas. Since various types of data are being processed by Ageas, generic principles (that also apply to personal data) govern how we manage data, including the ethical treatment of data, data quality and data security.

AGEAS APPROACH TO PERSONAL DATA MANAGEMENT

Ageas has implemented relevant policies, processes, procedures and a strong governance to ensure that data subject rights are being respected while processing personal data – Ageas ensures that such data is appropriately protected and used only for the purpose it has been collected and as consented where required by the data subject. Ageas has implemented a personal data management framework which consists of the rules and principles relative to the processing and protection of personal data within Ageas and its entities. These rules give more rights to data subjects on the one hand and provide strict and formal rules for Ageas when processing personal data on the other hand. Processes have been formalised and all relevant information is communicated to the data subjects, including information on the data transfer outside EEA. As such Ageas has strengthened transparency and control, protecting the interests of customers, staff, and other key stakeholders regarding data privacy.

Ageas also invests in permanent awareness, communication and mandatory training for individuals involved in processing of personal data.

Ageas has appointed Data Protection Officers (DPO's) within its head office and its European operating companies. Within Ageas a DPO is an independent function that provides adequate support to the management team with regard to their accountability for ensuring compliance with GDPR. The DPO develops and monitors the implementation of the Personal Data Management framework through appropriate management structures and controls, and performs analysis of security, privacy and data protection risks. The DPO provides the advice on Data Protection Impact Assessment (DPIA) and monitors related risks.

Furthermore, the DPO is at liberty to inform the local Data Protection Authority (DPA) in case the DPIA indicates that there would be a high risk for the data subjects and there are insufficient measures to mitigate those risks. The DPO also organises educational programmes to staff making sure that accountabilities and responsibilities within the entity are understood.

Dedicated assessments on Data Protection are also regularly performed.