1 Summary of Varma's information security policy

Varma's information security policy describes the importance of information security at Varma, the roles and responsibilities in the implementation of information security and the key means to manage information security risks. The aim of the policy is to ensure, for its part, that Varma's data/data retained by Varma is protected and that services function in both normal and exceptional situations. The policy applies to all Varma employees and stakeholder representatives who process Varma's data. The policy covers all data of Varma and the processing of data for the duration of their entire life cycle. Varma's Executive Group has approved the information security policy and is responsible for ensuring sufficient resourcing and that the policy is complied with in Varma's operations.

1.1 Importance and objectives of information security

The purpose of information security implemented at Varma is to support Varma's basic mission, that is, securing pensions. The objectives of information security have been established based on Varma's values and operational objectives.

The objectives are:

- Responsibility: Information security work is carried out responsibly and based on Varma's values and the statutory mission.
- Quality of pension services and investment activities: Information security is a part of developing and producing reliable, high-quality pension and insurance services, customer relationships, investment activities and partnerships.
- Efficiency: Information security is implemented efficiently in relation to the risks managed through information security.

All Varma employees and individuals working on assignments of Varma are responsible for complying with the information security policy, principles and instructions and for ensuring compliance with the information security, data protection and confidentiality obligations applicable at the given time. We ensure this through continuous training and through securing competence.

1.2 Data protection principles

Varma's data protection principles describe the basic principles for the processing of personal data at Varma and the importance of data protection in Varma's operations. The objective of the principles is to ensure that legislation concerning privacy protection and the processing of personal data is complied with at Varma. The data protection principles are based on the data protection principles of the EU's General Data Protection Regulation and the rights of data subjects. The principles cover the entire life cycle of personal data.

The principles are based on a risk-based approach to data protection. In other words, Varma implements the necessary technical and organisational measures required to ensure and demonstrate that the processing of personal data is compliant with the EU's General Data Protection Regulation, while considering the nature, scope, context and purposes of processing and the risks concerning the rights and freedoms of natural persons, with the risks varying in terms of probability and gravity.

1.3 Processing of personal data at Varma

1. Personal data is only processed lawfully and fairly and in a manner that is transparent to the data subject (lawfulness, fairness and transparency)
2. Personal data is only processed for specific, explicit and legitimate purposes, and the same applies to any further processing (purpose limitation)
3. Personal data is adequate, relevant and their processing is limited to what is necessary in relation to the purposes for which they are processed (data minimisation)
4. Personal data is accurate and, where necessary, kept up to date, and Varma implements all reasonable steps to ensure that personal data that is inaccurate is erased or rectified without delay (accuracy)
5. Personal data is kept in a form which permits identification of data subjects for no longer than is necessary due to legislation or for the purposes for which the personal data is processed (storage limitation)
6. Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful use (integrity and confidentiality).

The data protection principles are complied with in all phases of the processing of personal data. Varma must also be able to demonstrate that the obligation in question has been complied with.

Varma uses technical and organisational measures in the initial phase of the planning of processing functions in order to safeguard the privacy and data protection principles from the very beginning (data protection by design). In addition, Varma ensures by default that personal data is processed in accordance with the valid data protection regulations while ensuring a high level of privacy protection (e.g. only necessary data should be processed, short retaining periods, limited access) and that personal data is not accessible by default to an indefinite number of natural persons (data protection by default).