INFORMATION SECURITY POLICY

With regard to information provision and security, VCK Travel aims to assure all stakeholders, employees, customers and suppliers that any information they provide is processed, saved and accessed with care. We wish to distinguish ourselves by the extent to which and how we protect privacy-sensitive data. For this reason, our policy is aimed at implementing as few cloud solutions as possible, while providing hosting facilities ourselves as far as this is reasonably possible.

We are increasingly facing external threats. In addition, as more and more data flows are being processed and connected, we are also faced with internal risks. Choices between transparency and openness of information on the one hand and the security of confidential information on the other hand require careful consideration. In the coming years, VCK Travel will continue to work on increasing information security, protecting privacy and further professionalising the information security function in our organisation.

To control information security and protect privacy, an information management system has been set up and implemented throughout the VCK Travel organisation in all offices. This management system has been certified in accordance with the ISO 27001:2013 standard. The Data Protection Officer is responsible for maintaining and continuously improving this information management system. Our information security policy applies to the entire organisation and applies to all managers and employees of VCK Travel. VCK Travel's information security policy is in line with the relevant national and European laws and regulations.

The Management Team (MT) plays a crucial role in the implementation of this information security policy. For example, the MT makes an estimate of the importance of the various aspects of information provision for VCK Travel, the risks that VCK Travel runs as a result, and which of these risks are unacceptably high. Based on this, the MT draws up this information security policy. The Data Protection Officer is responsible for informing the organisation about this policy, while supporting and monitoring its implementation. VCK Travel has put in place and will maintain a coherent package of measures to safeguard the reliability of the information provision process.

Employees are periodically and in various ways made aware of the risks related to information security. They are also informed about the new information security policy, and receive instructions that help them to carry out their work properly and in compliance with the standards set by the policy.

We strive to prevent or reduce the information security risks of our business activities as much as possible, while continuously improving the information security system by means of the following objectives:

Starting points

The starting points of our information security policy are:

- The core of our business activities is data processing. All information and information systems are of critical and vital importance to VCK Travel. The responsibility for information security lies with the managers, with the MT bearing ultimate responsibility. The responsibilities for data protection and for the implementation of security procedures have been explicitly defined.

- VCK Travel aims to prevent data leaks and improper use of information.
- The quality of information provision is embedded within the organisation through periodic monitoring, organisation-wide planning and coordination. The information security policy, together with the information security plan, forms the basis for reliable information provision. In the information security plan, the reliability of information provision is addressed for the entire organisation.
- The plan is periodically updated on the basis of new developments, reports in the incident register and risk analyses.
- Every year, concrete objectives, actions and measures are agreed upon. The resources needed to achieve these objectives are assessed by the management and, if approved, made available.
- The Information Security Manager supports the organisation in monitoring and increasing the reliability of information provision and reports on this.
- VCK Travel makes the necessary people and resources available to secure its property and its work processes in accordance with this policy.
- VCK Travel's information security policy is in line with the relevant national and European laws and regulations and also complies with voluntarily endorsed requirements.
- Rules and responsibilities for the security policy will be established and documented.
- In the event of unexpected data leakages, the Data Leakage Protocol will enter into force and, where appropriate, the leakage will be reported to the Authority for Personal Data.
- All employees of VCK Travel are individually responsible with regard to information security. They shall be informed of and trained in the handling and use of the security procedures.
- VCK Travel aims to ensure that information can only be accessed by those who are authorised to do so. Every employee, whether permanent or temporary, has a duty to protect data and information systems from unauthorised access, use, alteration, disclosure, destruction, loss or transfer whenever this is necessary, and to report any suspected violations.

Information security system

VCK Travel has established an information security management system in accordance with the ISO 27001:2013 standard in the form of a manual. This manual has been published on the iChannel intranet. For efficiency and environmental reasons, it is only available digitally.

In VCK Travel's offices and departments, the information security management system is explained to all employees through presentations, workshops and articles on iChannel. Suppliers are informed about VCK Travel's information security policy by specific VCK Travel employees responsible for this task. Each department has appointed an employee who is responsible for information security and who is the point of contact for all matters concerning information security.