Information Security Practices

Introduction	Shop-Apotheke Europe (SAE) is a global company committed to ensure the protection of confidential information & personal data. As a company that is operating in the health sector, we are bound to strict regulations. We acknowledge that we have sensitive customer data and information about our customers that need to be protected sufficiently and therefore take the topic of data security and data privacy very seriously. SAE recognizes the importance of implementing appropriate technical and organizational security measures in order to prevent any unauthorized access, disclosure, alteration or destruction of such data. For this purpose, SAE implements industry standard security controls. This is not meant to be the SAE Security Policy but only a summary of the measures implemented for specific business activities. SAE security measures follow a risk assessment approach and embrace the principles privacy and security by design.
Certifications and standards	Quality management ISO 9001:2015 Payment Card Industry Data Security Standard (PCI DSS) Guidelines on Good Distribution practice of medicinal products for human use (GDP) Respecting OWASP Secure Coding Practices Legal compliance with the General Data Protection Regulation (GDPR) IT-Control Framework based on ITIL and COBIT
Relevant corporate security policies and procedures	Information security policy Business resumption plan Incident management process Security breach notification process Privacy breach notification process Adequate technical and organizational measures Transparent data privacy policy
Human Resources Security	All SAE employees are bound by confidentiality duties and have received all necessary information on the confidential handling of data. Above that, every incoming employee is sensitized in a mandatory session by our data protection coordinator. Starting in early 2021 every employee will receive data protection and security awareness trainings on an at least annual basis. Upon termination of a work relationship all access to information environments is removed and com company assets are retrieved.
Sub-contractors	SAE has concluded data protection agreements/addendums with its service providers in order to ensure that at least the same level of confidentiality and data security is implemented by its sub-contractors. SAE has the right to perform audits in order to monitor the compliance of its subcontractors with the agreed technical and organizational measures regarding data confidentiality and security.

Physical and Environmental Security	Access to premises and production environment is monitored through access controls and video surveillance in the production environment, so that only authorized personnel has access to equipment and information. Asset movement controls are in place and the building is engineered for seismic, flood and other similar risks. In order to ensure data availability and integrity, cloud services are used for hosting data. All applications and infrastructure used in production are monitored.
Technical and access controls	Access to all systems is password protected and granted only to authorized personnel. Password complexity as well as enforced password change are implemented to prevent unauthorized and inappropriate access. Two factor authentication and time-out of system access for remote access is in place. SAE uses encryption for data in transit and at rest. Access of system administrators and operators are audited and critical security updates released are installed. Detection and prevention systems are in place to protect network security.
Data protection and security	To be able to adequately be responsive to all issues arising around the topic of data protection, SAE has an internal data protection coordinator and in this position, is responsible for all issues around data security and data privacy. Next to that, an external data protection officer is in place who in close consultation holds an advisory and procedure directory function. On the executive level, the Chief Information Officer and the lead pharmacist are responsible for data privacy and security issues. We neither collect, nor process, nor transfer any personal data, (including both essential and non-essential personal data), without fulfilling our information obligations or, where needed, obtaining the customers' consent. Among others, the essential principles of lawfulness, fairness and transparency, and principles of data minimization, data economy and purpose limitation form the basis for designing the company's processes in this regard, inter alia meaning that only data essentially needed for running the business are collected and processed.