



Security and compliance.

Discover the catalogue of technical and organisational security measures employed to ensure Daily Control™ security and compliance.



Overview

SGR's services comply with the new Swiss Federal Data Protection Act of September 25, 2020 (nLPD) and international privacy regulations, including the Regulation (EU) 2016/679 on the Protection of personal data (GDPR).

SGR's privacy compliance ensures the confidentiality of personal data through appropriate security measures, and it also establishes data collection policies that ensure lawful and proper processing, limited to predefined purposes.

SGR is committed to ensuring and maintaining high standards of data security in the provision of its services and carefully monitors technological developments to constantly improve its data protection and security policies.

Discover the catalogue of technical and organisational security measures routinely employed by SGR as part of its ongoing commitment to ensure security and compliance.

SGR will update this document accordingly to reflect changes in the security measures adopted.

Further information regarding data processing and management can be requested at privacy@sgrcompliance.com.



Security measures

- Authentication

Strong authentication policies are adopted to ensure the confidentiality and integrity of access credentials during their assignment, communication, and storage (e.g., two-factor authentication and complex password requirements).

- Awareness and confidentiality

Staff members with access to data undergo appropriate training to ensure the correct handling of personal data, reducing the likelihood of events that could impact the confidentiality, integrity, or availability of data.

Staff members with access to data are also bound by confidentiality obligations.

- Backup and recovery

Backup and recovery solutions have been implemented to create copies of data and recover them quickly in case of loss or damage. A backup strategy has been developed, considering the frequency and security of copies, as well as the type of data to be protected and their retention policies.

- Data transfer

The data is processed and transferred in Switzerland and other countries with legislation that guarantees an adequate level of data protection or, in the absence of such legislation, based on appropriate contractual safeguards.

The adequate level of data protection in Switzerland has been recognised and confirmed also by the European Commission.

- Encryption

Data is transferred and stored using encryption modules that ensure adequate security both in the production and the backup phases.

- Firewall

Unauthorised access to servers and other devices within the network is prevented through appropriate Firewall systems.



- Processors

When selecting data processors or sub-processors, we ensure that we choose only those providing sufficient guarantees in terms of knowledge, reliability, and resources, and implementing appropriate technical and organisational measures to meet privacy and cyber security requirements.

- Roles and privileges

Data access is governed by the principle of least privilege. Authorisation profiles are periodically reviewed to ensure that authorised personnel accesses only data necessary for processing.

- Security breaches

A specific procedure is in place to handle events and security incidents with potential impacts on the confidentiality, availability, and integrity of data.

- Server protection

Servers used for SGR services are safeguarded to ensure data security and operational continuity. Security measures include access control systems, surveillance and intrusion detection systems, and emergency management tools.

- System administrators

Functions and responsibilities of System Administrators are defined in specific appointments. Before the designation, appropriate assessments are conducted to assess experience, skills, and reliability. Regular checks on performed activities are scheduled as well.

- Vulnerability assessment

Regular vulnerability assessment and penetration tests are conducted to assess exposure to known vulnerabilities and verify the security level of the systems. The results of these checks are carefully examined to identify areas of improvement necessary to ensure an updated security level.



Control Center™ Specs & Add-ons

Control Center™ is a multi-layered tool integrated into Daily Control™, designed to simplify and streamline the collection and management of relevant information within due diligence processes.

The suite of specific security measures includes:

- encryption modules to safeguard data transmission, storage, and archiving;
- customised access and visibility permissions based on users' roles and responsibilities;
- log registry to track all activities and their history, ensuring precise record-keeping;
- secure file sharing and structured data export functions for verification and auditing purposes.