Daily Control™ Services – Technical and Organizational measures.

SGR's services comply with the new Swiss Federal Data Protection Act of September 25, 2020 (nLPD) and the General Data Protection Regulation (GDPR) (EU) 2016/679.

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.

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

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

Technical measures	Firewall	Unauthorized access to servers and other devices within the network is prevented through appropriate Firewall systems.
	Encryption	Data is transferred and stored using encryption modules that ensure adequate security both in production and backup phases.
	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.
	Authentication	Authentication policies are adopted to ensure the confidentiality and integrity of access credentials during their assignment, communication, and storage.
	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.

	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.

Organizational measures	Training	Staff members with access to data receive necessary training to ensure the proper handling and adherence to the principles of confidentiality, availability, and integrity of the processed data.
	Confidentiality	Staff members with access to data are bound by confidentiality obligations.
	Roles and privileges	Data access is governed by the principle of least privilege. Authorization profiles are periodically reviewed to ensure that authorized personnel only accesses 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.

(Updated November 2023)