St.Galler Kantonalbank

Terms and conditions for electronic services

Version 11.2025

1. Applicability

These terms and conditions apply to the use of the electronic services (in particular e-banking and the mobile app) of St.Galler Kantonalbank AG. In all other respects, the basic agreement, including the basic documents and any special agreements, shall apply. The user confirms that they have taken note of the basic documents and declare them to be binding. The current version of the basic documents is published at https://www.sgkb.ch/en/legal-guidelines.

Information on the electronic services can be found at sgkb.ch/e-banking.

2. Identification

Access to the electronic services is granted to those who have identified themselves by entering the means of identification valid for the corresponding service. Anyone who has provided valid identification is deemed by the Bank to be authorised to use the corresponding service. The Bank may give this authorised person the right to make certain requests or raise queries, allow them to dispose of assets and receive orders and legally binding notifications from them. The user unconditionally authorises all transactions, orders and notifications made or submitted using their means of identification.

The Bank has the right to refuse to execute orders and to insist that the user identifies themself in another form (e.g. by signature or by personal appearance).

The Bank shall notify the user in advance in an appropriate manner if it changes or adapts the means of identification or the process.

3. Duty of care

The user must inform themself about the necessary security precautions and take reasonable precautions. Further information on security during use can be found at sgkb.ch/sicherheit.

3.1 Means of identification

The user is obliged to change the password provided by the Bank immediately upon receipt and regularly thereafter. The password must not consist of easily determinable combinations (such as name, telephone number, date of birth, car registration number or simple character strings).

The user shall keep their means of identification secret and protect them against misuse. They may not be handed over to third parties or otherwise made accessible.

If there is reason to believe that a third party has gained access to a means of identification, the user must delete or change the corresponding means of identification immediately. If this is not possible, they must immediately block access to the corresponding services.

3.2 End device and software

The user is obliged to minimise the security risks arising from the use of the respective medium (e.g. Internet, mobile phone) by using suitable, state-of-the-art protective measures (in particular software updates, antivirus programs). Updates provided by the Bank for the mobile app must be installed as soon as they are available.

When using biometric data (e.g. fingerprint or facial recognition) to unlock the mobile app, the user must ensure that they are the only person whose biometric data is stored on the end device.

3.3 Data input

The user must check all the data entered by them for completeness and accuracy. This applies in particular to the scanning and importing of invoices.

If the Bank asks the user to additionally confirm certain orders after they have been entered, the user must check the order information carefully and only confirm it if it matches the data provided for the order. If no confirmation is received, the order in question shall not be executed.

The user must regularly check the status of the orders placed. If they realise that the Bank has not or has only partially executed the order in accordance with the order details, they are obliged to report this to the Bank immediately.

3.4 Consequences of non-compliance with duty of care

Anyone who breaches their duty of care shall bear the resulting loss. If both the Bank and the user have contributed to the occurrence of the loss, the principles of contributory negligence shall determine the extent to which the Bank and the user must

bear the loss. If a loss occurs without the Bank or the user having failed to exercise due care, the loss shall be borne by the party in whose sphere of influence the cause of the harmful act was situated.

4. Security and data protection

The public and private data transmission networks and the user's end device (computer, mobile phone, etc.) are part of the overall system. However, they are outside the Bank's area of control and can become a weak point in the system. The client is aware of the following risks in particular:

- It is possible for a third party to gain undetected access to the user's end device and to take control or manipulate it.
- Even if the transmission is encrypted, the sender and the recipient details are not encrypted. It may therefore be possible for third parties to draw conclusions about an existing banking relationship.
- The encrypted data may be transmitted across borders, even if the sender and recipient are located in Switzerland. Abroad, the data is no longer subject to Swiss bank client confidentiality and Swiss data protection.
- If the user receives information from the Bank via e-mail, text message, etc., this is usually unencrypted.
- When downloading, installing and using apps (e.g. the Bank's mobile app), third parties (e.g. app store operators, network operators) can draw conclusions about the business relationship with the Bank.
- Transmission errors, technical faults and malfunctions, delays, and system interruptions and failures may occur.

Further information on security when using electronic services can be found at sgkb.ch/sicherheit.

The Bank collects personal data about the use of the services and user behaviour (e.g. IP address, location, access time). The information collected can be used for the provision, further development, optimisation and personalisation of the services, as well as to create service and product offers tailored to the user. Further information on the processing of personal data can be found in the Bank's privacy policy, the latest version of which is published at www.sgkb.ch/en/legal-guidelines.

5. Blocking and interruptions

The user may have their access to the services blocked. The Bank is authorised to restrict or block the user's access at any time and without giving reasons.

The Bank has the right to temporarily interrupt the services to prevent security risks, for maintenance work or in the event of disruptions.

No claims can be made against the Bank due to any blocking or interruptions, unless the Bank has failed to exercise due business care.

6. Execution of orders

The processing of an order depends on the technically flawless functioning of the systems, on third-party trading systems and on the Bank's service times. Stock exchange transactions are also dependent on the trading days and trading hours of the relevant stock exchanges. The round-the-clock fulfilment of an order that has been placed may not be possible.

Unless otherwise agreed, transactions in financial instruments that the user orders via e-banking or mobile banking are carried out without advice from the Bank (execution only). Consequently, the Bank does not check whether such transactions correspond to the client's investment objectives, including with regard to their risk sentiment. It also does not check whether the associated investment risks are financially viable for the client and whether the user or client can understand the risks associated with the transaction based on their knowledge and experience. The user or client waives a risk assessment by the Bank.

It is the responsibility of the user to comply with the legal and regulatory provisions applicable to the respective transaction and the respective financial center. The Bank is entitled to reject or cancel orders in the user's financial instruments, for example, if they do not comply with the relevant provisions governing the respective transaction and the respective financial center.

7. Foreign laws / import and export restrictions

The use of services from abroad may be subject to local legal restrictions. The user is responsible for recognising and observing such restrictions. The Bank accepts no liability in this respect.

8. Guarantee

The Bank shall exercise due business care when displaying and transmitting data, information and notifications. It is liable for any direct and immediate loss that it causes through a breach of due business care. Liability for indirect or consequential losses is excluded.

Insofar as the Bank makes data from third parties accessible via the electronic service, it guarantees the careful selection of these third parties. It is not liable for the accuracy, completeness and timeliness of the data. Prices may be displayed with a time delay.

9. Termination

The user or the Bank may terminate the services at any time without notice.

Furthermore, the Bank may terminate access to a service without notice and without special notification, e.g. if the user has not used the service for 18 consecutive months.

10. Changes to the terms and conditions and the services

The Bank reserves the right to change the terms and conditions for electronic services at any time. These are presented to the user for approval when logging in.

The Bank may change, restrict or completely discontinue the services at any time. As far as possible, it shall inform the user of this in good time.

11. Applicable law and place of jurisdiction

All legal relationships between the user and the Bank are subject to Swiss law. The place of jurisdiction is governed by mandatory statutory provisions. Insofar as these do not apply, the exclusive place of jurisdiction for all types of proceedings is St. Gallen. However, the Bank also has the right to take legal action against the user before the competent court or competent authority at the user's domicile or registered office or before any other competent court.