St.Galler Kantonalbank

Conditions applicables aux services électroniques

Version 07.2024

1. Champ d'application

Les présentes conditions s'appliquent à l'utilisation des services électroniques de la Banque cantonale de Saint-Gall SA. Pour le reste, le contrat de base, y compris les documents de base, ainsi que les éventuelles conventions particulières s'appliquent. L'utilisateur reconnaît avoir pris connaissance des documents de base et déclare qu'ils sont contraignants pour lui. La version actuelle des documents de base est publiée sur sgkb.ch/rechtliches.

Des informations sur les services électroniques peuvent être consultées sur sgkb.ch/e-banking.

2. Identification

L'accès aux services électroniques est accordé à toute personne qui s'est légitimée lors de l'utilisation en saisissant les moyens de légitimation valables pour le service correspondant. Toute personne qui s'est légitimée valablement est considérée par la banque comme autorisée à utiliser le service correspondant. La banque peut interroger cette personne légitimée, lui faire disposer de valeurs patrimoniales et recevoir d'elle des ordres et des communications juridiquement contraignantes.

La banque a le droit de refuser l'exécution d'ordres et d'insister pour que l'utilisateur se légitime d'une autre manière (par exemple par signature ou en se présentant personnellement).

La banque informe préalablement l'utilisateur, de manière appropriée, lorsqu'elle change ou adapte les moyens ou procédures de légitimation.

3. Devoirs de diligence

L'utilisateur s'informe des mesures de sécurité nécessaires et prend les dispositions raisonnables. Vous trouverez de plus amples informations sur la sécurité lors de l'utilisation de l'E-Banking et du Mobile Banking sous sgkb.ch/sicherheit.

3.1 Moyens de légitimation

L'utilisateur est tenu de modifier le mot de passe communiqué par la banque immédiatement après l'avoir reçu et régulièrement par la suite. Le mot de passe ne doit pas être composé de combinaisons faciles à trouver (comme le nom, le numéro de téléphone, la date de naissance, la plaque d'immatriculation ou de simples chaînes de caractères).

L'utilisateur garde secrets ses moyens de légitimation et les protège contre toute utilisation abusive. Ils ne doivent pas être remis à des tiers ou rendus accessibles d'une autre manière.

S'il y a lieu de craindre qu'un tiers ait eu accès à un moyen de légitimation, l'utilisateur doit immédiatement supprimer ou modifier le moyen de légitimation en question. Si cela n'est pas possible, il doit immédiatement bloquer l'accès aux services concernés.

3.2 Terminal

L'utilisateur est tenu de minimiser les risques de sécurité découlant de l'utilisation du support concerné (p. ex. Internet, téléphone portable) en mettant en œuvre des mesures de protection appropriées et conformes à l'état actuel de la technique (en particulier les mises à jour de logiciels, les programmes anti-virus).

3.3 Saisie des données

L'utilisateur doit vérifier l'exhaustivité et l'exactitude de toutes les données qu'il a saisies. C'est notamment le cas lors de la numérisation des factures.

Si la banque demande à l'utilisateur de confirmer en plus certains ordres après leur saisie, il doit vérifier soigneusement les informations relatives à l'ordre et ne les confirmer que si elles correspondent aux données prévues pour l'ordre. En l'absence de confirmation, l'ordre concerné ne sera pas exécuté.

L'utilisateur doit vérifier régulièrement le statut des commandes passées. S'il constate que la banque n'a pas exécuté l'ordre ou ne l'a exécuté que partiellement conformément à l'ordre, il est tenu de le signaler immédiatement à la banque.

3.4 Conséquences du non-respect des devoirs de diligence

Celui qui ne respecte pas son devoir de diligence assume les dommages qui en résultent. Si la banque et l'utilisateur ont tous deux contribué à la survenance du dommage, les principes de la faute partagée déterminent dans quelle mesure la banque et l'utilisateur doivent supporter le dommage. Si un dommage survient sans que la banque ou l'utilisateur n'ait manqué de diligence, le dommage est supporté par la partie sous l'influence de laquelle la cause du fait dommageable a été placée.

4. Sécurité et protection des données

Les réseaux publics et privés de transmission de données ainsi que le terminal (ordinateur, téléphone portable, etc.) de l'utilisateur font partie du système global. Ils échappent toutefois au contrôle de la banque et peuvent devenir un point faible du système. Le client est notamment conscient des risques suivants:

- Il est possible qu'un tiers accède au terminal de l'utilisateur à son insu et en prenne le contrôle ou le manipule.
- Même en cas de transmission cryptée, l'expéditeur et le destinataire restent chacun non cryptés. Pour des tiers, il peut donc être possible de tirer des conclusions sur une relation bancaire existante.
- Les données cryptées peuvent être transmises au-delà des frontières, même si l'expéditeur et le destinataire se trouvent en Suisse. A l'étranger, les données ne sont plus soumises au secret bancaire suisse et à la protection des données suisse.
- Si l'utilisateur se fait transmettre des informations de la banque par e-mail, SMS, etc., celles-ci ne sont généralement pas cryptées.
- Lors du téléchargement, de l'installation et de l'utilisation d'applications (p. ex. l'application mobile de la banque), des tiers (p. ex. exploitants des magasins d'applications, opérateurs de réseaux) peuvent tirer des conclusions sur la relation commerciale avec la banque.
- Des erreurs de transmission, des défauts et des pannes techniques, des retards ainsi que des interruptions et des défaillances du système peuvent survenir.

Vous trouverez de plus amples informations sur la sécurité lors de l'utilisation de l'E-Banking et du Mobile Banking sous sgkb.ch/sicherheit. D'autres informations sur le traitement des données personnelles sont contenues dans la déclaration de protection des données de la banque, publiée dans sa version actuelle sur sgkb.ch/rechtliches.

5. Blocages et interruptions

L'utilisateur peut faire bloquer son accès aux services. La banque est en droit de restreindre ou de bloquer l'accès de l'utilisateur à tout moment et sans avoir à se justifier.

La banque a le droit d'interrompre temporairement les services pour se prémunir contre des risques de sécurité, pour des travaux de maintenance ou en cas de perturbations.

Aucune réclamation ne peut être formulée contre la banque en raison d'éventuels blocages ou interruptions, à moins que la banque n'ait pas fait preuve de la diligence requise par les usages commerciaux.

6. Exécution des commandes

Le traitement d'un ordre dépend du bon fonctionnement technique des systèmes, des systèmes de négociation de tiers et des heures de service de la banque. Les transactions boursières dépendent en outre des jours de Bourse et des heures de négoce sur les Bourses concernées. Il se peut donc qu'un ordre donné ne puisse pas être exécuté 24 heures sur 24.

Les transactions en instruments financiers que l'utilisateur ordonne via l'E-Banking ou le Mobile Banking sont effectuées, sauf convention contraire, sans conseil de la banque (execution only). Par conséquent, la banque ne vérifie pas, lors de ces transactions, si elles correspondent aux objectifs de placement du client, y compris en ce qui concerne sa propension au risque. Elle ne vérifie pas non plus si les risques d'investissement qui en découlent sont financièrement supportables pour le client et si les connaissances et l'expérience de l'utilisateur ou du client lui permettent de comprendre les risques inhérents à la transaction. Il renonce à une évaluation des risques par la banque.

Il incombe à l'utilisateur de respecter les dispositions légales ou réglementaires applicables à l'opération et à la place boursière en question. La banque est en droit de refuser ou d'annuler des ordres portant sur des instruments financiers de l'utilisateur, par exemple s'ils ne sont pas conformes aux dispositions pertinentes régissant la transaction et la place boursière concernées.

7. Lois étrangères/restrictions à l'importation et à l'exportation

L'utilisation des services depuis l'étranger peut être soumise à des restrictions légales locales. Il incombe à l'utilisateur de prendre connaissance de ces restrictions et de les respecter. La banque décline toute responsabilité à cet égard.

8. Résiliation

L'utilisateur ou la banque peuvent résilier les services à tout moment sans préavis.
Par ailleurs, la banque peut supprimer l'accès à un service sans avis, par exemple si l'utilisateur n'a pas utilisé le service pendant 18 mois consécutifs.

9. Modifications des conditions et des services

La banque se réserve le droit de modifier à tout moment les conditions applicables aux services électroniques. Elles sont soumises à l'utilisateur pour approbation lors de la connexion.

La banque peut à tout moment modifier, restreindre ou supprimer les services. Dans la mesure du possible, elle en informe l'utilisateur suffisamment tôt.

10. Droit applicable et for compétent

Toutes les relations juridiques que l'utilisateur entretient avec la banque sont soumises au droit suisse. Le for compétent est régi par les dispositions légales contraignantes. Dans la mesure où celles-ci ne sont pas applicables, le for compétent exclusif pour tous les types de procédure est Saint-Gall. La banque a toutefois également le droit de poursuivre en justice l'utilisateur devant le tribunal compétent ou l'autorité compétente pour son lieu de domicile ou son siège social ou devant tout autre tribunal compétent.