Glarner Kantonalbank

Gewöhnliche elektronische Kommunikationswege und Kommunikation über die IT-Infrastruktur der Bank (e-Banking)

Wichtige Bestimmungen, die **besonderer Aufmerksamkeit** bedürfen, sind mit * gekennzeichnet.

1 Geltungsbereich *

Die folgenden Bestimmungen enthalten ergänzende Regeln

a) für die gewöhnlichen elektronischen Kommunikationswege über offene Netze (Fax, E-Mail, Mobiltelefon inkl. SMS, Messenger Services usw.),
b) für das Beziehen und Erbringen von Dienstleistungen über die IT-Infrastruktur der Bank (inkl. Kommunikation über diese IT-Infrastruktur, insbesondere mit SecureMail; e-Banking).

Die Bank kann Näheres über ihre Homepage/Informationsseiten innerhalb der IT-Infrastruktur regeln.

2 Gewöhnliche elektronische Kommunikationswege *

Die Bank geht davon aus, dass sie im verkehrsüblichen Rahmen die gewöhnlichen elektronischen Kommunikationswege benutzen darf. Dabei beachtet sie die Vorsicht, die sie dem Kunden empfiehlt (Allgemeine Bestimmungen zur Geschäftsbeziehung Ziff. 7).

Vorbehalten bleibt der für die Bank gut erkennbare Wille des Kunden,

– entweder auf den empfohlenen Schutz zu verzichten, z. B. durch Aufforderung zur Übermittlung sensitiver Daten auf dem gewöhnlichen elektronischen Kommunikationsweg,
– oder sich besser zu schützen, z. B. durch Kommunikation ausschliesslich über die IT-Infrastruktur der Bank oder die Weisung, E-Mails nur verschlüsselt zu senden; der Absender und der Empfänger verschlüsselter Daten bleiben auch so weiterhin erkennbar.

Daten, die über ein offenes Netz gesandt werden, können im Ausland gespeichert werden, auch wenn sich Sender und Empfänger in der Schweiz befinden. Dem Kunden ist ferner bewusst, dass sich Dritte zu Daten, die auf dem Weg der gewöhnlichen elektronischen Kommunikation (Ziff. 1) übermittelt werden, Zugang verschaffen können.

Die Bank haftet nicht für Nachteile, die dem Kunden aus der Benutzung der gewöhnlichen elektronischen Kommunikationswege entstehen.

3 Kommunikation über die IT-Infrastruktur der Bank

Soweit im Folgenden vom Benutzer die Rede ist, ist der Kunde oder dessen Bevollmächtigter gemeint, der mit der Bank über deren IT-Infrastruktur kommuniziert; soweit im Folgenden von Dienstleistungen die Rede ist, sind Dienstleistungen gemeint, welche dieser Benutzer über die IT-Infrastruktur der Bank beziehen kann.

3.1 Zugang zu den Dienstleistungen

a) Grundsatz

Die Bank öffnet dem Benutzer als Alternative zum Zugang über Post/Telefon einen Zugang über ihre IT-Infrastruktur. Sie schuldet ihm aber diesen Zugang nicht, sondern ist bestrebt, diesen Zugang, so gut es ihr möglich ist, offen bzw. ihre Internet-Plattform betriebsbereit zu halten.

Der Zugang des Benutzers erfolgt (i) mit einem Mobiltelefon und/oder Computer oder einem anderen internetfähigen Endgerät (nachfolgend «Endgerät») unter Einsatz (ii) eines Providers und (iii) einer Software über (iv) ein offenes, jedermann zugängliches Netz (z.B. Internet, Telefonnetz, Kabel usw.; im Folgenden «Netz») zur (v) IT-Infrastruktur der Bank.

Die Bank kann den Zugang zu den Dienstleistungen bzw. den Betrieb der Internet-Plattform jederzeit, insbesondere bei Sicherheitsrisiken, Verdacht der Datenmanipulation oder wegen Wartungsarbeiten, sperren oder unterbrechen.

b) Individuelle Sperre

Die Bank kann dem Benutzer den Zugang zudem sperren, wenn die elektronischen Dienstleistungen während 12 Monaten nicht mehr benutzt worden sind.

Auf Antrag des Benutzers sperrt die Bank den Zugang, sobald der Antrag von der zuständigen Stelle bearbeitet werden kann, was in der Regel während der Geschäftszeiten der Fall ist. Der Benutzer muss diese Weisung unverzüglich schriftlich bestätigen.

3.2 Legitimationsmittel (Selbstlegitimation) *

Zugang zu den jeweiligen Dienstleistungen erhält, wer sich mit den nachfolgend festgelegten Legitimationsmitteln ausweist.

Der Versand dieser Legitimationsmittel erfolgt an die der Bank bekannt gegebene Zustelladresse oder Telefonnummer des Benutzers. Der Benutzer hat die Entgegennahme der Legitimationsmittel sowie deren Verwendung zu überwachen. Das Risiko, dass eine unberechtigte Person die Legitimationsmittel verwendet, trägt er.

Als Legitimationsmittel gelten:

a) die dem Benutzer von der Bank zugestellte Vertragsnummer (erstes Identifikationsmerkmal),
b) sein persönliches, selbst wählbares Passwort (zweites Identifikationsmerkmal) und
c) je nach Wahl des Kommunikationsmittels
   – der SMS-Code, der dem Benutzer nach Eingabe der ersten zwei Identifikationsmerkmale übermittelt wird, oder
   – das Mosaikbild, das mittels – auf dem mobilen Endgerät (Smartphone, Tablet o. ä.) – installierter CrontoSign Swiss App oder eines von der Bank zugelassenen Lesegerätes entschlüsselt wird (drittes Identifikationsmerkmal).

Die Bank ist nicht zu einer weitergehenden Prüfung der Berechtigung verpflichtet. Sie hat aber jederzeit und ohne Angabe von Gründen das Recht, einen weitergehenden Nachweis der Berechtigung zu verlangen (z. B. durch Unterschrift, persönliche Vorsprache oder durch Transaktionsbestätigung bei Legitimationsmitteln, welche diese Option kennen) und Aufträge nicht auszuführen, solange dieser Nachweis nicht geleistet ist.

Glarner Kantonalbank

3.3 Gebotene Sorgfalt beim Umgang mit Legitimationsmitteln *

Der Benutzer hat das erste ihm von der Bank mitgeteilte Passwort (zweites Identifikationsmerkmal) unverzüglich nach Erhalt und später regelmässig zu ändern. Das Passwort darf nicht aus leicht ermittelbaren Kombinationen (wie Telefonnummer, Geburtsdatum, Autokennzeichen usw.) bestehen.

Der Benutzer hat das zweite und das dritte Identifikationsmerkmal voneinander getrennt aufzubewahren, geheim zu halten und gegen missbräuchliche Verwendung durch Unbefugte zu schützen. Insbesondere dürfen weder das zweite noch das dritte Identifikationsmerkmal ungeschützt auf dem Endgerät des Benutzers (z. B. Computer oder Mobiltelefon) abgelegt oder sonst wo aufgezeichnet werden. Ebenso wenig dürfen das zweite bzw. das dritte Identifikationsmerkmal Dritten ausgehändigt oder sonst zugänglich gemacht werden.

Muss der Benutzer befürchten, dass unberechtigte Dritte Kenntnis eines oder mehrerer Legitimationsmittel des Benutzers gewonnen haben, so hat er das entsprechende Legitimationsmittel unverzüglich zu wechseln bzw. zu ändern. Ist dies nicht möglich, hat er den Zugang zu den entsprechenden Dienstleistungen unverzüglich sperren zu lassen oder durch dreimalige Eingabe eines falschen Passwortes oder eines falschen Sicherheitscodes selbst zu sperren.

Bei Benutzung der CrontoSign Swiss App dürfen keine vom Software-Hersteller verbotenen Betriebssystemänderungen (z. B. Jailbreak, Rooting o. ä.) vorgenommen werden. Ausserdem ist der Bezug der CrontoSign Swiss App nur aus den vom Software-Hersteller offiziell anerkannten App-Stores erlaubt.

3.4 Schutzpflichten der Bank

Die Bank verpflichtet sich, zum Schutz des Benutzers ihre IT-Infrastruktur angemessen zu sichern und für die Nutzung der Dienstleistungen angemessene Sicherheitsmassnahmen einzusetzen, um das Risiko der Manipulation und der unbefugten Einsichtnahme gering zu halten. Was angemessen ist, ist nach dem Schutz zu beurteilen, den vergleichbare Banken üblicherweise bieten.

Dessen ungeachtet kann die Bank dem Benutzer Folgendes nicht zusichern:

- den steten Zugang zur IT-Infrastruktur (bzw. zu den Dienstleistungen) und das richtige Funktionieren der IT-Infrastruktur,
- die Unverletzlichkeit der IT-Infrastruktur gegen Eingriffe Dritter, insbesondere durch unbefugte Einsichtnahme oder Manipulation von Daten.

3.5 Sorgfalt, die der Benutzer im eigenen Interesse beachten muss *

Es obliegt dem Benutzer,

- die von ihm zur Übermittlung bestimmten Daten auf Vollständigkeit und Richtigkeit hin zu überprüfen,
- die Ausführung von Aufträgen, die er der Bank erteilt hat, zu prüfen und eventuelle Beanstandungen zu erheben, beides so zeitnah, dass ein Schaden vermieden oder möglichst klein gehalten werden kann (siehe dazu auch Allgemeine Bestimmungen zur Geschäftsbeziehung Ziff. 4),
- zu plausibilisieren, ob die Daten, die er von der Bank zu Konten oder Depots erhält (Kurse, Saldi, Auszüge), stimmen,
- zu prüfen, ob allgemein zugängliche Daten (Preise, Kurse), die er von der Bank erhält, stimmen, es sei denn, die Bank sichere die Verlässlichkeit dieser Daten explizit zu,
- sich genügende Systemkenntnisse zu verschaffen (z. B. um Daten nicht ungeschützt auf der Festplatte zu speichern),
- Endgerät, Provider und Software, die er für den Zugang zu den Dienstleistungen nutzt, sorgfältig auszuwählen, und insbesondere nur Software aus vertrauenswürdigen Quellen und virenfreie Datenträger (USB-Sticks) zu verwenden,
- Sicherheitsrisiken generell zu minimieren, z. B. indem er die auf den Internetseiten der jeweiligen Dienstleister angebrachten oder ihm sonst zugänglichen Sicherheitsinformationen (auch solche der Bank auf ihrer Homepage) beachtet, sich auf dem aktuellen Stand der Technik hält und empfohlene Sicherheitsmassnahmen innert nützlicher Frist trifft (z. B. wirksame Antiviren- und Firewall-Programme einrichtet und erneuert und sein Passwort regelmässig wechselt).

3.6 Risikobereiche und Haftung *

Sofern der Zugang zu den Dienstleistungen möglich ist (Ziff. 3.1), ist ihre Beanspruchung im Wesentlichen mit folgenden Risiken verbunden, die den Parteien wie folgt zugeordnet sind:

a) Risikobereich des Benutzers
   - Die IT-Umgebung des Benutzers wird beschädigt, von Dritten eingesehen oder benutzt, oder Daten, die übermittelt werden sollen, werden auf der IT-Umgebung des Benutzers von Dritten manipuliert.

b) Risikobereich der Bank
   - Die bei der Bank abgerufenen Daten sind nicht richtig.
   - Die IT-Infrastruktur der Bank wird von Dritten eingesehen, oder Daten, die übermittelt werden sollen, werden auf der IT-Infrastruktur der Bank von Dritten manipuliert.

c) Gemeinsamer Risikobereich
   - Die von einer Partei übermittelten Daten werden ausserhalb der jeweiligen IT-Umgebung der Parteien von Dritten eingesehen oder manipuliert.

Schaden, den eine Partei aus Umständen erleidet, die in ihrem eigenen oder im gemeinsamen Risikobereich liegen, trägt diese Partei selbst. Schaden, den eine Partei aus Umständen erleidet, die im Risikobereich der anderen Partei liegen, hat die andere Partei nur zu ersetzen, soweit sie ihre Schutzpflicht erheblich verletzt hat (mehr als nur leichtes Verschulden) und dadurch zum Schaden massgeblich beigetragen hat.

Für Schäden, welche die fordernde Partei durch den Einsatz angemessener Schutzmassnahmen (Geheimhaltung von Passwörtern, Verwenden von angemessenen Antiviren- und Firewall-Programmen inkl. Aktualisierung ihrer IT-Umgebung usw.) hätte vermeiden können, haftet die andere Partei nicht.

Daher haftet die Bank nicht, wenn

- mangels Zugang zu den Dienstleistungen Aufträge nicht rechtzeitig ausgeführt werden können,
- sie Zahlungsaufträge ausführt, die im Risikobereich des Benutzers oder im gemeinsamen Risikobereich manipuliert worden sind,
- der Benutzer für Börsenaufträge auf unrichtige und von der Bank nicht garantierte Kurse abstellt, ohne diese überprüft zu haben.

Glarner Kantonalbank

3.7 Vollmachten

Der Kunde kann neben der gewöhnlichen Vollmacht (d. h. der Vollmacht für nicht elektronische Dienstleistungen) eine spezielle Vollmacht (d. h. eine Vollmacht zur Benutzung der elektronischen Dienstleistungen) erteilen.

Die spezielle Vollmacht gilt bis zum schriftlichen Widerruf; sie erlischt weder mit dem Tod noch dem Verlust der Handlungsfähigkeit. Der Widerruf der gewöhnlichen Vollmacht gilt nicht als Widerruf der speziellen Vollmacht; der Kunde muss auch die spezielle Vollmacht explizit widerrufen.

Die Bank haftet nicht für Schaden, der dem Kunden aus mangelnder Handlungsfähigkeit seiner Person oder seiner Bevollmächtigten entsteht.

Die Bank muss eine Vollmacht nicht beachten, wenn sie eine Gefährdung der Interessen des Vollmachtgebers nicht ausschliessen kann.

3.8 Ausländische Gesetze/Import- und Exportbeschränkungen *

Der Benutzer nimmt zur Kenntnis, dass er mit der Benutzung der Dienstleistungen aus dem Ausland unter Umständen Regeln des ausländischen Rechts verletzen kann. Es ist Sache des Benutzers, sich darüber zu informieren. Die Bank lehnt diesbezüglich jede Haftung ab.

Sollte der Benutzer die Dienstleistungen vom Ausland aus benutzen, nimmt er insbesondere in Kauf, dass es Import- und Exportbeschränkungen für die Verschlüsselungsalgorithmen geben kann, gegen die er gegebenenfalls verstösst.

3.9 Kündigung

Bank und Benutzer können die Teilnahme an den jeweiligen Dienstleistungen jederzeit beenden. Die Kündigung ist schriftlich an die jeweils andere Partei zu richten.

3.10 Leistungsangebot *

Die jeweils von der Bank angebotenen Dienstleistungen sind auf den entsprechenden Internetseiten der Bank umschrieben.

Die Bank behält sich jederzeitige Änderungen des Leistungsangebotes vor. Sie informiert den Benutzer in geeigneter Weise.

3.11 Datenübermittlung bei auf SMS basierenden Dienstleistungen *

Beansprucht der Benutzer eine auf SMS basierende Dienstleistung (z. B. im Rahmen des Legitimationsverfahrens SMS-Code), nimmt er zur Kenntnis und erklärt sich damit einverstanden, dass die Bank die vom Benutzer ausgewählte Telefonnummer und die an ihn zu übertragenden Daten an die für den SMS-Versand notwendigen und in der Schweiz domizilierten Telekommunikationsunternehmen weiterleitet.

3.12 Börsenaufträge *

Börsenaufträge, die der Benutzer via Internet-Banking erteilt (im Folgenden «INBA-Börsenaufträge»), können nicht rund um die Uhr ausgeführt werden.

Erteilt der Benutzer INBA-Börsenaufträge, hat er die einschlägigen Normen, die für das jeweilige Geschäft und den jeweiligen Börsenplatz gelten, einzuhalten. Die Bank schuldet ihm hierbei weder Beratung noch Aufklärung, sondern beschränkt sich auf die Ausführung. Der Benutzer hat sich selbst zu vergewissern, dass er mit den Gepflogenheiten und Usanzen des

Börsengeschäftes vertraut ist, insbesondere die Strukturen und Risiken der einzelnen Geschäftsarten kennt.

Ohne die Verantwortung des Benutzers gemäss vorstehendem Absatz einzuschränken, ist die Bank berechtigt, Börsenaufträge zurückzuweisen oder zu stornieren, sofern diese mit den eben erwähnten einschlägigen Normen nicht in Einklang stehen.

Der Benutzer verpflichtet sich, die jeweils gültige Broschüre «Besondere Risiken im Effektenhandel» sowie die in den Dienstleistungen des Internet-Banking enthaltenen Risikoinformationen zu konsultieren.

Aus Gründen der besseren Lesbarkeit verwendet die Glarner Kantonalbank nur die männlichen Formen.