REICHMUTH & CO
PRIVATBANKIERS

Sicherheits- und Nutzungsbestimmungen für e-Connect

Version: 10. Mai 2023

1. Sicherheits- und Nutzungsbestimmungen für e-Connect

Mit diesen Sicherheits- und Nutzungsbestimmungen werden zwischen Kunden bzw. den Bevollmächtigten von Bankbeziehungen eines Kunden (nachfolgend gemeinsam „Vertragspartner“) und Reichmuth & Co („die Bank“) die Modalitäten des Zugriffs auf e-Connect geregelt. Der Zugriffsberechtigte ist der eigentliche Benutzer von e-Connect, als Vertragspartner oder von diesem bevollmächtigten Benutzer (nachfolgend gemeinsam „Zugriffsberechtigte“). Der Vertragspartner trägt die umfassende Verantwortung dafür, dass die von ihm bestimmten Zugriffsberechtigten die hierin enthaltenen Pflichten vollumfänglich beachten. **Der Bevollmächtigte von Bankbeziehungen eines Kunden ist zudem verpflichtet, das Einverständnis des Kunden zum Abschluss dieser Vereinbarung einzuholen sowie ihn insbesondere über die damit verbunden Risiken zu informieren.**

„EDV-System“ umfasst nachstehend jeweils Hardware und Software, inkl. mobile Endgeräte, Festnetz- und Mobiltelefone sowie weitere technische Hilfsmittel für die Verwendung der persönlichen Legitimationsmittel.

1.1 Persönliche Legitimationsmittel und Anleitung

Die Bank stellt den Zugriffsberechtigten die persönlichen Legitimationsmittel nur zum bestimmungsgemässen Gebrauch zur Verfügung. Der Zugriff auf e-Connect und die damit angebotenen Dienstleistungen erfolgen, nachdem der Zugriffsberechtigte sich unter Gebrauch der persönlichen Legitimationsmittel (Vertragsnummer, Passwort, SMS Authentifizierung) gegenüber der Bank legitimiert hat. Die Anleitung/Hilfe beschreibt die korrekte Verwendung der persönlichen Legitimationsmittel zum Nachweis der Zugriffsberechtigung und ist auf der Webseite der Bank verfügbar. Nach Erhalt der Anleitung/Hilfe wird diese mit dem ersten Einsatz der persönlichen Legitimationsmittel als verbindlich anerkannt (vgl. Ziff. 1.2). Die Bank kann die persönlichen Legitimationsmittel jederzeit austauschen oder anpassen.

1.2 Legitimation

Benützt der Zugriffsberechtigte eine Dienstleistung via e-Connect, so erfolgt die Identifikation durch die Bank nicht anhand einer Unterschriften- oder Ausweisprüfung. Die Legitimationsprüfung findet allein anhand der zur Verfügung gestellten, persönlichen Legitimationsmittel (Ziff. 1.1) statt (Selbstlegitimation).

Jede Person, die sich mit den persönlichen Legitimationsmitteln und dem in der „Anleitung/Hilfe“ beschriebenen Legitimationsverfahren erfolgreich Zugang zu e-Connect verschafft (Selbstlegitimation), gilt der Bank gegenüber als zugriffsberechtigt; dies gilt unabhängig davon, ob es sich bei dieser Person tatsächlich um den Zugriffsberechtigten handelt bzw. diese vom Vertragspartner entsprechend autorisiert wurde.

Die Bank gilt als beauftragt und ermächtigt, die bei ihr über e-Connect eingehenden Aufträge auszuführen sowie den Instruktionen und Mitteilungen nachzukommen, sobald ihnen eine korrekte Legitimationsprüfung zugrunde liegt; diese gelten als vom Zugriffsberechtigten verfasst. Die Bank ist somit ihren Verpflichtungen nachgekommen, wenn sie den bei ihr eingehenden Aufträgen, Instruktionen und Mitteilungen im Rahmen des üblichen Geschäftsgangs Folge leistet.

1.3 Sorgfaltspflicht

a) Der Zugriffsberechtigte ist verpflichtet, die persönlichen Legitimationsmittel besonders sorgfältig und voneinander getrennt aufzubewahren. Diese dürfen keinesfalls weitergegeben oder in einer anderen Weise einer anderen Person zugänglich gemacht werden. Passwörter sind unverzüglich nach Erhalt zu ändern (10-14 Zeichen lang, Grossbuchstaben, Kleinbuchstaben und Zahl sowie Sonderzeichen) und geheim zu halten. Passwörter dürfen weder notiert, noch elektronisch gespeichert werden. Passwörter dürfen nicht leicht ermittelbar sein (keine Telefonnummern, Geburtsdaten, Autokennzeichen, einfach ermittelbare Zahlenfolgen usw.)

b) Auf E-Mails, die angeblich von der Bank stammen und zur Bekanntgabe von persönlichen Legitimationsmitteln auffordern (z.B. durch Eingabe auf Webseiten, die via Link aufgerufen werden können), darf nicht reagiert werden. Die Bank ist umgehend darüber zu informieren. Besteht Grund zur Annahme, dass eine andere Person von Passwort Kenntnis erhalten hat, muss der Zugriffsberechtigte diese unverzüglich ändern. Bei Verlust Ihres Mobiletelefons, Wechsel Ihrer Telefonnummer oder Kündigung Ihres Abonnements, ist die Bank sofort

zu benachrichtigen. Die Bank empfiehlt das Mobiltelefon mittels Sperre vor unerlaubtem Zugriff zu schützen.

c) Wird via Internet oder anderen elektronischen Netzwerken mit e-Connect Verbindung aufgenommen, ist der Zugriffsberechtigte zwecks Bekämpfung von Irrtümern und Missbräuchen verpflichtet, die Richtigkeit der angewählten Bankadresse und die Echtheit des zugehörigen Bank-Server-Zertifikats zu verifizieren, sofern dies nicht von den für die Anmeldung (Login) eingesetzten persönlichen Legitimationsmitteln bereits automatisch ausgeführt wird (nähere Angaben dazu finden sich in der „Anleitung/Hilfe"). Bei Unregelmässigkeiten darf keine Anmeldung (Login) erfolgen bzw. ist die Verbindung umgehend abzubrechen und die Bank zu kontaktieren. Die persönlichen Legitimationsmittel sind ausschliesslich an die Bank zu übermitteln. Die Anmeldung (Login) hat immer nur auf der Webseite der Bank zu erfolgen und nie auf einer Webseite eines Drittanbieters.

d) Es ist möglich, dass sich unberechtigte Dritte unbemerkt Zugang zum EDV-System des Zugriffsberechtigten zu verschaffen versuchen (u.a. auch mit elektronischen Wartungstools etc.). Deshalb ist der Zugriffsberechtigte verpflichtet, die üblichen Schutzmassnahmen zu treffen, um bestehende Sicherheitsrisiken (z.B. die Risiken in öffentlichen elektronischen Netzwerken wie dem Internet) zu minimieren. Insbesondere Betriebssystem und Browser sind aktuell zu halten. D.h. die von den jeweiligen Anbietern zur Verfügung gestellten und empfohlenen Sicherheitskorrekturen (Patches) sind vom Zugriffsberechtigten zu installieren. Die für öffentliche elektronische Netzwerke üblichen Sicherheitsvorkehrungen sind zu treffen (z.B. durch Installation einer Firewall und den Einsatz eines Anti-Virusprogrammes, die laufend aktualisiert werden). Es ist die Verantwortung des Zugriffsberechtigten, sich über die erforderlichen Sicherheitsvorkehrungen genau zu informieren und diesen nachzukommen. Ausserdem ist der Zugriffsberechtigte verpflichtet, die notwendigen Vorkehrungen zur Sicherheit allfälliger auf seinem EDV-System gespeicherter Daten zu treffen.

e) Zur Erhöhung der Sicherheit kann der Zugriffsberechtigte bei der Erteilung von Aufträgen aufgefordert werden, ausgewählte Transaktionsdaten, wie z.B. den Begünstigten, oder die ganze Transaktion zu bestätigen. In diesem Fall ist der Zugriffsberechtigte verpflichtet, die zur Bestätigung angezeigten Informationen entsprechend der ihm ursprünglich (physisch) vorliegenden Auftragsinstruktion, d.h. unabhängig von den in e-Connect angezeigten Informationen, auf Richtigkeit zu überprüfen, und sofern korrekt, mit Hilfe der persönlichen Legitimationsmittel zu bestätigen. Die korrekte und sorgfältige Ausführung der
Bestätigung liegt in der alleinigen Verantwortung des Zugriffsberechtigten. Die Bank kann die vorhandenen Schutzmechanismen jederzeit anpassen sowie neue einführen.

f) Der Vertragspartner trägt die umfassende Verantwortung dafür, dass die von ihm bestimmten Zugriffsberechtigten die vorstehenden Pflichten vollumfänglich beachten.

1.4 Zahlungsverkehr

a) Die Bank ist vom Vertragspartner beauftragt, die bei ihr über e-Connect eingehenden Aufträge auszuführen sowie den Instruktionen und Mitteilungen nachzukommen, falls die systemgemässe Legitimationsprüfung nach Ziffer 1.2 erfolgt ist. Werden der Bank mit e-Connect Aufträge erteilt, so ist sie berechtigt, einzelne Aufträge nach ihrem freiem Ermessen abzulehnen, falls für diese ein freies Guthaben oder eine werthaltige Sicherheit fehlt oder der Rahmen der verfügbaren Kreditlimiten überschritten ist.
b) Liegen mehrere Zahlungsaufträge vor, deren Gesamtbetrag das verfügbare Guthaben oder den gewährten Kredit übersteigt, so werden diese an dem jeweiligen gewünschten Ausführungsdatum, und nur soweit Deckung vorhanden ist, ausgeführt.
c) Die Bank kann einen Zahlungsauftrag trotz fehlendem Guthaben im Interesse des Kunden ausführen.
d) Ohne Angabe bzw. bei Angabe eines unmöglichen, zu kurzfristigen oder unlogischen Ausführungsdatums gilt die Bank als ermächtigt, den Zahlungsauftrag nach dessen bankseitiger Erfassung auszuführen, sofern die sonstige Voraussetzung gemäss Buchstabe a) erfüllt ist. Fällt das vom Kunden bzw. Bevollmächtigten gemäss Zahlungsauftrag vorgegebene Ausführungsdatum auf einen Samstag, Sonntag oder Feiertag, so gilt als Ausführungsdatum der nächstfolgende Werktag.
e) Die korrekte Abwicklung des elektronischen Zahlungsverkehrs über e-Connect ist Sache des Kunden bzw. Bevollmächtigten.

1.5 Risiken

Die Legitimationsabrede (Ziff. 1.2) bedeutet, dass die Risiken beim Zugriffsberechtigten liegen, die sich (i) aus Manipulation an dessen EDV-System durch Unbe-

fugte, (ii) aus missbräuchlicher Verwendung der persönlichen Legitimationsmittel, (iii) aus Verletzung von Sorgfaltspflichten oder (iv) aus Eingriffen unberechtigter Dritter in die Datenübermittlung ergeben.

Der Zugriffsberechtigte ist sich der Risiken bezüglich des Informations- und Datenaustauschs über öffentliche und private Datenübermittlungsnetze bewusst. Es ist möglich, dass gezielte Manipulationen am EDV-System des Zugriffsberechtigten durch Unbefugte nicht ausgeschlossen werden kann. Die Gefahr solcher Manipulationen fällt in den Einflussbereich des Kunden, der die entsprechenden Risiken dafür zu tragen hat.

1.6 Sperre

Jeder Zugriffsberechtigte kann den Zugang zu e-Connect bei einer von der Bank bekanntgegebenen Stelle während den Geschäftszeiten sperren lassen. Zusätzlich kann er seinen Zugang (bzw. seine Legitimation) selber sperren, indem er sein Legitimationsmittel zur betreffenden Dienstleitung so oft falsch einsetzt, bis das System die Sperre anzeigt (z.B. durch wiederholte Eingabe eines falschen Passwortes oder Codes).

Der Zugriffsberechtige trägt das Risiko von Einsätzen der persönlichen Legitimationsmittel vor Wirksamwerden der Sperre innert geschäftsüblicher Frist.

1.7 Länderspezifische Schranken, ausländische Import- und Exportbeschränkungen

Das Angebot von Finanzdienstleistungen für Zugriffsberechtigte im Ausland kann lokalen rechtlichen Restriktionen unterliegen. Verfügt die Bank nicht über die notwendigen lokalen Bewilligungen, muss der Umfang der Dienstleistungen für Zugriffsberechtigte jenes Landes eingeschränkt werden. Diese Beschränkungen unterliegen einem laufenden Wandel der Rechtsentwicklung und des regulatorischen Umfeldes jedes Landes. Die Bank ist berechtigt, den Umfang der zur Verfügung stehenden Dienstleistungen jederzeit und ohne vorgängige Anzeige anzupassen bzw. zu beschränken.

Die von der Bank überlassenen persönlichen Legitimationsmittel können spezifische Import-/Export- sowie Nutzungsrestriktionen unterliegen. Zudem kann der Import/Export und der Gebrauch der persönlichen Legitimationsmittel durch den Zugriffsberechtigten in Drittländer(n) zusätzlichen länderspezifischen Gesetzen unterliegen. Die Kenntnis und Beachtung obliegen dem Zugriffsberechtigten. Die Bank lehnt diesbezüglich jede Haftung ab.

1.8 Übermittlungsfehler, technische Störungen, Betriebsausfälle und rechtswidrige Eingriffe

Für die durch Übermittlungsfehler, Fehlleitungen, technische Mängel und Störungen, Betriebsausfälle oder rechtswidrige Eingriffe in EDV-Systeme des Zugriffsberechtigen oder eines Dritten (inkl. jedermann zugänglicher Systeme und Übermittlungsnetze) verursachten Schäden, übernimmt die Bank keine Haftung, es sei denn, die Bank habe die geschäftsübliche Sorgfalt verletzt. Solange die Bank die geschäftsübliche Sorgfalt wahrnimmt, übernimmt die Bank keine Gewähr für störungsfreien, jederzeit ununterbrochenen Zugang zu ihren Dienstleistungen. Damit entfällt auch jede Haftung für Schäden infolge Störung, Unterbrüchen (inkl. systembedingter Wartungsarbeiten) oder Überlastung von Automaten bzw. EDV-Systemen der Bank.

1.9 Vollmachtsbestimmungen

Bevollmächtigter im Sinne dieser Vereinbarung ist, wer eine schriftliche Vollmacht auf einem Vollmachtsdokument der Bank erhalten hat. Zugriffsberechtigungen bzw. persönliche Legitimationsmittel werden nicht automatisch ungültig; z.B. durch Tod, Handlungsunfähigkeit, Streichung der Zeichnungsbefugnis oder Löschung aus einem Register. Unabhängig davon muss die Sperre der Zugriffsberechtigung bzw. der persönlichen Legitimationsmittel immer ausdrücklich durch den Kunden/seine Rechtsnachfolger/die Zugriffsberechtigten angeordnet werden.

1.10 Bankgeheimnis/Datenschutz, Marketing

Das schweizerische Recht (z.B. zum Bankgeheimnis, Datenschutz) beschränkt sich allein auf schweizerisches Territorium. Somit verlieren alle ins Ausland gelangenden Daten den Schutz nach schweizerischem Recht. Der Vertragspartner nimmt in Kauf, dass die Daten über ein offenes, jedermann zugängliches Netz transportiert werden. Dabei können die Daten unkontrolliert grenzüberschreitend übermittelt werden, auch wenn sich Sender und Empfänger in der Schweiz befinden. Ebenso nimmt der Vertragspartner in Kauf, dass Informationen der Bank, welche sich der Benutzer separat via E-Mail, SMS etc. (Legitimationsverfahren, Alert Funktionen) übermitteln lässt, in der Regel unverschlüsselt erfolgen, weshalb das Bankgeheimnis nicht gewahrt ist. Selbst bei verschlüsselter Uebermittlung bleiben Absender und Empfänger jeweils unverschlüsselt. Der Rückschluss auf eine bestehende Bankbeziehung kann deshalb für Dritte möglich sein.

1.11 Änderungen der Bestimmungen

Der Bank steht in begründeten Fällen das Recht zu, die vorliegenden „Sicherheits- und Nutzungsbestimmungen“, die „Anleitung/Hilfe“, allfällige Zusatzvereinbarungen oder besondere Bestimmungen zu den einzelnen Dienstleistungen jederzeit zu ändern. Dabei obliegt es der Bank, die Änderungen vorgängig, schriftlich, elektronisch am Bildschirm, auf dem Zirkularweg oder in anderer geeigneter Weise bekannt zu geben. Ohne schriftlichen Wiederspruch innert Monatsfrist seit Bekanntgabe, auf jeden Fall aber mit dem nächsten Einsatz der persönlichen Legitimationsmittel, gelten die Änderungen als genehmigt. Im Widerspruchsfall steht es dem Kunden frei, die betroffene Dienstleistung vor Inkrafttreten der Änderungen mit sofortiger Wirkung zu kündigen, falls der Kunde sich mit der Bank bis zu jenem Zeitpunkt nicht anderweitig einigen kann.

1.12 Kündigung

Eine Kündigung einzelner oder sämtlicher e-Connect Dienstleistungen kann jederzeit sowohl durch den Zugriffsberechtigten als auch durch die Bank erfolgen. Nach vollständiger Kündigung von e-Connect sind die überlassenen persönlichen Legitimationsmittel (z.B. Vertragsnummer, Passwort) unbrauchbar/unleserlich zu machen und der Bank unaufgefordert und unverzüglich zurückzugeben.

Die Bank bleibt trotz Kündigung berechtigt, sämtliche noch vor Rückgabe der persönlichen Legitimationsmittel ausgelösten Transaktionen rechtsverbindlich für den Vertragspartner zu verarbeiten. Zudem ist die Bank jederzeit berechtigt, einzelne Dienstleistungen fristlos und ohne Anzeige an den Zugriffsberechtigten zu kündigen, sobald sie während mehr als zwei Jahren nicht mehr benutzt wurde.

1.13 Leistungen der Bank

Die elektronischen Dienstleistungen werden von der Bank im Rahmen ihrer Möglichkeiten und ohne Gewähr angeboten. Technischen Support bietet die Bank ausschliesslich während den Geschäftszeiten. Ein unterbruchsfreier oder fehlerfreier Zugang kann nicht gewährleistet werden. Ebenso sind jederzeit zeitliche Verzögerungen bei der Datenübermittlung möglich. Die Bank ist sodann jederzeit berechtigt, die elektronischen Dienstleistungen aus Wartungsgründen zu unterbrechen. Die Bank wählt ihre Dienstleister mit der branchenüblichen Sorgfalt aus. Sie trägt aber keine Verantwortung dafür, dass die von ihr beauftragten Dienstleister ihr stets die korrekten Daten übermitteln (z.B. Börsen- und Devisenkurse) oder die von ihr bereitgestellten Daten zeitgerecht und fehlerfrei an die Zugangs-EDV des Kunden übermitteln.

1.14 Haftung der Bank

Die Bank haftet nicht für Schäden des Kunden aus Pflichtverletzungen im Zusammenhang mit elektronischen Dienstleistungen. Die Haftung für indirekte Schäden und Folgeschäden wie entgangener Gewinn, Ansprüche Dritter oder Schäden, die aus der Nichterfüllung vertraglicher Pflichten des Kunden entstehen, wird ausgeschlossen.