BEDINGUNGEN FÜR VOLKSBANK ELECTRONIC-BANKING (INTERNETBANKING)
Fassung November 2018

A. Allgemeine Bestimmungen

1. Zweck

Electronic-Banking ermöglicht für entsprechend definierte Konten die Durchführung von Bankgeschäften, insbesondere von Zahlungs- und Wertpapieraufträgen und Konto-/Depotabfragen und dient ferner der Übermittlung von Informationen und Willenserklärungen.

2. Leistungsumfang

Im Electronic-Banking hat der Kunde je nach Vereinbarung die Möglichkeit, Abfragen zu tätigen (z.B. Kontostände, Kontoumsätze, etc.), Aufträge zu erteilen (z.B. Zahlungsaufträge, Wertpapierorders, etc.) und rechtsverbindliche Willenserklärungen abzugeben (z.B. Produkteröffnungen, etc.).

Die Verwendung von Electronic-Banking (außer über Kontoinformations- oder Zahlungsauslösedienstleister) ist nur in Verbindung mit Betriebssystemen und Browsern möglich, die durch den jeweiligen Hersteller mit Sicherheitspatches versorgt werden und die die für einen einwandfreien und sicheren Betrieb benötigten Technologien unterstützen.

3. Abwicklung

Die Berechtigung zur Disposition über Electronic-Banking kann nur Kontoinhabern oder Zeichnungsberechtigten erteilt werden. Diese Personen werden im Folgenden als „Nutzer“ bezeichnet. Darüber hinaus kann der Kontoinhaber weitere Personen als lediglich ansichtsberechtigt, also ohne Dispositionsmöglichkeit, bestimmen („Ansichtsberechtigte“).

Im Rahmen von Electronic-Banking übermittelt der Nutzer der Bank Aufträge über ein Datenübertragungsnetz.

4. Einstieg/Zugang und Aufträge (Zugriffsberechtigung)

Zugang zu einem Konto im Rahmen von Electronic-Banking erhalten nur Kunden, die sich durch Eingabe ihrer persönlichen Identifikationsmerkmale (z.B. Benutzername, Passwort) legitimiert haben. Zusätzlich kann die Bank alternative Login Verfahren bereitstellen (z.B. Einmalpasswort oder biometrische Verfahren).

Auf mobilen Endgeräten ist auch ein Zugriff mittels vereinfachter Authentifizierung (Gerätebindung in Kombination mit nutzerspezifischen vierstelliger Quick-ID und/oder biometrischer Authentifizierung) möglich. Dabei kann der Funktionsumfang auf eine reine Ansichtsberechtigung (keine Dispositionsmöglichkeit) eingeschränkt sein.

Für Dispositionen und rechtsverbindliche Willenserklärungen hat sich der Nutzer durch Eingabe seiner persönlichen Identifikationsmerkmale zu legitimieren und zusätzlich gemäß dem gewählten Autorisierungsverfahren (zB smartLogin App) als berechtigt auszuweisen. Die Berechtigung zur Ansicht bzw zur Vornahme von Dispositionen wird von der Bank nur aufgrund der persönlichen Identifikationsmerkmale und eines Einmal-Passworts überprüft. Erfordert das Electronic-Banking das Zusammenwirken mehrerer Nutzer, muss die Autorisierung jeweils von den gemeinsam berechtigten Nutzern gesondert, jedoch innerhalb eines Zeitraumes von 60 Tagen veranlasst werden. Bei gemeinsamer (kollektiver) Zeichnung ist die Nutzung von Teilbereichen des Electronic-Banking (z.B. eps Online-Überweisung) nicht möglich.

Die Bank ist berechtigt, das Verfahren der Zugriffsberechtigung und/oder Autorisierungsberechtigung nach vorheriger Mitteilung an den Nutzer oder Ansichtsberechtigten abzuändern.

Die Zustellung persönlicher Identifikationsmerkmale erfolgt entweder durch Übergabe am Schalter oder durch Postversand. Bei Office Banking sind Zugangsdaten für Konten bei anderen Banken bei diesen Banken gesondert zu beantragen.

4.1. SmartLogin App

Die Übermittlung der für den Zugang und die Autorisierung von Aufträgen erforderlichen Transaktionsnummern erfolgt an eine App, die von der Bank zur Verfügung gestellt wird. Jedes Endgerät auf dem die App installiert ist muss dem Nutzer nach Installation der Anwendung zugeordnet werden (= Herstellung der Gerätebindung). Die Authentifizierung erfolgt mittels Gerätebindung und persönlicher Identifikationsnummer = Quick-ID oder ein biometrisches Verfahren. Der Nutzer kann die Gerätebindung und seine persönliche Quick ID direkt im Electronic-Banking ändern.

Zu Kontrollzwecken werden im Zuge der Freigabe auch Angaben über die durchzuführenden Aufträge, insbesondere Empfänger-IBAN und Betrag oder ein Referenzcode (Elektronischer Begleitzettel) und Kontrollwert (Summe aller Aufträge), mitgeliefert.

Der Nutzer ist verpflichtet, diese auf Übereinstimmung mit den im Electronic-Banking eingegebenen Aufträgen zu prüfen. Die Freigabe darf nur bei Übereinstimmung erteilt werden.

4.3. mobileTAN

Beim mobileTAN-Verfahren hat der Nutzer eine Mobiltelefonnummer bekannt zu geben. Die für die Autorisierung von Aufträgen erforderlichen Transaktionsnummern werden dem Nutzer mittels SMS an die der Bank bekannt gegebene Mobiltelefonnummer gesendet.

Zu Kontrollzwecken werden in der TAN-SMS auch Angaben über die durchzuführenden Aufträge, insbesondere Empfänger-IBAN und Betrag oder ein

Referenzcode (Elektronischer Begleitzettel) und Kontrollwert (Summe aller Aufträge), mitgeliefert. Der Nutzer ist verpflichtet, diese auf Übereinstimmung mit den im Electronic-Banking eingegebenen Aufträgen zu prüfen. Die mobileTAN darf nur bei Übereinstimmung eingegeben werden. Eine mobileTAN ist nur für die Durchführung jenes Auftrages gültig, für den sie angefordert wurde und verliert nach Eingabe ihre Gültigkeit. Der Nutzer kann die Mobiltelefonnummer direkt im Electronic-Banking ändern. Eine Änderung der Mobiltelefonnummer kann auch durch den Nutzer persönlich in der Bank vorgenommen werden.

Es liegt in der Verantwortung des Nutzers, dafür zu sorgen, dass alle vertraglichen Grundlagen mit einem Mobilfunkanbieter und bei seinem Mobiltelefon alle technischen Voraussetzungen für den Empfang von SMS vorhanden sind. Der Nutzer hat weiters zu beachten, dass ein SMS-Empfang nur bei ausreichender Netzabdeckung des Aufenthaltsorts möglich ist.

5. Sorgfaltspflichten

Persönliche Identifikationsmerkmale dürfen nicht an Dritte, außer an vom Nutzer autorisierte Kontoinformations- oder Zahlungsauslösedienstleister, weitergegeben werden. Jeder Nutzer ist verpflichtet, eine besondere Sorgfalt bei der Aufbewahrung walten zu lassen, um missbräuchliche Zugriffe zu vermeiden. Die persönlichen Identifikationsmerkmale dürfen nur an einem sicheren Ort aufbewahrt werden. Bei Verlust oder wenn diese von einem unbefugten Dritten missbräuchlich verwendet werden, hat der Nutzer sein Passwort selbständig zu ändern. Ist es dem Nutzer nicht möglich, sein Passwort zu ändern, so hat er unverzüglich die Bank zu benachrichtigen.

6. Sperre

Die Bank wird die Nutzung des Electronic-Banking über ausdrücklichen Wunsch des Kontoinhabers zur Gänze oder über Wunsch eines Nutzers oder Ansichtsberechtigten nur diesen betreffend sperren. Der Nutzer kann seinen Zugang auch selbst im Electronic Banking sperren.

Sperrt die Bank den Zugang zu Electronic-Banking gemäß Z 15 der Allgemeinen Geschäftsbedingungen, so erfolgt die Benachrichtigung des Nutzers telefonisch, ist eine telefonische Benachrichtigung nicht möglich, erfolgt die Verständigung schriftlich an die vom Nutzer zuletzt bekanntgegebene Adresse.

Nach dreimaliger Falscheingabe der persönlichen Codes beim Login wird der Zugang zu Electronic Banking temporär gesperrt, weitere Fehleingaben erhöhen gemäß folgender Aufstellung die vorübergehende Sperre des Zugangs für den Nutzer.

- ab dem 3. Fehlversuch 30 Sekunden Wartezeit bis zum nächsten Versuch
- ab dem 5. Fehlversuch 2 Minute Wartezeit bis zum nächsten Versuch
- ab dem 7. Fehlversuch 10 Minuten Wartezeit bis zum nächsten Versuch
- ab dem 10. Fehlversuch 1 Stunde Wartezeit bis zum nächsten Versuch

Nach einmaliger richtiger Eingabe der persönlichen Codes ist der Zugang zu Electronic Banking wiederhergestellt.

Eine Sperre kann über schriftlichen Auftrag bzw. telefonisch mit einer gültigen Autorisierung wieder aufgehoben werden. Die Bank kann ein telefonisches Entsperren auch bei Nennung einer gültigen Autorisierung aus Sicherheitsgründen ablehnen.

7. Beendigung

Eine Weiterverwendung von der Bank zur Verfügung gestellter Software nach Beendigung der Kontoverbindung ist unzulässig.

Werden die Identifikationsmerkmale mehr als 18 Monate lang nicht verwendet, müssen aus Sicherheitsgründen neue Identifikationsmerkmale persönlich beantragt werden.

8. Aktualisierungen und technische Anpassungen

Die Bank ist jederzeit berechtigt, entsprechend dem technischen Fortschritt und allenfalls zusätzlichen Sicherheitsmaßnahmen, Updates und Abänderungen im Datenübertragungsbereich oder an der Programmoberfläche durchzuführen. Der Kunde ist verpflichtet, für eine ordnungsgemäße Installation von Programmupdates zu sorgen. Darüber hinaus ist die Bank auch zur Erweiterung des Funktionsumfanges des Electronic-Bankings insoweit berechtigt, als hierdurch dem Kunden keine zusätzlichen Kosten oder Verpflichtungen erwachsen.

9. Haftung

Ist der Kunde Unternehmer, trifft die Bank für Schäden, die im Zusammenhang mit Störungen bei Hard- oder Software des Nutzers oder Ansichtsberechtigten – einschließlich Computerviren und Eingriffen Dritter – oder durch nicht in der Sphäre der Bank gelegene Störungen im Verbindungsaufbau, keine Haftung. Die Bank übernimmt keine Garantie für die fehlerfreie Funktion der Programme; die entsprechenden Systemvoraussetzungen sind zu beachten. Installation und Gebrauch erfolgt immer auf eigenes Risiko.

10. Vermögensübersicht

Soweit im Electronic-Banking eine Vermögensübersicht dargestellt wird und dort auch Sparbücher angezeigt werden, gibt diese nur die zum Erfassungszeitpunkt gültige Zuordnung des Sparbuches wieder und berücksichtigt eine allfällige Weitergabe nicht automatisch. Der Kunde ist in diesem Fall verpflichtet, die Berichtigung der Vermögensübersicht zu veranlassen.

B. Besondere Bedingungen für Internet-Banking

1. Auftragsdurchführung

Unternehmer verpflichten sich nur für den Zahlungsverkehr relevante Daten weiterzugeben. Sie unterlassen insbesondere die Weitergabe von Mitteilungen mit werbeähnlichem Charakter. Bei Missbrauch behält sich die Bank etwaige rechtliche Schritte vor.

Bei Vereinbarung eines Referenzkontos können Dispositionen nur zu Gunsten dieses Referenzkontos getroffen werden.

2. Kontoauszüge

Wurde ein Kontoauszug bereits über eine Electronic-Banking-Applikation angefordert, steht dieser in einer anderen Electronic-Banking-Applikation bzw. über Kontoauszugsdrucker nicht mehr zur Verfügung; dasselbe gilt auch umgekehrt.

3. Datentransfer zum Kunden

Ist der Kunde Unternehmer, ist die Bank beim Datentransfer Bank-Kunde (insbesondere Retourdatenträger) für die Richtigkeit der ihr von Dritten zur Verfügung gestellten und dem Kunden übermittelten Daten nicht verantwortlich. Die Übermittlung von Daten, bei denen das Kunden-Mehrzweckfeld laut Datenträgerabkommen nicht auswertbar ist, ist ausgeschlossen.