V: 11/2015

BEDINGUNGEN FÜR DOLOMITENBANK OFFICE-BANKING
(nur für Kommerzkunden)

Fassung November 2015 (31.10.2018)

A. Allgemeine Bestimmungen

1. Zweck

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

2. Leistungsumfang

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

Die Verwendung von Office-Banking 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 Office-Banking kann nur Kontoinhabern oder Zeichnungsberechtigten erteilt werden. Diese Personen werden im Folgenden als „Verfüger“ bezeichnet. Darüber hinaus kann der Kontoinhaber weitere Personen als lediglich ansichtsberechtigt, also ohne Dispositionsmöglichkeit, bestimmen („Ansichtsberechtigte“).

Im Rahmen von Office-Banking übermittelt der Verfüger der Bank Aufträge über ein Datenübertragungsnetz. Für DolomitenBank Office Banking benutzt er dazu eine von der Bank zur Verfügung gestellte Software, deren Weitergabe oder Vervielfältigung verboten ist.

4. Zugriffsberechtigung

Zugang zu einem Konto im Rahmen von Internebanking erhalten nur Kunden, die sich durch Eingabe ihrer persönlichen Identifikationsmerkmale (Verfügernummer, Verfügername, persönliche Identifikationsnummer = PIN, EB-PIN für das cardTAN-Verfahren) legitimiert haben.

Auf mobilen Endgeräten ist auch ein Zugriff mittels vereinfachter Authentifizierung (Gerätebindung in Kombination mit Verfüger spezifischen vierstelligen PIN-Code) möglich. Dabei kann der Funktionsumfang auf eine reine Ansichtsberechtigung (keine Dispositionsmöglichkeit) eingeschränkt sein.

Für Dispositionen und rechtsverbindliche Willenserklärungen hat sich der Verfüger durch Eingabe seiner persönlichen Identifikationsmerkmale zu legitimieren und zusätzlich durch Eingabe einer geheimen, einmal verwendbaren Transaktionsnummer (TAN) oder mittels Digitaler Signatur als berechtigt auszuweisen. Die Berechtigung zur Vornahme von Dispositionen wird von der Bank nur aufgrund der persönlichen Identifikationsmerkmale und TANs bzw. Digitaler Signatur überprüft, die Ansichtsberechtigung nur aufgrund der persönlichen Identifikationsmerkmale. Erfordert das Office-Banking das Zusammenwirken mehrerer Verfüger, muss die Autorisierung jeweils von den gemeinsam berechtigten Verfügern gesondert, jedoch innerhalb eines Zeitraumes von 28 Tagen veranlasst werden. Bei gemeinsamer (kollektiver) Zeichnung ist die Nutzung von Teilbereichen des Office-Banking s (z.B. eps OnlineÜberweisung) nicht möglich.

Die Bank ist berechtigt, das Verfahren der Zugriffsberechtigung nach vorheriger Mitteilung an den Verfüger oder Ansichtsberechtigten abzuändern.

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

4.1.mobileTAN

Beim mobileTAN-Verfahren hat der Verfüger eine Mobiltelefonnummer bekannt zu geben. Die für die Autorisierung von Aufträgen erforderlichen Transaktionsnummern werden dem Verfüger 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 Verfüger ist verpflichtet, diese auf Übereinstimmung mit den im Office-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 Verfüger kann die Mobiltelefonnummer direkt im Office-Banking ändern. Eine Änderung der Mobiltelefonnummer kann auch durch den Verfüger persönlich in der Bank vorgenommen werden.

Es liegt in der Verantwortung des Verfügers, 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 Verfüger hat weiters zu beachten, dass ein SMS-Empfang nur bei ausreichender Netzabdeckung des Aufenthaltsorts möglich ist.

4.2. TAN-App

Die Übermittlung der für die Autorisierung von Aufträgen erforderlichen Transaktionsnummern erfolgt an eine App, die von der Bank zur Verfügung gestellt wird. Die App muss zuvor auf einem registrierten mobilen Endgerät des Verfügers (= Herstellung der Gerätebindung) installiert sein. Die Authentifizierung erfolgt mittels Gerätebindung und persönlicher Identifikationsnummer = shortPIN. Der Verfüger kann die Gerätebindung und seine persönliche shortPIN direkt im Office-Banking ändern.

Zu Kontrollzwecken werden in der Nachricht mit der TAN auch Angaben über die durchzuführenden Aufträge, insbesondere EmpfängerIBAN und Betrag oder ein Referenzcode (Elektronischer Begleitzettel) und Kontrollwert (Summe aller Aufträge), mitgeliefert. Der Verfüger ist verpflichtet, diese auf Übereinstimmung mit den im Office-Banking eingegebenen Aufträgen zu prüfen. Die TAN darf nur bei Übereinstimmung eingegeben werden.

4.3. cardTAN

Zur Verwendung der cardTAN sind eine cardTAN-fähige Karte und ein von der Bank zur Verfügung gestelltes cardTAN-Lesegerät erforderlich. Der Kunde wird Eigentümer des cardTAN-Lesegeräts.

Die Ermittlung von TANs am cardTAN-Lesegerät wird durch Einstecken einer cardTAN-fähigen Karte (Maestro oder cardTAN SecurityCard) in das cardTAN-Lesegerät und Eingabe eines eigens für dieses Verfahren erstellten EB-PIN gestartet. Den EB-PIN erhält der Verfüger im Rahmen der Freischaltung für das cardTAN-Verfahren von der Bank. Der Verfüger kann den EB-PIN direkt im Office-Banking ändern.

Den Verfüger trifft die Obliegenheit, die am cardTAN-Lesegerät generierten Auftragsdaten mit den im Office-Banking eingegebenen Aufträgen abzugleichen. Die cardTAN darf nur bei Übereinstimmung eingegeben werden.

4.4. Digitale Signatur

Anstelle der persönlichen Identifikationsmerkale und TANs kann zur Legitimierung und zur Erteilung von Aufträgen und rechtsverbindlichen Willenserklärungen gegenüber der Bank ein digitales Zertifikat verwendet werden.

5. Sorgfaltspflichten

Persönliche Identifikationsmerkmale, TANs und cardTAN-fähige Karten dürfen nicht an Dritte, insbesondere auch nicht an andere Zahlungsdienstleister, weitergegeben werden. Jeder Verfüger 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 Verfüger seine PIN selbstständig zu ändern oder durch viermalige Falscheingabe der PIN eine Sperre vorzunehmen. Ist dem Verfüger eine selbstständige Sperre nicht möglich, so hat er unverzüglich die Bank zu benachrichtigen.

6. Sperre

Die Bank wird die Nutzung des Office-Banking s über ausdrücklichen Wunsch des Kontoinhabers zur Gänze oder über Wunsch eines Verfügers oder Ansichtsberechtigten diesen betreffend sperren.

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

Der Zugang wird automatisch gesperrt, wenn viermal in ununterbrochener Reihenfolge eine falsche PIN oder TAN eingegeben wird. Eine Sperre kann persönlich am Schalter oder über schriftlichen Auftrag bzw. telefonisch mit einer gültigen TAN wieder aufgehoben werden. Die Bank kann ein telefonisches Entsperren auch bei Nennung einer gültigen TAN aus Sicherheitsgründen ablehnen.

7. Beendigung

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

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 Office-Banking s insoweit berechtigt, als hierdurch dem Kunden keine zusätzlichen Kosten oder Verpflichtungen erwachsen.

9. Haftung

Ist der Kunde Unternehmer, trifft die Bank für Schäden, die in Zusammenhang mit Störungen bei Hard- oder Software des Verfügers 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 Office-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, Office Banking und MBS

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 Office-Banking oder Dolomitenbank Office Banking angefordert, steht dieser in einer anderen Office-Banking oder Office 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.

4. Nutzung über fremde MBS Software-Produkte

Der Kunde kann MBS auch über andere Softwareprodukte, mit denen er Verbindung zur Datenverarbeitungsanlage der Bank herstellen kann, in Anspruch nehmen. Abhängig von der Berechtigungsverwaltung dieser Softwareprodukte kann der Verfüger, sowie ermächtigte Ansichtsberechtigte Zugriff auf Informationen und Daten der teilnehmenden Konten nehmen. Für Kundenanfragen, die diese Anwendung betreffen, ist die Hotline der Bank zuständig, welche die Hauptlizenz für MBS zur Verfügung stellt.