DenizBank (Wien) AG

Bedingungen für das Internetbanking

1. Leistungsangebot

(1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels Online Banking oder der DenizMobile App in dem von der Bank angebotenen Umfang und deren technischen Vorgaben abwickeln. Zudem können sie Informationen der Bank mittels Online Banking abrufen. Des Weiteren sind sie gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absätze 33 und 34 Zahlungsdiensteaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.

(2) Kunde und Bevollmächtigte werden einheitlich als „Teilnehmer", Konto und Depot einheitlich als „Konto" bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

(3) Zur Nutzung des Online Banking gelten die mit der Bank gesondert vereinbarten Verfügungslimite.

2. Voraussetzungen zur Nutzung des Online Banking

(1) Der Teilnehmer kann das Online Banking nutzen, wenn die Bank ihn authentifiziert hat.

(2) Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).

(3) Authentifizierungselemente sind
- Wissenselemente, also etwas, das nur der Teilnehmer weiß (z.B. persönliche Identifikationsnummer (PIN)),
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z.B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern (TAN), die den Besitz des Teilnehmers nachweisen, wie die girocard mit TAN-Generator oder das mobile Endgerät), oder
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z.B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

(4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.

3. Zugang zum Online Banking

(1) Der Teilnehmer erhält Zugang zum Online Banking der Bank, wenn
- er seine individuelle Teilnehmerkennung (z.B. Kontonummer, Anmeldename) angibt und
- er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9 dieser Bedingungen) vorliegt.

Nach Gewährung des Zugangs zum Online Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge erteilt werden.

(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z.B. zum Zweck der Änderung der Anschrift des Kunden) fordert die Bank den Teilnehmer auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Online Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kontoinhabers und die Kontonummer sind für den vom Teilnehmer genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Zahlungsdaten (§ 1 Absatz 26 Satz 2 ZAG).

4. Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss einem Auftrag (z.B. Überweisung) zu dessen Wirksamkeit zustimmen. Auf Anforderung hat er hierzu Authentifizierungselemente (zum Beispiel Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden.
Die Bank bestätigt mittels Online Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z.B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Internetbanking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Online Banking ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z.B. Überweisung) auf der Online-Banking-Seite der Bank oder in Nummer 2.2.1 der Bedingungen für den Überweisungsverkehr bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank angegebenen oder in Nummer 2.2.1 der Bedingungen für den Überweisungsverkehr bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Nummer 2.2.1 der Bedingungen für den Überweisungsverkehr der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1. dieser Bedingungen).
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z.B. Wertpapierorder) liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Internetbanking Verfügungslimit ist nicht überschritten.
- Die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z.B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird dem Teilnehmer hierüber mittels Online Banking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6. Information des Kunden über Online Banking-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Internetbanking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers

7.1 Schutz der Authentifizierungselemente

(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummer 3 und 4 dieser Bedingungen).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

DenizBank(Wien) AG, Zweigniederlassung Frankfurt am Main Münchener Straße 7, 60329 Frankfurt am Main
Tel.: 0800 488 6600 (kostenlos) **Tel.:** +49 (69) 4272 603-0 **Fax:** +49 (69) 4272603-4629 **E-Mail:** servicecenter@denizbank.de **www.denizbank.de**
BLZ: 500 307 00 **UID Nr.** DE813681135 **Sitz:** Frankfurt am Main **HRB** 56884 **Amtsgericht** Frankfurt am Main

ENBD

Die DenizBank (Wien) AG ist eine Zweigniederlassung der DenizBank AG, Thomas-Klestil-Platz 1, 1030 Wien, Sitz: Wien, FN 142199t (Handelsgericht Wien),

(a) Wissenselemente, wie z.B. die PIN, sind geheim zu halten; sie dürfen insbesondere
- nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des Online Banking in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden,
- nicht ungesichert elektronisch gespeichert (z.B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z.B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z.B. mobiles Endgerät mit Anwendung für das Online Banking und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z.B. die girocard mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
- sind die girocard mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z.B. Mobiltelefon) nicht zugreifen können,
- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z.B. Mobiltelefon) befindliche Anwendung für das Online Banking (z.B. Online-Banking-App, Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für das Online Banking (z.B. Online-Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf oder Entsorgung des Mobiltelefons),
- dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb des Online Banking mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden und
- muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z.B. Mobiltelefon mit Anwendung für das Online Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online Banking des Teilnehmers aktivieren.

(c) Seinselemente, wie z.B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Online Banking das von der Bank ausgegebene Wissenselement (z.B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (zum Beispiel Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.

(4) Die für das mobile-TAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Online Banking nicht mehr nutzt.

(5) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 4 darf der Teilnehmer seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden (siehe Nummer 1 Absatz 1 Sätze 3 und 4 dieser Bedingungen). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

7.2 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise auf der Online-Banking-Seite der Bank, insbesondere zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (zum Beispiel mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

8. Anzeige und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl eines Besitzelements zu Authentifizierung (z.B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.

(3) Hat der Teilnehmer den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Kunde hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1 dieser Bedingungen,
- den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
- seine Authentifizierungselemente zur Nutzung des Online Banking.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Online-Banking-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungselements des Teilnehmers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Wege unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

9.4 Automatische Sperre eines chipbasierten Besitzelements

(1) Eine Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur falsch eingegeben wird.

(2) Ein TAN-Generator als Bestandteil einer Chipkarte, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.

(3) Die in Absätzen 1 und 2 genannten Besitzelemente können dann nicht mehr für das Online Banking genutzt werden. Der

DenizBank(Wien) AG, Zweigniederlassung Frankfurt am Main Münchener Straße 7, 60329 Frankfurt am Main
Tel.: 0800 488 6600 (kostenlos) **Tel.:** +49 (69) 4272 603-0 **Fax:** +49 (69) 4272603-4629 **E-Mail:** servicecenter@denizbank.de **www.denizbank.de**
BLZ: 500 307 00 **UID Nr.** DE813681135 **Sitz:** Frankfurt am Main **HRB** 56884 **Amtsgericht** Frankfurt am Main

ENBD

Die DenizBank (Wien) AG ist eine Zweigniederlassung der DenizBank AG, Thomas-Klestil-Platz 1, 1030 Wien, Sitz: Wien, FN 142199t (Handelsgericht Wien),

Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Online Banking wiederherzustellen.

9.5 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Kunden verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Bank wird den Kunden über eine solche Zugangsverweigerung auf dem vereinbarten Weg unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Bank die Zugangssperre auf. Hierüber unterrichtet sie den Kunden unverzüglich.

10. Haftung

10.1 Haftung der Bank bei eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Bank bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

10.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn
- es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach
- Nummer 7.1 Absatz 2,
- Nummer 7.1 Absatz 4,
- Nummer 7.3 oder
- Nummer 8.1 Absatz 1

dieser Bedingungen verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Sein (siehe Nummer 2 Absatz 3 dieser Bedingungen).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

(6) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 dieser Bedingungen nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(8) Ist der Kunde kein Verbraucher, gilt ergänzend Folgendes:
- Der Kunde haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

10.2.2 Haftung des Kunden bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten (z.B. Wertpapiertransaktionen) vor der Sperranzeige

Beruhen nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten (z.B. Wertpapiertransaktionen) vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-Banking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.2.4 Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

11, DenizMobile App

11.1 Analog anwendbare Bedingungen

Die vorstehenden Bedingungen gelten sinngemäß für die Nutzung des Online Bankings über eine App der Bank („DenizMobile App“) auf einem mobilen Endgerät, soweit sich nachfolgend keine Abweichungen ergeben.

11.2 Technische Voraussetzungen und Abweichungen

Zur Nutzung des Onlinebankings per DenizMobile App ist diese auf ein mobiles Endgerät (zB Smartphone, Tablet) zu installieren und anhand der Eingabe des Passwortes und der TAN zu registrieren. Seine auf dem mobilen Endgerät verwendete Mobilfunknummer hat der Kunde der Bank mitzuteilen und dort zu registrieren. Der Zugriff auf ein registriertes Endgerät stellt ein Authentifizierungselement dar. Es bestehen folgende technische Eigenschaften:

(1) Passwort: Bei der Ersteinrichtung gibt die Bank dem Kunden ein aus einer Buchstaben-/Ziffernkombination bestehendes Passwort vor, die dem Kunden an die von ihm angegebene Mobiltelefonnummer per SMS (Short-Message-Service) zugesandt wird. Das Passwort dient der Legitimierung des Kunden beim

D **DenizBank(Wien) AG, Zweigniederlassung Frankfurt am Main** Münchener Straße 7, 60329 Frankfurt am Main
T **Tel.:** 0800 488 6600 (kostenlos) **Tel.:** +49 (69) 4272 603-0 **Fax:** +49 (69) 4272603-4629 **E-Mail:** servicecenter@denizbank.de **www.denizbank.de**
B **BLZ:** 500 307 00 **UID Nr.** DE813681135 **Sitz:** Frankfurt am Main **HRB** 56884 **Amtsgericht** Frankfurt am Main

ENBD

D
V Die DenizBank (Wien) AG ist eine Zweigniederlassung der DenizBank AG, Thomas-Klestil-Platz 1, 1030 Wien, Sitz: Wien, FN 142199t (Handelsgericht Wien),

Internetbanking per Internet bzw. DenizMobile App. Nach dem erstmaligen Einstieg muss der Kunde das Passwort ändern. Das vom Kunden geänderte Passwort hat mindestens sechs Stellen, höchstens aber 25 Stellen, mindestens einen Großbuchstaben, einen Kleinbuchstaben und 2 Ziffern zu enthalten, Sonderzeichen sind nicht zulässig. Um eine sichere Übermittlung des Passwortes via SMS gewährleisten zu können, hat der Kunde der Bank Änderungen seiner Mobiltelefonnummer unverzüglich mitzuteilen. Gibt der Kunde Änderungen der Mobiltelefonnummer nicht bekannt, wird das Passwort an die letzte vom Kunden der Bank bekanntgegebene Mobiltelefonnummer gesendet. Das Passwort kann vom Kunden via Onlinebankings jederzeit geändert werden. Darüber hinaus kann der Kunde persönlich in jeder Filiale der Bank während der Filialöffnungszeiten oder schriftlich ein neues Passwort anfordern. Das neue Passwort wird dem Kunden an die vom Kunden angegebene Mobiltelefonnummer per SMS zugesandt.

(2) smsTAN: Die für das OnlineBanking erforderliche TAN wird dem Kunden mittels SMS-Nachricht auf die vom Kunden bekanntgegebene Mobiltelefonnummer übermittelt (smsTAN). In der smsTAN werden dem Kunden zur Kontrolle auch Angaben über die durchzuführende Transaktion zum Empfänger und Betrag übermittelt. Eine smsTAN kann nur für die Durchführung jener Transaktion verwendet werden, für die sie angefordert wurde und ist zeitlich begrenzt, aktuell nur 3 Minuten, gültig. Änderungen am erfassten Transaktionsauftrag bedürfen einer neuen smsTAN.

Der Kunde kann nur dann eine smsTAN auf das Endgerät erhalten, wenn die Voraussetzungen für den Empfang von SMS erfüllt sind, wie beispielsweise, dass

- das Telefon technisch in der Lage ist, SMS zu empfangen,
- die vertraglichen Grundlagen mit dem Mobiltelefonprovider zum Empfang von SMS gegeben sind und
- sich der Kunde in einem Gebiet befindet, für das sein Mobiltelefonprovider die Zustellung einer SMS vorsieht.

(3) Fingerprint/FaceID: Fingerprint und FaceID sind Seinselemente des Kunden, die seine Authentifizierung per App ermöglichen und von diesem in der DenizMobile App im Bereich „Einstellungen“ freigeschaltet werden können. Der Fingerprint bzw. FaceID ist eine alternative Möglichkeit zur Authentifizierung des Kunden, zu deren Nutzung dieser über ein Fingerprint/FaceID fähiges mobiles Endgerät (z.B. Smartphone, Tablet) verfügen muss.

PushTAN: Bei Kunden welche die DenizMobile App nutzen und sich in dieser auf ihrem Endgerät per Passwort und TAN entsprechend registriert haben, wird die TAN durch eine pushFreigabe (pushTAN) ersetzt. Hierbei erhält der Kunde über die DenizMobile App eine Benachrichtigung auf seinem Endgerät und kann die Transaktion über die Benachrichtigung per DenizMobile App freigeben. Der Zugriff auf das registrierte Endgerät stell hierbei ein eigenes Authentifizierungselement dar.

In der pushTAN werden dem Kunden zur Kontrolle auch Angaben über die durchzuführende Transaktion zum Empfänger und Betrag übermittelt. Eine pushTAN kann nur für die Durchführung jener Transaktion verwendet werden, für die sie angefordert wurde und ist zeitlich begrenzt, aktuell nur 3 Minuten, gültig. Änderungen am erfassten Transaktionsauftrag bedürfen einer neuen pushTAN. Der Kunde kann nur dann eine Benachrichtigung zur Freigabe mittels pushTAN auf ein mobiles Endgerät erhalten, wenn die Voraussetzungen für den Empfang von Push Nachrichten erfüllt sind, wie beispielsweise, dass:

- eine aktuelle Version der vom Kunden verwendeten DenizBank Mobile App der Bank installiert ist
- das Gerät in der Geräteverwaltung der vom Kunden verwendeten Internetbanking-App der Bank registriert und für Push-Freigabe vorgesehen ist und
- sich der Kunde in einem Gebiet befindet, für das eine Internet-Datenverbindung gegeben ist.

DenizBank(Wien) AG, Zweigniederlassung Frankfurt am Main Münchener Straße 7, 60329 Frankfurt am Main
Tel.: 0800 488 6600 (kostenlos) **Tel.:** +49 (69) 4272 603-0 **Fax:** +49 (69) 4272603-4629 **E-Mail:** servicecenter@denizbank.de **www.denizbank.de**
BLZ: 500 307 00 **UID Nr.** DE813681135 **Sitz:** Frankfurt am Main **HRB** 56884 **Amtsgericht** Frankfurt am Main

ENBD

Die DenizBank (Wien) AG ist eine Zweigniederlassung der DenizBank AG, Thomas-Klestil-Platz 1, 1030 Wien, Sitz: Wien, FN 142199t (Handelsgericht Wien),