

## BESONDERE BEDINGUNGEN FÜR ELECTRONIC BANKING PER WESTERN UNION DIGITAL BANKING APP

Die Besonderen Bedingungen für electronic banking per Western Union Digital Banking App sind aus Gründen der leichteren Lesbarkeit nicht geschlechterspezifisch formuliert und gelten in gleicher Weise für alle Geschlechter.

Für die Zwecke dieser Besonderen Bedingungen bezeichnet der Begriff "Kontodokumente" im Folgenden alle Dokumente im Zusammenhang mit dem Onboarding-Prozess des Kunden im Rahmen der Western Union Digital Banking App, einschließlich, aber nicht beschränkt auf die von der Western Union International Bank GmbH bereitgestellten vorvertraglichen Informationen, die Allgemeinen Geschäftsbedingungen der Western Union International Bank GmbH, die Besonderen Bedingungen für Debitkarten und virtuelle Debitkarten, diese Besonderen Bedingungen, Besondere Bedingungen für SEPA-Sofortzahlungen und damit verbundene Preislisten, die von Fall zu Fall je nach den von der Bank für den Kunden zu erbringenden Dienstleistungen anwendbar sind, sowie alle anderen ergänzenden Unterlagen, die für den Abschluss oder die Durchführung des Onboarding-Prozesses im Rahmen der Western Union Digital Banking App erforderlich sind, wie sie vom Kunden ausdrücklich und individuell akzeptiert und von Zeit zu Zeit geändert werden.

### 1. Allgemeines

#### 1.1. Nutzung des electronic banking per Western Union Digital Banking App (im Folgenden „e-banking“)

(1) Diese Bedingungen regeln die Nutzung des e-banking der Western Union International Bank GmbH handelnd durch ihre Zweigniederlassung Western Union International Bank GmbH Niederlassung Deutschland (im Folgenden „Bank“) durch den Kunden.

(2) Die Western Union Digital Banking App (im Folgenden „App“) ist eine App der Bank, die es dem Kunden ermöglicht, bei Einhaltung der in diesen Bedingungen vereinbarten Voraussetzungen, über ein mobiles Endgerät (z. B. Smartphone) Abfragen zu tätigen (z. B. Kontostand, Umsätze) und Aufträge zu erteilen (z. B. Zahlungsaufträge) sowie rechtsverbindliche Willenserklärungen und sonstige Erklärungen abzugeben.

(3) Beim e-banking handelt es sich um eine Form des Internetbankings im Sinne der Anlage zur Verbraucherzahlungskonto-Dienstverordnung (BGBl II Nr. 60/2018).

#### 1.2. Voraussetzung für die Nutzung der App

Die Möglichkeit zur Nutzung der App setzt das Bestehen einer Geschäftsbeziehung zwischen der Bank und dem Kunden und eine Vereinbarung für das e-banking zwischen dem Kunden und der Bank voraus. Die Geschäftsbeziehung an sich wird durch die Kontodokumente und die darin enthaltenen Geschäftsbedingungen geregelt; insbesondere regeln diese Besonderen Bedingungen die Nutzung des e-banking per App durch den Kunden.

### 1.3. Registrierung in der App

Die Registrierung in der App erfolgt durch die von der App vorgegebenen Schritte. Ein Schritt im Registrierungsprozess ist die Eingabe der E-Mail-Adresse und des Passworts, welche (i) der Kunde für die Anmeldung im wu.com Profil verwendet oder (ii) welche vom Kunden bei der Registrierung in der App erstellt werden. Nach der Erstellung des Benutzernamens und des Passworts hat der Kunde die Möglichkeit, biometrische Erkennung zu aktivieren oder einen Zugangscode zu erstellen.

### 1.4. Begriffsbestimmungen

#### Passwort

Das Passwort ist das vom Kunden (i) zum Login in sein wu.com Profil verwendete oder (ii) bei der Registrierung in der App festgelegte Geheimwort (Kombination aus 8-16 Zeichen mit mindestens 1 Großbuchstaben, 1 Kleinbuchstaben und 1 Zahl oder Sonderzeichen). Das Passwort ist ein persönliches Identifikationsmerkmal des Kunden, welches bei zusätzlicher Angabe der E-Mail-Adresse der Identifizierung des Kunden beim e-banking dient. Das Passwort kann vom Kunden in der App geändert werden.

#### Zugangscode

Der Zugangscode ist eine sechsstellige Zahl, die der Kunde erstellen und anstelle des Passworts zum Login verwenden kann. Die Erteilung von Aufträgen sowie die Abgabe von rechtsverbindlichen Willenserklärungen oder sonstigen Erklärungen kann durch die Eingabe des Zugangscode erfolgen. Zum Zweck der Kontrolle durch den Kunden werden dazu Details über den zu autorisierenden Auftrag (z. B. IBAN des Empfängers und der Betrag des Zahlungsvorgangs) oder über die rechtsverbindliche Willenserklärung bzw. sonstige Erklärung angezeigt.

Die Eingabe des Zugangscode ist auch für den Zugang zur App erforderlich, wenn nach dem österreichischen Zahlungsdienstegesetz 2018 oder der Delegierten Verordnung (EU) 2018/389 eine starke Kundenauthentifizierung vorgeschrieben ist. Der Zugangscode kann vom Kunden in der App geändert werden.

#### Touch ID

Die Touch ID ist ein persönliches Identifikationsmerkmal des Kunden, das eine Identifizierung beim e-banking mittels Fingerabdrucks ermöglicht und vom Kunden in der App freigeschaltet werden muss. Die Touch ID ist eine alternative Möglichkeit zur Identifikation des Kunden durch E-Mail-Adresse und Passwort. Die Erteilung von Aufträgen sowie die Abgabe von rechtsverbindlichen Willenserklärungen oder sonstigen Erklärungen kann durch die Eingabe der Touch ID erfolgen. Zum Zweck der Kontrolle durch den Kunden werden dazu Details über den zu autorisierenden Auftrag (z. B. IBAN des Empfängers und der Betrag des Zahlungsvorgangs) oder über die rechtsverbindliche Willenserklärung bzw. sonstige Erklärung angezeigt. Zur Nutzung der Touch ID muss der Kunde über ein Touch ID-fähiges mobiles Endgerät (z. B. Smartphone) verfügen und der Kunde muss die Touch ID-Funktion aktiviert haben

#### Face ID

Die Face ID ist ein persönliches Identifikationsmerkmal des Kunden, das eine Identifizierung beim e-banking mittels Gesichtserkennung ermöglicht und vom Kunden in der App freigeschaltet werden muss. Die Face ID ist eine alternative

Möglichkeit zur Identifikation des Kunden durch E-Mail-Adresse und Passwort. Die Erteilung von Aufträgen sowie die Abgabe von rechtsverbindlichen Willenserklärungen oder sonstigen Erklärungen kann durch die Eingabe der Face ID erfolgen. Zum Zweck der Kontrolle durch den Kunden werden dazu Details über den zu autorisierenden Auftrag (z. B. IBAN des Empfängers und der Betrag des Zahlungsvorgangs) oder über die rechtsverbindliche Willenserklärung bzw. sonstige Erklärung angezeigt. Zur Nutzung der Face ID muss der Kunde über ein Face ID-fähiges mobiles Endgerät (z. B. Smartphone) verfügen und der Kunde muss die Face ID-Funktion aktiviert haben.

### **e-Postfach**

Das e-Postfach ist ein Postfach für den Kunden, um im Falle von Anfragen Mitteilungen an die Bank zu senden oder wenn der Kunde Unterstützung benötigt und um Mitteilungen von der Bank zu erhalten.

### **Authentifizierungscode**

Der Authentifizierungscode ist ein Code, der bei starker Kundenauthentifizierung im Sinne des österreichischen Zahlungsdienstegesetzes 2018 und der Delegierten Verordnung (EU) 2018/389 generiert wird und mit dem zu autorisierenden Schritt (z. B. mit dem zu autorisierenden Auftrag oder mit der abzugebenden Willenserklärung des Kunden) dynamisch verlinkt ist. Mit jeder Eingabe des Zugangscodes wird ein einmaliger Authentifizierungscode generiert.

### **Starke Kundenauthentifizierung**

Die starke Kundenauthentifizierung ist das im österreichischen Zahlungsdienstegesetz 2018 und der Delegierten Verordnung (EU) 2018/389 geregelte Verfahren zur starken Kundenauthentifizierung.

## **2. Zugang – Aufträge und Erklärungen**

(1) Zugang zum e-banking erhalten nur Kunden, die sich durch die Eingabe von E-Mail-Adresse und Passwort oder durch Touch ID bzw. Face ID oder Zugangscodes legitimiert haben. Die zusätzliche Eingabe des Zugangscodes für den Zugang zur App ist dann erforderlich, wenn seit der letzten starken Kundenauthentifizierung mehr als 30 Tage verstrichen sind, oder wenn der Kunde das erste Mal auf sein Zahlungskonto zugreift.

(2) Die Erteilung von Aufträgen und die Abgabe rechtsverbindlicher Willenserklärungen oder sonstiger Erklärungen durch den Kunden erfolgt durch die Eingabe seines Zugangscodes, seiner Touch ID bzw. Face ID.

(3) Die Abgabe rechtsverbindlicher Willenserklärungen durch den Kunden kann auch dadurch erfolgen, dass der Kunde im e-banking ein ihm von der Bank ausdrücklich unterbreitetes Anbot dadurch annimmt, dass er die Annahme erklärt (etwa durch das Anklicken einer Box mit seiner Einverständniserklärung) und er seine Annahme danach bestätigt (etwa durch das Betätigen eines Buttons); auf diese Weise kann der Kunde auch sonstige Erklärungen abgeben.

(4) Die Bank ist berechtigt, aber nicht verpflichtet, Überweisungen des Kunden unter den Voraussetzungen der Art 10 bis 21 der Delegierten Verordnung (EU) 2018/389 auch ohne Autorisierung durch den Zugangscodes, der Touch ID bzw. Face ID durchzuführen.

(5) Die Entgegennahme von Aufträgen durch die Bank gilt nicht als Durchführungsbestätigung.

## **3. Sorgfaltspflichten und empfohlene Sicherheitsmaßnahmen**

### **3.1. Verpflichtung zur Einhaltung**

Jeder Kunde ist zur Einhaltung der in Punkt 3.2. vereinbarten Sorgfaltspflichten verpflichtet. Kunden, die Unternehmer sind, sind zusätzlich zur Einhaltung der empfohlenen Sicherheitsmaßnahmen gemäß Absatz 3.3. verpflichtet. Kunden, die Verbraucher sind, empfiehlt die Bank die Einhaltung der empfohlenen Sicherheitsmaßnahmen, ohne dass Verbraucher zur Einhaltung verpflichtet sind. Eine Verletzung dieser Verpflichtungen kann gemäß Punkt 7. (im Verhältnis zu Verbrauchern) bzw. Punkt 8. (im Verhältnis zu Unternehmern) zu Schadenersatzpflichten des Kunden oder zum Entfall bzw. zur Minderung seiner Schadenersatzansprüche gegenüber der Bank führen.

### **3.2. Sorgfaltspflichten**

#### **3.2.1. Geheimhaltungs- und Sperrverpflichtung**

(1) Der Kunde hat sein Passwort und den Zugangscodes geheim zu halten; er darf diese Dritten nicht mitteilen und auch nicht auf eine sonstige Weise an Dritte weitergeben. Die Weitergabe an Zahlungsauslösedienstleister und Kontoinformationsdienstleister ist jedoch zulässig, soweit sie erforderlich ist, damit diese ihre Dienstleistungen für den Kunden erbringen können.

(2) Der Kunde ist verpflichtet, größte Sorgfalt bei der Aufbewahrung und Verwendung seines Passworts und des Zugangscodes walten zu lassen, um einen Missbrauch zu vermeiden. Der Kunde hat insbesondere darauf zu achten, dass sein Passwort und der Zugangscodes bei deren Verwendung nicht ausgespäht werden; der Kunde darf sie auch nicht in seinem mobilen Endgerät, auf welchem er die App installiert hat, speichern bzw. elektronisch notieren, etwa in einer App für Notizen, es sei denn, eine solche Speicherung oder App ist vor dem Zugriff Dritter gesichert.

(3) Bei Verlust von Passwort und/oder Zugangscodes sowie dann, wenn der Kunde von einer missbräuchlichen Verwendung oder einer sonstigen nicht autorisierten Nutzung des e-banking Kenntnis erlangt hat, hat der Kunde die Sperre des Zugangs zu seinem e-banking unverzüglich zu veranlassen.

(4) Bei Verlust oder Diebstahl jenes mobilen Endgerätes des Kunden, auf welchem die App installiert ist, hat der Kunde unverzüglich die Sperre seines Zugangs zum e-banking zu veranlassen; dies gilt auch dann, wenn der Kunde die App auf mehreren mobilen Endgeräten installiert hat und eines von diesen gestohlen wird oder verloren geht.

#### **3.2.2. Sorgfaltspflichten zur Sperre des Endgeräts und bei der Installation**

(1) Der Kunde ist verpflichtet, den Zugang zum Gebrauch des mobilen Endgerätes, auf welchem die App installiert ist, bzw. den Zugriff auf dort gespeicherte Daten für Nichtberechtigte zu sperren, wenn er das Endgerät nicht benutzt.

(2) Der Kunde darf die App ausschließlich aus dem Apple App Store oder dem Google Play Store installieren.

### 3.2.3. Sorgfaltspflichten bei Aufträgen und Erklärungen

Die in der App nach der Eingabe durch den Kunden an-gezeigten Daten sind vom Kunden vor der Verwendung des Zugangscodes, der Touch ID bzw. Face ID auf ihre Richtigkeit hin zu überprüfen. Nur bei Übereinstimmung der in der App angezeigten Daten mit dem gewünschten Auftrag bzw. der gewünschten rechtsverbindlichen Willenserklärung oder sonstigen Erklärung darf der Zugangscode, die Touch ID bzw. Face ID zur Erteilung von Aufträgen bzw. zur Abgabe von Erklärungen verwendet werden.

### 3.3. Empfohlene Sicherheitsmaßnahmen bei der Nutzung von e-banking

(1) Dem Kunden wird empfohlen, das Passwort und den Zugangscode regelmäßig, spätestens alle zwei Monate, selbstständig zu ändern.

(2) Dem Kunden wird empfohlen, unverzüglich die Sperre des Zugangs zum e-banking zu veranlassen, wenn Anlass zur Befürchtung besteht, dass unbefugte Dritte Kenntnis von Passwort und/oder Zugangscode erlangt haben, oder wenn sonstige Umstände vorliegen, die einem unbefugten Dritten Missbrauch ermöglichen könnten.

(3) Dem Kunden wird empfohlen, sein mobiles Endgerät, auf welchem die App installiert ist, hinsichtlich Risiken aus dem Internet abzusichern, insbesondere dieses am aktuellen Stand zu halten, sowie Sicherheitsupdates des Betriebssystems des mobilen Endgeräts durchzuführen und einen aktuellen Virenschutz zu verwenden.

## 4. Sperre

### 4.1. Automatische Sperre

(1) Der Zugang zum e-banking wird automatisch vorübergehend gesperrt, wenn während eines Zugriffs dreimal aufeinanderfolgend das Passwort falsch eingegeben wurde. Nach der automatischen Aufhebung der ersten vorübergehenden Sperre kommt es nach erneuter zweimaliger aufeinanderfolgender falscher Eingabe des Passworts zu einer zweiten vorübergehenden Sperre. Nach Aufhebung der zweiten vorübergehenden Sperre kommt es bei jeder weiteren falschen Eingabe des Passworts jeweils zu einer erneuten vorübergehenden Sperre. Die maximale Gesamtanzahl der falschen Eingaben des Passworts, die zu einer vorübergehenden Sperre führt, ist neun. Nach der zehnten falschen Eingabe des Passworts wird der Zugang zum e-banking automatisch dauerhaft gesperrt. Die Bank wird dem Kunden unverzüglich die Dauer der jeweiligen vorübergehenden Sperre bekanntgeben.

(2) Der Zugang zum e-banking wird automatisch dauerhaft gesperrt, wenn der Zugangscode fünfmal aufeinanderfolgend falsch eingegeben wurde.

### 4.2. Sperre durch den Kunden

Der Kunde kann die Sperre des Zugangs zum e-banking durch die fünfmalige aufeinanderfolgende falsche Eingabe des Zugangscodes selbst vornehmen oder jederzeit telefonisch unter +496990235063 veranlassen.

### 4.3. Sperre durch die Bank

(1) Die Bank ist berechtigt, das e-banking für einen Kunden zu sperren, wenn objektive Gründe im Zusammenhang mit der Sicherheit dies rechtfertigen oder der Verdacht einer nicht autorisierten oder betrügerischen Verwendung besteht.

(2) Die Bank wird den Kunden über eine Sperre des e-banking und deren Gründe möglichst vor, spätestens aber unverzüglich nach der Sperre informieren, soweit die Bekanntgabe der Sperre oder der Gründe für die Sperre nicht eine gerichtliche oder verwaltungsbehördliche Anordnung verletzen bzw. nationalen oder europäischen Rechtsnormen oder objektiven Sicherheitserwägungen zuwiderlaufen würde.

### 4.4. Bekanntgabe und Aufhebung der Sperre

(1) Bevor eine Sperre dauerhaft wird, erhält der Kunde eine Warnung.

(2) Die Bank wird eine Sperre gemäß Punkt 4.3. aufheben, sobald die Gründe für die Sperre nicht mehr vorliegen. Die Bank wird den Kunden über die Aufhebung der Sperre unverzüglich informieren.

(3) Der Kunde kann die Aufhebung einer Sperre jederzeit telefonisch unter +496990235063 beauftragen.

## 5. Rechtsverbindliche Verfügungen und Erklärungen des Kunden

(1) Aufträge und rechtsverbindliche Willenserklärungen sowie sonstige Erklärungen des Kunden im e-banking gelten als vom Kunden erteilt bzw. abgegeben, wenn der Kunde diese mittels Zugangscode, Touch ID bzw. Face ID freigegeben hat. Der Kunde kann Willenserklärungen auch auf die in Punkt 2. Absatz 3 geregelte Weise abgeben.

(2) Die Bank ist nicht verpflichtet, eine Bestätigung über den Auftrag oder die rechtsverbindliche Willenserklärung oder sonstige Erklärung einzuholen. Das in Z 4 der „Allgemeinen Geschäftsbedingungen der Western Union International Bank GmbH“ (nachfolgend „AGB“) vereinbarte Recht der Bank, eine Auftragsbestätigung einzuholen, bleibt davon unberührt.

(3) Aufträge und rechtsverbindliche Willenserklärungen sowie sonstige Erklärungen des Kunden können unter Verwendung der App nur in jenem Umfang erteilt bzw. abgegeben werden, als sie durch eine Verfügungsberechtigung gemäß Z 31 AGB gedeckt sind.

## 6. Eingangszeitpunkt / Durchführung von Zahlungsaufträgen

(1) Eingangszeitpunkt von Zahlungsaufträgen: Der Zeitpunkt, zu dem ein Zahlungsauftrag via e-banking bei der Bank eingeht, gilt als Eingangszeitpunkt. Geht der Zahlungsauftrag an einem Geschäftstag nach dem Annahmeschluss oder nicht an einem Geschäftstag der Bank ein, so wird der Auftrag so behandelt, als wäre er erst am nächsten Geschäftstag bei der Bank eingegangen.

(2) Der Annahmeschluss für Zahlungsaufträge an einem Geschäftstag ist Absatz II. 5.2 der „Vorvertraglichen Informationen der Western Union International Bank GmbH“ zu entnehmen.

(3) Zahlungsaufträge: Sofern kein in der Zukunft liegendes Durchführungsdatum vom Kunden mitgeteilt wird, erfolgt die Durchführung taggleich, wenn die Datenbestände für den Zahlungsverkehr spätestens bis zum Annahmeschluss der Bank zur Bearbeitung vorliegen. Andernfalls erfolgt die Durchführung

spätestens an dem Geschäftstag, der dem Tag der Datenübertragung durch den Auftraggeber folgt. Voraussetzung für die Durchführung ist eine ausreichende Kontodeckung (Guthaben oder Überziehungsmöglichkeit).

(4) Ergänzend gelten Z 39 und Z 39a AGB, in denen Überweisungsaufträge geregelt sind.

## **7. Haftung des Kunden als Verbraucher**

(1) Der Kunde, der Verbraucher ist, haftet für den gesamten Schaden eines nicht autorisierten Zahlungsvorgangs, welchen er der Bank durch (i) die vorsätzliche oder grob fahrlässige Verletzung der Sorgfaltspflichten gemäß Punkt 3.2. zugefügt hat oder (ii) in betrügerischer Absicht.

(2) Ist die Verletzung der Sorgfaltspflichten gemäß Punkt 3.2. auf leichte Fahrlässigkeit des Kunden zurückzuführen, ist seine Haftung auf höchstens 50,- EUR beschränkt. Hat der Kunde die Sorgfaltspflichten gemäß Punkt 3.2 weder in betrügerischer Absicht noch vorsätzlich verletzt, sind bei einer allfälligen Schadenteilung zwischen dem Kunden und der Bank insbesondere die Art der personalisierten Sicherheitsmerkmale sowie die besonderen Umstände, unter denen die missbräuchliche Verwendung des e-banking stattgefunden hat, zu berücksichtigen.

(3) War für den Kunden vor der Zahlung der Verlust oder Diebstahl des mobilen Endgeräts, auf welchem die App installiert ist, oder die missbräuchliche Verwendung des e-banking nicht bemerkbar, haftet er bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß Punkt 3.2. nicht. Der Kunde haftet bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß Punkt 3.2 auch dann nicht, wenn der Verlust der persönlichen Identifikationsmerkmale durch Handlungen oder Unterlassungen der Bank (einschließlich ihrer Mitarbeiter und Vertreter und sonstiger Einrichtungen, an die solche Dienstleistungen ausgelagert wurden) verursacht wurden.

(4) Abweichend von Punkt 7 (2) haftet der Kunde nicht, wenn die Bank bei einer missbräuchlichen Verwendung des e-banking oder bei einer nicht autorisierten Zahlung über das e-banking keine starke Kundenauthentifizierung verlangt hat. Wurde ein nicht autorisierter Zahlungsvorgang in betrügerischer Absicht durch den Kunden ermöglicht, so haftet der Kunde unabhängig davon, ob die Bank eine starke Kundenauthentifizierung verlangt hat oder nicht.

(5) Der Kunde haftet nicht, wenn der Schaden aus einer nicht autorisierten Nutzung des e-banking entstanden ist, nachdem der Kunde WUIB über einen Verlust, Diebstahl oder eine missbräuchliche Verwendung gemäß Punkt 3.2.1(3) oder Punkt 4. informiert hat, es sei denn, der Kunde hat in betrügerischer Absicht gehandelt.

## **8. Haftung gegenüber Unternehmern / Haftung des Kunden als Unternehmer**

Im Verhältnis zu Unternehmern wird § 68 des österreichischen Zahlungsdienstegesetzes 2018 zur Gänze abbedungen; die Haftung der Bank für leicht fahrlässig verursachte Schäden ist ausgeschlossen. Für jene Schäden, die im Zusammenhang mit der Hard- oder Software des Kunden oder die durch das Nichtzustandekommen des Verbindungsaufbaues mit dem Rechenzentrum der Bank, oder die durch einen vorübergehenden Ausfall der Einrichtungen der Bank zur Abwicklung des e-banking entstehen, sowie dann, wenn der Unternehmer die in Punkt 3. festgelegten Sorgfaltspflichten verletzt hat oder wenn der Unternehmer den in Punkt 3. enthaltenen empfohlenen Sicherheitsmaßnahmen nicht entsprochen hat, ist die Haftung der

Bank unabhängig vom Grad ihres Verschuldens ausgeschlossen. Hat der Unternehmer die in Punkt 3. festgelegten Sorgfaltspflichten verletzt oder den in Punkt 3. enthaltenen empfohlenen Sicherheitsmaßnahmen nicht entsprochen, haftet er der Bank für den daraus resultierenden Schaden.

## **9. Erklärungen und Kommunikation**

(1) Rechtsgeschäftliche Erklärungen, Mitteilungen und Informationen der Bank (nachfolgend gemeinsam „Erklärungen“) erhält der Kunde in einer mit ihm vereinbarten Kommunikationsform. Als Kommunikationsformen werden E-Mail, SMS, Push-Benachrichtigungen und die Übermittlung ins e-Postfach des Kunden zum e-banking unter Verständigung des Kunden vereinbart. Schließen der Kunde und die Bank Vereinbarungen über weitere Kommunikationsformen ab, bleibt deren Wirksamkeit von dieser Bestimmung unberührt; dies gilt auch für die Kommunikation über die App. Die Wirksamkeit schriftlicher Erklärungen (auch bei Übermittlung per Post) bleibt ebenfalls unberührt.

(2) Die Bank kann dem Kunden Erklärungen an die von ihm der Bank bekanntgegebene angegebene E-Mail-Adresse übermitteln. Erklärungen der Bank, welche sie gegenüber dem Kunden per E-Mail an diese E-Mail-Adresse abgibt, sind daher wirksam. Auch der Kunde kann mit der Bank per E-Mail kommunizieren und per E-Mail und über das e-Postfach in der App wirksame Erklärungen abgeben. Der Kunde kann nicht mit der Bank kommunizieren und Erklärungen wirksam abgeben, wenn der Kunde in einem E-Mail darauf hingewiesen wird, dass an diese E-Mail-Adresse keine Antwort möglich ist („no-reply-Adressen“).

(3) Bei einer Änderung seiner E-Mail-Adresse hat der Kunde der Bank seine neue E-Mail-Adresse unverzüglich bekannt zu geben; dies ist telefonisch unter +496990235063 oder in der App möglich. Hat der Kunde der Bank seine geänderte E-Mail-Adresse nicht bekannt gegeben und erhält die Bank eine Information, dass die E-Mail-Adresse nicht mehr aktuell ist, gelten Erklärungen der Bank als dem Kunden zugegangen, wenn sie die Bank sowohl an die letzte vom Kunden bekannt gegebene E-Mail-Adresse gesendet als auch ins e-Postfach des Kunden zum e-banking unter Verständigung des Kunden übermittelt hat; hat die Bank keine solche Information erhalten, gelten Erklärungen der Bank als dem Kunden zugegangen, wenn sie die Bank an die letzte vom Kunden bekannt gegebene E-Mail-Adresse gesendet hat.

## **10. Änderung der Bedingungen über das e-banking per Western Union Digital Banking App**

(1) Änderungen dieser Bedingungen werden dem Kunden von der Bank mindestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Inkrafttretens angeboten; dabei werden die vom Änderungsangebot betroffenen Bestimmungen und die vorgeschlagenen Änderungen dieser Bedingungen in einer dem Änderungsangebot angeschlossenen Gegenüberstellung (im Folgenden „Gegenüberstellung“) dargestellt. Das Änderungsangebot wird dem Kunden mitgeteilt. Die Zustimmung des Kunden gilt als erteilt, wenn vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens kein schriftlicher oder in einer mit dem Kunden vereinbarten Weise elektronisch (z. B. per E-Mail oder in der App) erklärter Widerspruch des Kunden bei der Bank einlangt. Die Bank wird den Kunden im Änderungsangebot darauf aufmerksam machen, dass sein Stillschweigen durch das Unterlassen eines schriftlichen oder in einer mit dem Kunden vereinbarten Weise elektronisch erklärten Widerspruchs als

Zustimmung zu den Änderungen gilt, sowie dass der Kunde, der Verbraucher ist, das Recht hat, sowohl die Vereinbarung über das e-banking als auch die Kontodokumente, zu denen das e-banking vereinbart ist, vor Inkrafttreten der Änderungen kostenlos fristlos zu kündigen. Außerdem wird die Bank die Gegenüberstellung sowie die vollständige Fassung der neuen Bedingungen für das e-banking per Western Union Digital Banking App auf ihrer Internetseite veröffentlichen und dem Kunden auf sein Ersuchen die vollständige Fassung der neuen Bedingungen übersenden; auch darauf wird die Bank im Änderungsangebot hinweisen.

(2) Die Mitteilung und das Änderungsangebot gemäß Abs. 1 von Punkt 11 wird dem Kunden über die Übermittlung des Änderungsangebots samt Gegenüberstellung per E-Mail angeboten. Die Mitteilung erfolgt derart, dass das Kreditinstitut das Änderungsangebot nicht mehr einseitig abändern kann und der Kunde die Möglichkeit hat, die Mitteilung zudem bei sich abzuspeichern und auszudrucken. Das Änderungsangebot gilt in jenem Zeitpunkt als dem Kunden zugegangen, in dem er die E-Mail erhält und in der Lage ist, diese Information unter normalen Umständen abzurufen.

(3) Die Änderung von Leistungen der Bank durch eine Änderung dieser Bedingungen nach Punkt 11, Absatz (1) ist auf sachlich gerechtfertigte Fälle beschränkt; eine sachliche Rechtfertigung liegt dann vor,

(i) wenn die Änderung durch eine Änderung der für Zahlungsdienste sowie ihre Abwicklung maßgeblichen gesetzlichen Bestimmungen oder durch Vorgaben der Finanzaufsicht, der Europäischen Bankenaufsichtsbehörde, der Europäischen Zentralbank, der Österreichischen Nationalbank oder einer anderen zuständigen Behörde erforderlich ist,

(ii) wenn die Änderung durch die Entwicklung der für Zahlungsdienste sowie ihre Abwicklung maßgeblichen Judikatur erforderlich ist,

(iii) wenn die Änderung die Sicherheit des Bankbetriebs oder die Abwicklung der Geschäftsverbindung mit dem Kunden zum e-banking fördert,

(iv) wenn die Änderung zur Umsetzung technischer Entwicklungen oder zur Anpassung an neue Programme zur Nutzung mobiler Endgeräte oder der App erforderlich ist,

(v) wenn die Änderung durch eine Änderung der gesetzlichen Bestimmungen für die Erteilung von Aufträgen und für die Abgabe von Erklärungen über die App erforderlich ist,

(vi) wenn die Änderung durch eine Änderung der gesetzlichen Bestimmungen für jene Bankgeschäfte, welche der Kunde über die App abwickeln kann, erforderlich ist.

Die Einführung von Entgelten und die Änderung vereinbarter Entgelte durch eine Änderung dieser Bedingungen sind ausgeschlossen.

