Schoellerbank
Private Banking

~~Bedingungen zur Teilnahme am~~ Electronic Banking ~~Bedingungen~~ der Schoellerbank AG

(Gegenüberstellung der geänderten Klauseln)

Fassung April 2017	**Fassung 01. April 2020**
	Schoellerbank Electronic Banking (Schoellerbank Online Banking, Schoellerbank Business Banking sowie Multi Bank Standard Service (MBS)) ermöglicht für entsprechend definierte Konten die Durchführung von Bankgeschäften, insbesondere von Zahlungs- und Wertpapieraufträgen und Konto-/Depotabfragen. Der Leistungsumfang kann je nach Bankprodukt unterschiedlich sein oder abweichen.
1. Gegenstand der Vereinbarung	**1. Allgemein**
Diese Vereinbarung regelt die Teilnahme am Schoellerbank Electronic Banking, einer Dienstleistung der Schoellerbank Aktiengesellschaft (in der Folge „Schoellerbank“), die dem Kunden erlaubt, über eine Datenübertragungsleitung via Internet eine Kommunikation mit unserem Rechenzentrum aufzubauen und nach elektronischer Autorisierung darüber Bankgeschäfte zu tätigen oder Informationen abzufragen. Schoellerbank Electronic Banking umfasst Schoellerbank Online Banking (Online-Konto, Online-Depot), Schoellerbank Business Banking sowie Multi Bank Standard Service (MBS-Service). Im Rahmen von Online Banking kann auch eine für mobile Geräte (z.B. Smartphones und Tablets) optimierte Version des Online Banking genutzt werden.	~~Diese Vereinbarung regelt die Teilnahme am Schoellerbank Electronic Banking, einer Dienstleistung der Schoellerbank Aktiengesellschaft (in der Folge „Schoellerbank“), die dem Kunden erlaubt,~~ **1.1** Internetbanking (Schoellerbank Online Banking) ist ein spezielles Dienstleistungsprodukt der Schoellerbank AG (im Folgenden kurz: Bank), durch das ein Kunde als Konto-/Depotinhaber oder Zeichnungsberechtigter über eine Datenübertragungsleitung via Internet eine Kommunikation mit dem Bankrechenzentrum aufbauen und nach elektronischer Autorisierung ~~darüber Bankgeschäfte zu tätigen oder~~ Informationen abfragen sowie Aufträge zu Konten und Wertpapierdepots erteilen kann. ~~Schoellerbank Electronic Banking umfasst Schoellerbank Online Banking (Online-Konto, Online-Depot), Schoellerbank Business Banking sowie Multi Bank Standard Service (MBS-Service).~~ Im Rahmen des Internetbankings kann auch eine für mobile Geräte (z.B. Smartphones und Tablets) optimierte Version des Internetbankings genutzt werden.
Der Umfang der Inanspruchnahme des Electronic Banking durch den Kunden richtet sich nach der getroffenen Electronic Banking Vereinbarung und erstreckt sich nicht automatisch auf das gesamte Angebot an bestehenden sowie künftig von der Schoellerbank angebotenen Dienstleistungen. Electronic Banking ist ein Zusatzprodukt zum Konto-/Depotführungsvertrag, unterliegt somit den Bedingungen des Konto-/Depotführungsvertrages, das hinsichtlich bestimmter Geschäfte bzw. Dienstleistungen ergänzend zur herkömmlichen Abwicklung auch eine Abwicklung im Rahmen einer elektronischen Kommunikation ermöglicht.	~~Der Umfang der Inanspruchnahme des Electronic Banking durch den Kunden richtet sich nach der getroffenen Electronic Banking Vereinbarung und erstreckt sich nicht automatisch auf das gesamte Angebot an bestehenden sowie künftig von der Schoellerbank angebotenen Dienstleistungen. Electronic Banking ist ein Zusatzprodukt zum Konto-/Depotführungsvertrag, unterliegt somit den Bedingungen des Konto-/Depotführungsvertrages, das hinsichtlich bestimmter Geschäfte bzw. Dienstleistungen ergänzend zur herkömmlichen Abwicklung auch eine Abwicklung im Rahmen einer elektronischen Kommunikation ermöglicht.~~
Zwischen dem Kunden und der Schoellerbank wird je nach beantragtem Produkt der „Antrag zur Teilnahme am Online Banking und zur Online-Abwicklung von Wertpapieraufträgen“, „Antrag zur Teilnahme am Online Banking inklusive Portfolioanalyse und zur Online-Abwicklung von Wertpapieraufträgen“, „Antrag zur Teilnahme am Schoellerbank Business Banking“ bzw. „Antrag zur Teilnahme am Electronic Banking Service der Schoellerbank Aktiengesellschaft – Multi Bank Standard	**1.2** Zwischen dem Kunden und der ~~Schoellerbank wird je nach beantragtem Produkt der „Antrag zur Teilnahme am Online Banking und zur Online-Abwicklung von Wertpapieraufträgen“, „Antrag zur Teilnahme am Online Banking inklusive Portfolioanalyse und zur Online-Abwicklung von Wertpapieraufträgen“, „Antrag zur Teilnahme am Schoellerbank Business Banking“ bzw. „Antrag zur Teilnahme am Electronic Banking Service der Schoellerbank Aktiengesellschaft – Multi Bank Standard~~

PC282D-Gegenüberstellung 20200101

Service“ auf unbefristete Dauer abgeschlossen, auf Grund derer der Kunde zur Nutzung von Online Banking, Schoellerbank Business Banking bzw. MBS-Service berechtigt ist.

~~Service“ auf unbefristete Dauer abgeschlossen, auf Grund derer der Kunde zur Nutzung von Online Banking, Schoellerbank Business Banking bzw. MBS-Service berechtigt ist.~~ Bank wird der „Online Banking Antrag“ oder „Online Banking Antrag mit Portfolioansicht“ der Bank (im Folgenden kurz: die Vereinbarung) auf unbefristete Dauer abgeschlossen, aufgrund dessen der Kunde zur Nutzung des Internetbankings berechtigt ist. Der Kunde erhält damit zu allen Konten und Depots, bei welchen er Konto- bzw. Depotinhaber ist, die Internetbanking-Berechtigung.

Die Regelungen betreffend Einzel- und Gemeinschafts-zeichnungsberechtigung laut Unterschriftsprobenblatt sind auch für Dispositionen mittels Electronic Banking verbindlich. Bei gemeinsamer (kollektiver) Zeichnung ist die Nutzung von Teilbereichen des Electronic Banking (z.B. eps Online- Überweisung) nicht möglich. Der Kontoinhaber muss der Erteilung einer Electronic Banking- Berechtigung an einen Zeichnungsberechtigten schriftlich zustimmen. Diese Zustimmung kann jeder Konto-/Depotinhaber jederzeit widerrufen. Der Teilnehmer kann seine Berechtigung auch selbst jederzeit durch eine schriftliche Mitteilung an uns beenden. Bei einem Gemeinschaftskonto müssen alle Kontoinhaber der Erteilung der Electronic Banking-Berechtigung an einen anderen Kontoinhaber oder an einen Zeichnungs-berechtigten schriftlich zustimmen.

~~Die Regelungen betreffend Einzel- und Gemeinschafts-zeichnungsberechtigung laut Unterschriftsprobenblatt sind auch für Dispositionen mittels Electronic Banking verbindlich. Bei gemeinsamer (kollektiver) Zeichnung ist die Nutzung von Teilbereichen des Electronic Banking (z.B. eps Online- Überweisung) nicht möglich.~~ Der Konto- bzw. Depotinhaber muss der Erteilung einer ~~Electronic Banking-~~ Internetbanking-Berechtigung an einen Zeichnungs-berechtigten schriftlich zustimmen. ~~Diese Zustimmung kann jeder Konto-/Depotinhaber jederzeit widerrufen. Der Teilnehmer kann seine Berechtigung auch selbst jederzeit durch eine schriftliche Mitteilung an uns beenden.~~ Bei einem Gemeinschaftskonto/-depot müssen alle Konto- bzw. Depotinhaber der Erteilung der ~~Electronic Banking-~~ Internetbanking-Berechtigung an einen ~~anderen Kontoinhaber~~ einzelnen Konto- bzw. Depotinhaber oder an einen Zeichnungsberechtigten schriftlich zustimmen.

Sofern bei einem Depot ein kollektives Zeichnungsrecht vereinbart ist, können über Internetbanking keine Aufträge vorgenommen werden, sondern ist die Internetbanking-Berechtigung bei diesen Depots auf die Einholung von Depotinformationen beschränkt. Bei einer kollektiven Zeichnung auf einem Konto, kann der Kunde die beabsichtigte Transaktion nur mit sämtlichen weiteren berechtigten Personen vornehmen.

Ein nur von einem kollektiv zeichnungsberechtigten Benutzer mit seiner TAN erstgezeichneter Auftrag, der nicht binnen 28 Tagen vom zweiten kollektiv zeichnungsberechtigten Benutzer mittels seiner TAN gegengezeichnet wird, wird ohne weitere Kontoinformation seitens der Bank unwiderruflich und ohne Durchführung aus dem System gelöscht.

2. Bedienungs- und Sicherheitshinweise

Obwohl Schoellerbank Electronic Banking einfach, benutzerfreundlich und nach dem Stand der Technik manipulationssicher angelegt ist, erklärt sich der Kunde damit einverstanden, sich vor seiner ersten Transaktion mit den Bedienungs- und Sicherheitshinweisen vertraut zu machen. Die Bedienungs- und Sicherheitshinweise können vom Kunden jederzeit über die „Hilfe“ im Schoellerbank Electronic Banking bzw. über die Schoellerbank Homepage abgerufen und ausgedruckt werden. Sie beschreiben die aktuell verfügbaren Funktionen und bilden in ihrer jeweils gültigen Fassung einen Bestandteil dieser Vereinbarung.

~~**2. Bedienungs- und Sicherheitshinweise**~~

~~Obwohl Schoellerbank Electronic Banking einfach, benutzerfreundlich und nach dem Stand der Technik manipulationssicher angelegt ist, erklärt sich der Kunde damit einverstanden, sich vor seiner ersten Transaktion mit den Bedienungs- und Sicherheitshinweisen vertraut zu machen. Die Bedienungs- und Sicherheitshinweise können vom Kunden jederzeit über die „Hilfe“ im Schoellerbank Electronic Banking bzw. über die Schoellerbank Homepage abgerufen und ausgedruckt werden. Sie beschreiben die aktuell verfügbaren Funktionen und bilden in ihrer jeweils gültigen Fassung einen Bestandteil dieser Vereinbarung.~~

3. Zugang zum Schoellerbank Electronic Banking

Die Berechtigung zur Teilnahme wird durch die Vergabe von persönlichen Identifikationsmerkmalen erteilt, das sind:

- Verfügernummer
- Verfügername
- Passwort (PIN = Persönliche Identifikations Nummer)
- Transaktionsnummer (= TAN)

~~**3. Zugang zum Schoellerbank Electronic Banking**~~

~~Die Berechtigung zur Teilnahme wird durch die Vergabe von persönlichen Identifikationsmerkmalen erteilt, das sind:~~

- ~~Verfügernummer~~
- ~~Verfügername~~
- ~~Passwort (PIN = Persönliche Identifikations Nummer)~~
- ~~Transaktionsnummer (= TAN)~~

Im Rahmen des Electronic Banking kann der Kunde wählen, ob er mobileTAN, tresorTAN oder cardTAN verwenden möchte.

~~Im Rahmen des Electronic Banking kann der Kunde wählen, ob er mobileTAN, tresorTAN oder cardTAN verwenden möchte.~~

Soweit in diesen Bedingungen zur Teilnahme am Electronic Banking auf die TAN Bezug genommen wird, gilt die betreffende Bestimmung – soweit nichts anderes bestimmt – sowohl für mobileTAN, tresorTAN als auch für cardTAN.

~~Soweit in diesen Bedingungen zur Teilnahme am Electronic Banking auf die TAN Bezug genommen wird, gilt die betreffende Bestimmung – soweit nichts anderes bestimmt – sowohl für mobileTAN, tresorTAN als auch für cardTAN.~~

Bei Verwendung der digitalen Signatur erfolgt anstelle der Eingabe einer TAN die Freigabe der Transaktion durch Verwendung der entsprechenden Berechtigungskarte und der zugehörigen Berechtigungsmerkmale.

~~Bei Verwendung der digitalen Signatur erfolgt anstelle der Eingabe einer TAN die Freigabe der Transaktion durch Verwendung der entsprechenden Berechtigungskarte und der zugehörigen Berechtigungsmerkmale.~~

Verfügernummer (= Benutzerkennung)
Jeder Kunde erhält von der Schoellerbank eine Verfügernummer, anhand derer die Schoellerbank einen Kunden zu den zum Electronic Banking berechtigten Konten zuordnen kann, mittels Brief zugestellt. Sie besteht aus einem mehrstelligen Zahlencode und wird bei Ausstellung vom System vorgegeben. Die Verfügernummer kann vom Kunden nicht geändert werden.

2. Definitionen
2.1 ~~Verfügernummer~~ Benutzername (=Benutzerkennung/ BK): Jeder Kunde erhält von der ~~Schoellerbank eine Verfügernummer, anhand derer die Schoellerbank einen Kunden zu den zum Electronic Banking berechtigten Konten zuordnen kann, mittels Brief zugestellt. Sie besteht aus einem mehrstelligen Zahlencode und wird bei Ausstellung vom System vorgegeben. Die Verfügernummer kann vom Kunden nicht geändert werden.~~ Bank einen einzigartigen, mehrstelligen Benutzernamen, anhand dessen die Bank einen Kunden eindeutig zuordnen kann. Der Benutzername wird dem Kunden anlässlich der Unterfertigung der Vereinbarung bekannt gegeben. Der Benutzername kann vom Kunden geändert werden.

Verfügername
Der Verfügername ist ein zusätzliches Sicherheitsmerkmal bei der Anmeldung (Login). Beim Ersteinstieg wird der Kunde vom System automatisch aufgefordert, einen frei wählbaren Verfügernamen festzulegen. Bei jedem weiteren Einstieg muss sich der Kunde unter Angabe dieses, vom Kunden selbst festgelegten, Verfügernamens identifizieren. Der Verfügername kann jederzeit und sofort wirksam im Online Banking unter Verwendung einer TAN geändert werden.

~~Verfügername~~
~~Der Verfügername ist ein zusätzliches Sicherheits-merkmal bei der Anmeldung (Login). Beim Ersteinstieg wird der Kunde vom System automatisch aufgefordert, einen frei wählbaren Verfügernamen festzulegen. Bei jedem weiteren Einstieg muss sich der Kunde unter Angabe dieses, vom Kunden selbst festgelegten, Verfügernamens identifizieren. Der Verfügername kann jederzeit und sofort wirksam im Online Banking unter Verwendung einer TAN geändert werden.~~

Passwort (= PIN/Persönliche Identifikations Nummer)
Das Passwort dient der Legitimierung des Kunden beim Electronic Banking und ist eine Voraussetzung dafür, dass der Kunde über Electronic Banking Aufträge erteilen bzw. Daten und Informationen abfragen kann. Die PIN besteht aus einer 16-stelligen Zahlen-/Buchstabenkette, die dem Kunden in einem verschlossenen Kuvert persönlich ausgehändigt oder auf dem Postweg zugesandt wird. Diese Erst-PIN muss im Rahmen des Ersteinstiegs zum gewählten Electronic Banking Produkt vom Kunden abgeändert werden. Bei jedem weiteren Einstieg muss sich der Kunde unter Angabe dieser, nun vom Kunden geänderten, PIN identifizieren. Die PIN kann jederzeit und sofort wirksam im jeweils genutzten Electronic Banking Produkt unter Verwendung einer TAN geändert werden. Eine neue Erst-PIN kann der Kunde telefonisch bei seinem Kundenbetreuer beantragen.

2.2 Passwort (= PIN/persönliche Identifikations-nummer):
~~Das Passwort dient der Legitimierung des Kunden beim Electronic Banking und ist eine Voraussetzung dafür, dass der Kunde über Electronic Banking Aufträge erteilen bzw. Daten und Informationen abfragen kann. Die PIN besteht aus einer 16-stelligen Zahlen-/Buchstabenkette, die dem Kunden~~ Dem Kunden wird von der Bank ein Passwort vorgeschlagen, welches vom Kunden im Rahmen des Ersteinstiegs in das Internetbanking abzuändern ist. Der Kunde muss sich bei jedem weiteren Einstieg in das Internetbanking unter Angabe des Benutzernamens, des selbst definierten Passworts und des entsprechenden Loginverfahrens (z.B. cardTan-Verfahren) authentifizieren. Der Kunde erhält das Passwort in einem verschlossenen Kuvert entweder anlässlich der Unterfertigung der Vereinbarung persönlich ausgehändigt oder auf dem Postweg zugesandt ~~wird~~. Das Passwort kann vom Kunden jederzeit im Internetbanking unter Verwendung einer TAN geändert werden. Das geänderte Passwort ist bei jeder Anmeldung im Internetbanking anzugeben. Aus Sicherheitsgründen kann die Bank den Kunden beim Login in das Internetbanking auffordern, das Passwort auf ein Passwort mit mehr Zeichen bzw. mit größerem Sicherheitsniveau umzustellen. Der Kunde kann persönlich in jedem Standort der Bank während der Öffnungszeiten ein

neues Passwort anfordern. Das neue Passwort wird dem Kunden sodann entweder in einem vom Kunden gewählten Standort der Bank persönlich ausgehändigt oder auf dem Postweg zugesandt.

Fingerprint/Touch ID
Der Fingerprint/die Touch ID ist ein persönliches Identifikationsmerkmal des Kunden, das eine Identifizierung beim Online Banking per App mittels Fingerabdruck ermöglicht und vom Kunden im Online Banking per App freigeschaltet werden muss. Der Fingerprint/die Touch ID ist eine alternative Möglichkeit zur Identifikation des Kunden mittels Verfügernummer, Verügername und PIN. Zur Nutzung des Fingerprints/der Touch ID muss der Kunde über ein Fingerprint/Touch ID fähiges mobiles Endgerät (z.B. Smartphone, Tablet) verfügen.

~~Fingerprint/Touch ID~~
~~Der Fingerprint/die Touch ID ist ein persönliches Identifikationsmerkmal des Kunden, das eine Identifizierung beim Online Banking per App mittels Fingerabdruck ermöglicht und vom Kunden im Online Banking per App freigeschaltet werden muss. Der Fingerprint/die Touch ID ist eine alternative Möglichkeit zur Identifikation des Kunden mittels Verfügernummer, Verügername und PIN. Zur Nutzung des Fingerprints/der Touch ID muss der Kunde über ein Fingerprint/Touch ID fähiges mobiles Endgerät (z.B. Smartphone, Tablet) verfügen.~~

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

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

2.4 Fido Token (Loginverfahren)
Der Fido Token (Hardware mit USB-Anschluss) ist im Handel käuflich erwerblich und ermöglicht dem Kunden, die Authentifizierung im Rahmen des Logins zum Internetbanking durchzuführen. Dazu muss der Kunde den Fido Token mit seinem Gerät über den USB-Anschluss verbinden und den Authentifizierungsvorgang bestätigen.

Transaktionsnummer (= TAN)
Für die Vornahme von Dispositionen und die Abgabe von sonstigen rechtsverbindlichen Willenserklärungen gegenüber der Schoellerbank im Rahmen des Electronic Banking sind zusätzlich zu den persönlichen Identifikationsmerkmalen Transaktionsnummern notwendig. Eine TAN dient dem Kunden als Unterschriftsersatz und muss im Rahmen des Electronic Banking in dem dafür vorgesehenen Eingabefeld zur verbindlichen Freigabe der gewünschten Disposition bzw. zur rechtsverbindlichen Willenserklärung eingegeben werden.

2.5 Transaktionsnummer (= TAN)
~~Für die Vornahme von Dispositionen~~ Eine TAN ist ein im konkreten Einzelfall generierter Authentifizierungscode, der beim Einstieg (Loginverfahren) in das Internetbanking (zusätzlich zum Benutzernamen und Passwort) und für die Erteilung von Aufträgen und die Abgabe von sonstigen rechtsverbindlichen Willenserklärungen gegenüber der ~~Schoellerbank~~ Bank im Rahmen des ~~Electronic Banking~~ Internetbankings ~~sind zusätzlich zu den persönlichen Identifikationsmerkmalen Transaktionsnummern notwendig~~ zu verwenden ist. ~~Eine TAN dient dem Kunden als Unterschriftsersatz und muss im Rahmen des Electronic Banking in dem dafür vorgesehenen Eingabefeld zur verbindlichen Freigabe der gewünschten Disposition bzw. zur rechtsverbindlichen Willenserklärung eingegeben werden.~~

Mit Verwendung der TAN in dem dafür vorgesehenen Feld sowie der Betätigung des dafür vorgesehenen Buttons gilt ein Auftrag als erteilt bzw. eine Willenserklärung als abgegeben.
Die Bank stellt dem Kunden verschiedene TAN-Verfahren zur Nutzung des Internetbankings zur Verfügung. Sollte die Bank ein vom Kunden genütztes TAN-Verfahren nicht weiter zur Verfügung stellen können, weil

- objektive Gründe im Zusammenhang mit der Sicherheit dieses TAN-Verfahrens oder der Systeme, für das es eingesetzt wird, eine Einstellung rechtfertigen, oder
- aufgrund gesetzlicher oder aufsichtsrechtlicher Bestimmungen die Bank ein vom Kunden genütztes TAN-Verfahren nicht weiter zur Verfügung stellen darf, wird die Bank den Kunden über die Gründe hierfür informieren

und, sofern der Kunde nicht bereits ein weiteres, für ihn freigeschaltetes TAN-Verfahren mit einem höheren Sicherheitsstandard nützt, einen kostenlosen Umstieg auf ein anderes TAN-Verfahren mit einem höheren Sicherheitsstandard anbieten. Dieses Angebot wird die Bank dem Kunden auf die mit ihm im Rahmen der Geschäftsverbindung für die Zustellung von Mitteilungen vereinbarten Weise so rechtzeitig mitteilen, dass ihm dieses spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt des Umstiegs zugeht. Dieses Angebot gilt als vom Kunden angenommen, wenn vor dem vorgeschlagenen Zeitpunkt des Umstiegs kein Widerspruch des Kunden bei der Bank einlangt, wobei die Bank in der Mitteilung auf die Folgen seines Stillschweigens sowie auf das dem Kunden nach Punkt 11.3 zustehende kostenlose Kündigungsrecht hinweisen wird.

- Sofern der Kunde in diesem Fall durch Widerspruch das Angebot der Bank nicht annimmt und von seinem Kündigungsrecht nicht Gebrauch macht, wird der Benutzername gesperrt. Widerspricht der Kunde dem angebotenen Umstieg auf ein anderes TAN-Verfahren mit einem höheren Sicherheitsstandard, wird die Einstellung des vom Kunden genutzten TAN-Verfahrens frühestens zwei Monate nach Mitteilung des Angebots auf Umstieg erfolgen. Der Kunde kann trotz eines Widerspruchs bis zur endgültigen Einstellung des von ihm genutzten TAN-Verfahrens jederzeit auf das angebotene TAN-Verfahren mit einem höheren Sicherheitsstandard umsteigen. Den Wunsch, auf das angebotene TAN-Verfahren umzusteigen, kann der Kunde der Bank entweder persönlich in einem Standort, telefonisch oder schriftlich auf dem Postweg mitteilen.

• mobileTAN
Entscheidet sich der Kunde für das mobileTAN-Verfahren, bekommt er für die Unterfertigung einer erfassten Electronic Banking-Transaktion nach seiner Anforderung die erforderliche mobileTAN mittels SMS (Short Message Service) auf ein Mobiltelefon übermittelt.

a) mobileTAN
~~Entscheidet sich der Kunde für das mobileTAN-Verfahren, bekommt er für die Unterfertigung einer erfassten Electronic Banking-Transaktion nach seiner Anforderung die erforderliche mobileTAN mittels SMS (Short Message Service) auf ein Mobiltelefon übermittelt.~~

Möchte der Kunde das mobileTAN-Verfahren verwenden, kann er dies der Bank entweder persönlich in einem Standort, telefonisch oder schriftlich auf dem Postweg mitteilen. Verwendet der Kunde das mobileTAN Verfahren, bekommt er die für den Login in das Internetbanking, die Zeichnung einer bereits erfassten Internetbanking-Transaktion oder die Abgabe einer Willenserklärung erforderliche mobileTAN mittels SMS (Short Message Service) auf ein mobiles Gerät (wie z.B. Mobiltelefon oder Tablet) übermittelt.

Die Telefonnummer des dafür vorgesehenen Mobiltelefons ist vom Kunden anlässlich seiner Entscheidung für das mobileTAN-Verfahren bekannt zu geben. Eine Änderung der bekannt gegebenen Mobiltelefonnummer kann durch den Kunden persönlich beim Kundenbetreuer vorgenommen oder auch direkt im Electronic Banking geändert werden, sofern dem Kunden eine SMS mit der dafür erforderlichen mobileTAN auf die bei der Schoellerbank bisher gespeicherte Telefonnummer gesendet werden kann.

Für die SMS-Benachrichtigung ist die Telefonnummer des dafür vorgesehenen Mobiltelefons ~~ist~~ vom Kunden persönlich in einem Standort rechtzeitig vor der erstmaligen Verwendung des mobileTAN-Verfahrens ~~anlässlich seiner Entscheidung für das mobileTAN-Verfahren~~ bekannt zu geben. ~~Eine Änderung der bekannt gegebenen Mobiltelefonnummer kann durch den Kunden persönlich beim Kundenbetreuer vorgenommen oder auch direkt im Electronic Banking geändert werden,~~ Die für die Zusendung der SMS bekannt gegebene Mobiltelefonnummer kann durch den Kunden persönlich in einem Standort der Bank oder - sofern dem Kunden eine SMS ~~mit der dafür erforderlichen mobileTAN~~ auf die bei der ~~Schoellerbank~~ Bank bisher gespeicherte

	Mobiltelefonnummer gesendet werden kann - im Internetbanking mittels mobileTAN geändert werden. Die Möglichkeit der Änderung der Mobiltelefonnummer und die Möglichkeit der Änderung der Art der Zustellung von mobileTAN via Internetbanking können aus Sicherheitsgründen vonseiten der Bank ausgesetzt werden, wenn objektive Gründe im Zusammenhang mit der Sicherheit der persönlichen Identifikationsmerkmale oder der Systeme, für die sie benutzt werden können, dies rechtfertigen.
In der SMS mit der mobileTAN werden zu Kontrollzwecken auch Angaben über die durchzuführende Transaktion, insbesondere Empfänger-IBAN und Betrag oder ein Referenzcode (Elektronischer Begleitzettel) und Kontrollwert (Summe aller Aufträge), mitgeliefert. Eine mobileTAN kann nur für die Durchführung jener Transaktion verwendet werden, für die sie angefordert wurde, und behält maximal 30 Tage Gültigkeit. Sofern ein erfasster Überweisungsauftrag nach Anforderung der mobileTAN verändert wurde, kann die zugesandte mobileTAN nicht mehr verwendet werden, sondern es muss eine neue mobileTAN angefordert werden. Sobald eine mobileTAN verwendet wurde, verliert sie ihre Gültigkeit.	In der Nachricht ~~SMS~~ mit der mobileTAN werden dem Kunden zu Kontrollzwecken auch Angaben über die durchzuführende Transaktion~~,~~ (insbesondere bei Zahlungsaufträgen: International Bank Account Number (IBAN) bzw. Kontonummer des Empfängers, Bank Identifier Code (BIC) bzw. Bankleitzahl der Bank des Empfängers und der Überweisungsbetrag) ~~Empfänger-IBAN und Betrag oder ein Referenzcode (Elektronischer Begleitzettel) und Kontrollwert (Summe aller Aufträge),~~ mitgeliefert. Eine mobileTAN kann nur für die Durchführung jener Transaktion verwendet werden, für die sie angefordert wurde~~, und behält maximal 30 Tage Gültigkeit~~. Sofern ein erfasster Überweisungsauftrag nach Anforderung der mobileTAN verändert wurde, kann die zugesandte mobileTAN nicht mehr verwendet werden, sondern es muss eine neue mobileTAN angefordert werden. Sobald eine mobileTAN verwendet wurde, verliert sie ihre Gültigkeit.
Der Kunde hat zu beachten, dass er eine SMS mit einer mobileTAN nur dann auf das Mobiltelefon erhalten kann, wenn die Voraussetzungen für den Empfang von SMS erfüllt sind, wie z.B., dass das Telefon technisch in der Lage ist SMS zu empfangen, die vertraglichen Grundlagen mit dem Mobiltelefonprovider zum Empfang von SMS gegeben sind und dass sich der Kunde in einem Gebiet befindet, für das sein Mobiltelefonprovider die Zustellung einer SMS vorsieht.	~~Der Kunde hat zu beachten, dass er eine SMS mit einer mobileTAN nur dann auf das Mobiltelefon erhalten kann, wenn die Voraussetzungen für den Empfang von SMS erfüllt sind,~~ Bei der Nutzung des mobileTAN-Verfahrens ist der Kunde verpflichtet, die in der Nachricht gemeinsam mit der mobileTAN übermittelten Auftragsdaten (z. B. IBAN des Empfängerkontos, Überweisungsbetrag) auf Übereinstimmung mit seinem Auftrag zu prüfen und die mobileTAN nur im Falle einer Übereinstimmung dieser Auftragsdaten zusammen mit dem Passwort zu verwenden. Zustellung der mobileTAN per SMS: Der Kunde kann nur dann eine SMS mit einer mobileTAN auf das Mobiltelefon erhalten, wenn die Voraussetzungen für den Empfang von SMS erfüllt sind, wie z.B. dass: - das Telefon technisch in der Lage ist, SMS zu empfangen, - die vertraglichen Grundlagen mit dem Mobiltelefonprovider zum Empfang von SMS gegeben sind und ~~dass~~ - sich der Kunde in einem Gebiet befindet, für das sein Mobiltelefonprovider die Zustellung einer SMS vorsieht.
• tresorTAN Die Übermittlung der für die Autorisierung von Aufträgen erforderlichen Transaktionsnummern erfolgt an die Tresor-App, die von der Schoellerbank zur Verfügung gestellt wird. Die App muss zuvor auf einem mobilen Endgerät des Kunden, inklusive Herstellung der Gerätebindung, installiert sein. Die Authentifizierung erfolgt mittels Gerätebindung und den vom Kunden vergebenen Zugangsdaten (Verfügernummer, Verfügername und persönliche Identifikationsnummer). Auch ein Zugriff mittels vereinfachter Authentifizierung (Gerätebindung in Kombination mit vierstelligem PIN-Code = shortPIN und Fingerprint/Touch ID) ist möglich. Der Kunde kann die Gerätebindung und seine shortPIN jederzeit im Online	~~• tresorTAN~~ ~~Die Übermittlung der für die Autorisierung von Aufträgen erforderlichen Transaktionsnummern erfolgt an die Tresor-App, die von der Schoellerbank zur Verfügung gestellt wird. Die App muss zuvor auf einem mobilen Endgerät des Kunden, inklusive Herstellung der Gerätebindung, installiert sein. Die Authentifizierung erfolgt mittels Gerätebindung und den vom Kunden vergebenen Zugangsdaten (Verfügernummer, Verfügername und persönliche Identifikationsnummer). Auch ein Zugriff mittels vereinfachter Authentifizierung (Gerätebindung in Kombination mit vierstelligem PIN-Code = shortPIN und Fingerprint/Touch ID) ist möglich. Der Kunde kann die Gerätebindung und seine shortPIN jederzeit im Online~~

PC282D-Gegenüberstellung 20200101

Banking ändern. Hinweis: die Verwendung der tresorTAN ist nur mit Internetverbindung möglich.

Zu Kontrollzwecken werden in der Nachricht mit der TAN auch Angaben über die durchzuführenden Aufträge mitgeliefert. Bei Überweisungsaufträgen werden insbesondere Empfänger-IBAN und Betrag oder ein Referenzcode (Elektronischer Begleitzettel) und Kontrollwert (Summe aller Aufträge) angeführt. Der Kunde ist verpflichtet, diese auf Übereinstimmung mit den eingegebenen Aufträgen zu prüfen. Die tresorTAN darf nur bei Übereinstimmung eingegeben werden.

Die jeweilige tresorTAN ist nur für die Durchführung jener Transaktion gültig, für die sie angefordert wurde und verliert ihre Gültigkeit, sobald sie verwendet wurde.

(siehe Punkt 8. App)

• cardTAN
Bei der Verwendung des cardTAN-Verfahrens wird die TAN zur Autorisierung von Transaktionen im Electronic Banking durch ein spezielles, auf dem Chip einer Bankomatkarte (TANCard) gespeichertes Programm errechnet. Für das cardTAN-Verfahren benötigt der Kunde eine aktive cardTAN-fähige Bankkarte (Maestro Bankomatkarte der Schoellerbank mit cardTAN-Logo auf der Rückseite) und einen speziellen Kartenleser (cardTAN-Generator). Darüber hinaus muss das cardTAN-Verfahren seitens der Schoellerbank für den Kunden aktiviert werden.

~~Banking ändern. Hinweis: die Verwendung der tresorTAN ist nur mit Internetverbindung möglich.~~

~~Zu Kontrollzwecken werden in der Nachricht mit der TAN auch Angaben über die durchzuführenden Aufträge mitgeliefert. Bei Überweisungsaufträgen werden insbesondere Empfänger-IBAN und Betrag oder ein Referenzcode (Elektronischer Begleitzettel) und Kontrollwert (Summe aller Aufträge) angeführt. Der Kunde ist verpflichtet, diese auf Übereinstimmung mit den eingegebenen Aufträgen zu prüfen. Die tresorTAN darf nur bei Übereinstimmung eingegeben werden.~~

~~Die jeweilige tresorTAN ist nur für die Durchführung jener Transaktion gültig, für die sie angefordert wurde und verliert ihre Gültigkeit, sobald sie verwendet wurde.~~

b) Schoellerbank ID App
Die Schoellerbank ID App ist eine Applikation für (mobile) Endgeräte und ermöglicht die Authentifizierung des Kunden. Um die Authentifizierung durchzuführen, bekommt der Kunde im Internetbanking eine Zahl angezeigt. Zur gleichen Zeit wird dem Kunden in der Schoellerbank ID App der konkrete Authentifizierungsbedarf (z.B. die Details zu einem Zahlungsauftrag) und eine Reihe von Zahlen angezeigt. Um die Authentifizierung durchzuführen muss der Kunde nun jene Zahl auswählen (durch "Touch" auf die Zahl), die ihm auch im Internetbanking angezeigt wird.
Jedes Endgerät, auf dem die App installiert ist, muss dem Kunden nach Installation der Anwendung zugeordnet werden (= Herstellung der Gerätebindung). Die Authentifizierung erfolgt mittels Gerätebindung und shortPIN oder eines biometrischen Verfahrens (Fingerprint oder FaceID). Der Benutzer kann die Gerätebindung und seine persönliche shortPIN direkt im Internetbanking ändern.
Zu Kontrollzwecken werden dem Kunden im Zuge der Freigabe auch Angaben über die durchzuführende Transaktion, insbesondere Empfänger-IBAN und Betrag oder ein Referenzcode (Elektronischer Begleitzettel) und Kontrollwert (Summe aller Aufträge) mitgeliefert. Der Kunde ist verpflichtet, diese auf Übereinstimmung mit den im Internetbanking eingegebenen Aufträgen zu prüfen. Die Freigabe darf nur bei Übereinstimmung erteilt werden.

Der Kunde kann nur dann eine Zahl von der Schoellerbank ID App auf einem mobilen Endgerät wie Smartphone oder Tablet erhalten, wenn folgende Voraussetzungen gegeben sind:
- eine aktuelle Version der vom Kunden verwendeten Internetbanking-App der Bank (Schoellerbank ID App) installiert ist,
- sich der Kunde in einem Gebiet befindet, für das eine Internet-Datenverbindung über seinen Mobiltelefon-provider oder per WLAN über einen Netzbetreiber gegeben ist.

• **cardTAN**
Möchte der Kunde das cardTAN-Verfahren verwenden, hat er dies der Bank entweder persönlich in einem Standort der Bank, telefonisch oder schriftlich per Post mitzuteilen.

Für die Verwendung des cardTAN-Verfahrens benötigt er einen speziellen Kartenleser (cardTAN-Generator), ~~Bei der Verwendung des cardTAN-Verfahrens wird die TAN zur Autorisierung von Transaktionen im Electronic Banking durch ein spezielles, auf dem Chip einer Bankomatkarte (TANCard) gespeichertes Programm errechnet. Für das~~

Nach der Eingabe der Auftragsdaten wählt der Kunde das cardTAN-Verfahren zur Autorisierung aus. Dann wird die Bankkarte (TANcard) in den cardTAN-Generator eingesteckt und mittels Eingabe der eigens für dieses Verfahren erstellten EB-PIN aktiviert. Den EB-PIN erhält der Kunde im Rahmen der Freischaltung für das cardTAN-Verfahren von der Schoellerbank. Der Kunde kann den EB-PIN direkt im Electronic Banking ändern. In weiterer Folge werden bestimmte Daten der eingegebenen Transaktion entweder über eine optische Schnittstelle („Flicker“) oder durch manuelle Eingabe an den cardTAN-Generator übertragen, im Kartenchip verarbeitet und eine TAN zur Freigabe des Auftrags erzeugt. Diese cardTAN ist vom Kunden einzugeben und danach kann der Auftrag zur Schoellerbank übertragen werden.

~~cardTAN-Verfahren benötigt der Kunde~~ eine aktive (weder gesperrte noch abgelaufene) cardTAN-fähige ~~Bankkarte (Maestro-Bankomatkarte der Schoellerbank mit cardTAN-Logo auf der Rückseite) und einen speziellen Kartenleser (cardTAN-Generator)~~ Karte (Debitkarte oder TANcard), sowie einen EB-PIN (Electronic Banking PIN). ~~Darüber hinaus muss das cardTAN-Verfahren seitens der Schoellerbank für den Kunden aktiviert werden.~~

Ein cardTAN-Generator kann vom Kunden direkt bei der Bank angefordert werden. Nachdem die cardTAN-fähige Karte (Debitkarte oder TANcard) in den cardTAN-Generator eingeführt und die EB-PIN eingegeben wurde, werden Daten der im Internetbanking vorzunehmenden Anmeldung oder Transaktion entweder über eine optische Schnittstelle (siehe Modus „Flicker“) oder durch manuelle Eingabe im cardTAN-Generator erfasst und verarbeitet. Dann wird über ein spezielles, auf dem Chip der Debitkarte bzw. TANcard gespeichertes Programm eine cardTAN erzeugt. Die cardTAN ist vom Kunden im Internetbanking einzugeben und wird von der Bank auf Gültigkeit geprüft. Der cardTAN-Generator kann im Modus „Flicker“ oder „manuelle Eingabe“ verwendet werden. Der Modus „Flicker“ ist die einfachere Methode, bei Problemen mit der Wiedergabe oder Übernahme des Flicker-Codes kann durch den Kunden durch Nutzung einer im Internetbanking angebotenen Umschaltmöglichkeit auf „manuelle Eingabe am cardTAN-Generator“ geändert werden.

~~Nach der Eingabe der Auftragsdaten wählt der Kunde das cardTAN-Verfahren zur Autorisierung aus. Dann wird die Bankkarte (TANcard) in den cardTAN-Generator eingesteckt und mittels Eingabe der eigens für dieses Verfahren erstellten EB-PIN aktiviert. Den EB-PIN erhält der Kunde im Rahmen der Freischaltung für das cardTAN-Verfahren von der Schoellerbank. Der Kunde kann den EB-PIN direkt im Electronic Banking ändern. In weiterer Folge werden bestimmte Daten der eingegebenen Transaktion entweder über eine optische Schnittstelle („Flicker“) oder durch manuelle Eingabe an den cardTAN-Generator übertragen, im Kartenchip verarbeitet und eine TAN zur Freigabe des Auftrags erzeugt. Diese cardTAN ist vom Kunden einzugeben und danach kann der Auftrag zur Schoellerbank übertragen werden.~~

Bei der „Flicker-Methode“ werden die für die Berechnung der cardTAN erforderlichen Daten vom Bankserver mittels einer schwarz/weiß blinkenden Grafik über optische Schnittstellen vom Bildschirm des Kunden an den cardTAN-Generator übertragen. Die übertragenen Transaktionsdaten werden zu Kontrollzwecken durch den Kunden am Display des cardTAN-Generators angezeigt. Der Kunde ist dabei verpflichtet, die am cardTAN-Generator generierten Auftragsdaten mit den im Electronic Banking eingegebenen Aufträgen abzugleichen und die cardTAN nur im Falle einer Übereinstimmung der Transaktionsdaten zu verwenden.

~~Bei der „Flicker-Methode“ werden~~ Modus „Flicker“: Die für die Berechnung der cardTAN erforderlichen Daten, insbesondere die Transaktionsdaten, werden vom Bankserver mittels einer schwarz/weiß blinkenden Grafik über optische Schnittstellen vom Bildschirm des Eingabegeräts des Kunden (z.B. Computer, Tablet, etc.) an den cardTAN-Generator übertragen. Die ~~übertragenen~~ Transaktionsdaten, welche die vom Kunden zu autorisierende Transaktion repräsentieren, werden zur Überprüfung durch den Benutzer ~~werden zu Kontrollzwecken durch den Kunden~~ am Display des cardTAN-Generators angezeigt. ~~Der Kunde ist dabei verpflichtet, die am cardTAN-Generator generierten Auftragsdaten mit den im Electronic Banking eingegebenen Aufträgen abzugleichen und die cardTAN nur im Falle einer Übereinstimmung der Transaktionsdaten zu verwenden.~~ Bei der Nutzung des cardTAN-Verfahrens mit dem Modus „Flicker“ ist der Kunde verpflichtet, die übermittelten Transaktionsdaten (z.B. bei Zahlungsaufträgen IBAN des Empfängerkontos, Überweisungsbetrag) auf Übereinstimmung mit seinem Auftrag zu prüfen und die cardTAN nur im Falle einer Übereinstimmung dieser Transaktionsdaten zu verwenden.

Modus „manuelle Eingabe“: Dabei müssen bestimmte auf der Eingabemaske im Internetbanking abgefragte Daten, insbesondere die Transaktionsdaten, durch den Kunden selbstständig am cardTAN-Generator erfasst werden. Beim Modus „manuelle Eingabe“ hat der Kunde die eingegebenen Transaktionsdaten auf Übereinstimmung mit seinem Auftrag zu prüfen und die dafür erzeugte cardTAN nur im Falle einer Übereinstimmung dieser Transaktionsdaten zu verwenden.

Eine cardTAN ist nur für die Durchführung jener Aufträge gültig, für die sie generiert wurde. Wird ein erfasster Auftrag nach Generierung der cardTAN verändert, verliert die cardTAN ihre Gültigkeit und muss vom cardTAN-Generator neu erzeugt werden. Sobald die cardTAN verwendet wurde, verliert sie ebenfalls ihre Gültigkeit.

Eine cardTAN ~~ist~~ kann nur für die Durchführung jener ~~Aufträge gültig, für die sie generiert~~ Transaktion verwendet werden, für die sie erzeugt wurde. ~~Wird~~ Sofern ein erfasster Überweisungsauftrag nach ~~Generierung~~ Erzeugung der cardTAN verändert~~, verliert die cardTAN ihre Gültigkeit und muss~~ wurde, kann diese cardTAN nicht mehr verwendet werden, sondern muss eine neue cardTAN vom cardTAN-Generator ~~neu~~ erzeugt werden. Sobald ~~die~~ eine cardTAN verwendet wurde, verliert sie ihre Gültigkeit.

Digitale Signatur

Die Freigabe der Transaktion erfolgt durch Verwendung der Karte mit digitaler Signatur (z.B. Bürgerkarten-funktion auf der e-card, a.sign premium). Für die Nutzung ist vom Kunden eine lokale Bürgerkartenumgebung (oder eine gleichwertige Software) samt Kartenleser sicherzustellen. Zu Kontrollzwecken werden auch die Angaben über die durchzuführenden Aufträge angezeigt. Bei Überweisungsaufträgen werden insbesondere Empfänger-IBAN und Betrag oder ein Referenzcode und Kontrollwert (Summe aller Aufträge) angeführt. Der Kunde ist verpflichtet, diese auf Übereinstimmung mit den eingegebenen Aufträgen zu prüfen. Die Signatur-PIN darf nur bei Übereinstimmung eingegeben werden.

~~**Digitale Signatur**~~

~~Die Freigabe der Transaktion erfolgt durch Verwendung der Karte mit digitaler Signatur (z.B. Bürgerkarten-funktion auf der e-card, a.sign premium). Für die Nutzung ist vom Kunden eine lokale Bürgerkartenumgebung (oder eine gleichwertige Software) samt Kartenleser sicherzustellen. Zu Kontrollzwecken werden auch die Angaben über die durchzuführenden Aufträge angezeigt. Bei Überweisungsaufträgen werden insbesondere Empfänger-IBAN und Betrag oder ein Referenzcode und Kontrollwert (Summe aller Aufträge) angeführt. Der Kunde ist verpflichtet, diese auf Übereinstimmung mit den eingegebenen Aufträgen zu prüfen. Die Signatur-PIN darf nur bei Übereinstimmung eingegeben werden.~~

Dieses Signaturverfahren ist keine Anwendung der Schoellerbank. Eine Sperre bzw. ein Widerruf des Zertifikats ist beim Zertifikatsanbieter zu veranlassen.

~~Dieses Signaturverfahren ist keine Anwendung der Schoellerbank. Eine Sperre bzw. ein Widerruf des Zertifikats ist beim Zertifikatsanbieter zu veranlassen.~~

Für die Nutzung im Electronic Banking kann der Kunde dieses Zeichnungsverfahren im Online Banking und Business Banking mit seiner Signaturkarte aktivieren oder die Schoellerbank durch Bekanntgabe der Cardholder Identification Number (CIN) mit der Aktivierung beauftragen.

~~Für die Nutzung im Electronic Banking kann der Kunde dieses Zeichnungsverfahren im Online Banking und Business Banking mit seiner Signaturkarte aktivieren oder die Schoellerbank durch Bekanntgabe der Cardholder Identification Number (CIN) mit der Aktivierung beauftragen.~~

2.6 Biometrische Daten

Bei Verwendung von Internetbanking-Apps der Bank auf mobilen Geräten (Smartphone oder Tablet) kann der Kunde - abhängig von den technischen Möglichkeiten des Endgeräts - optional das Passwort mit biometrischen Daten (wie Fingerprints oder FaceID), deren Erfassung das jeweilige Mobilgerät ermöglicht, mit der jeweiligen Internetbanking-App verbinden. In diesem Fall ersetzt die Verifizierung des Kunden anhand der von ihm in der Internetbanking-App gespeicherten biometrischen Daten die Angabe des Passworts beim Login in das mobile Internetbanking.

2.7 Persönliche Identifikationsmerkmale

Benutzername (BK), Passwort, Transaktionsnummern (TAN) sowie in Internetbanking Apps der Bank gespeicherte biometrische Daten bilden beim Internetbanking die persönlichen Identifikationsmerkmale des Kunden.

3. Authentifizierung
Die Bank prüft die Berechtigung des Kunden für die Nutzung des Internetbankings anhand der persönlichen Identifikationsmerkmale.

4. Inanspruchnahme von Dienstleistungen
Die Inanspruchnahme von Dienstleistungen im Rahmen des Schoellerbank Electronic Banking, die durch eine TAN oder durch Verwendung der digitalen Signatur gesichert ist, berechtigt die Schoellerbank Aufträge, die ihr im Rahmen dieser Geschäftsverbindung erteilt werden, auf Rechnung des Kunden durchzuführen.

Der Kunde nimmt jedoch zur Kenntnis, dass Dienstleistungen, mit denen über seine Konten bzw. Depots nicht disponiert wird, wie etwa Abfragen des Kontostandes und Depotbewertungen, ohne TAN oder digitaler Signatur möglich sind und daher die strikte Geheimhaltung aller persönlichen Identifikationsmerkmale in seinem dringenden Interesse liegt.

Das Schoellerbank Electronic Banking ist für den Kunden täglich von 00:00 bis 24:00 Uhr verfügbar. Im Zeitraum von 00:00 bis 06:00 Uhr können Wartungsarbeiten an den Bankrechnern erfolgen, wodurch Einschränkungen bei der Nutzung von Electronic Banking entstehen können. Müssen Wartungsarbeiten von 06:00 bis 24:00 Uhr stattfinden, wird die Schoellerbank die Kunden nach Möglichkeit darauf im Vorhinein hinweisen.

(siehe Punkt 6. Transaktionen über Electronic Banking)

~~**4. Inanspruchnahme von Dienstleistungen**~~
~~Die Inanspruchnahme von Dienstleistungen im Rahmen des Schoellerbank Electronic Banking, die durch eine TAN oder durch Verwendung der digitalen Signatur gesichert ist, berechtigt die Schoellerbank Aufträge, die ihr im Rahmen dieser Geschäftsverbindung erteilt werden, auf Rechnung des Kunden durchzuführen.~~

~~Der Kunde nimmt jedoch zur Kenntnis, dass Dienstleistungen, mit denen über seine Konten bzw. Depots nicht disponiert wird, wie etwa Abfragen des Kontostandes und Depotbewertungen, ohne TAN oder digitaler Signatur möglich sind und daher die strikte Geheimhaltung aller persönlichen Identifikationsmerkmale in seinem dringenden Interesse liegt.~~

~~Das Schoellerbank Electronic Banking ist für den Kunden täglich von 00:00 bis 24:00 Uhr verfügbar. Im Zeitraum von 00:00 bis 06:00 Uhr können Wartungsarbeiten an den Bankrechnern erfolgen, wodurch Einschränkungen bei der Nutzung von Electronic Banking entstehen können. Müssen Wartungsarbeiten von 06:00 bis 24:00 Uhr stattfinden, wird die Schoellerbank die Kunden nach Möglichkeit darauf im Vorhinein hinweisen.~~

4. Transaktionen über Internetbanking
4.1 Die Dispositionen und Willenserklärungen (zusammen kurz: Transaktionen) können über das Internetbanking grundsätzlich 24 Stunden pro Tag und 7 Tage pro Woche an die Bank übermittelt werden. Da fallweise Wartungs- und Servicearbeiten an den Bankrechnern der Bank vorzunehmen sind, ist in der Zeit von 00:00 Uhr bis 6:00 Uhr ein Servicefenster vorgesehen. In diesem Zeitraum kann das Internetbanking bei Vornahme solcher Wartungs- und Servicearbeiten zeitweilig nicht zur Verfügung stehen. Müssen Wartungsarbeiten von 06:00 Uhr bis 24:00 Uhr stattfinden, wird die Bank die Kunden nach Möglichkeit darauf im Vorhinein hinweisen.

4.2 Der Kunde stellt die Verbindung zum Bankrechner dadurch her, dass er sich über die Homepage der Bank unter Verwendung seines Benutzernamens, seines Passworts und des jeweiligen Loginverfahrens in das Internetbanking einloggt.
Der Kunde hat die für die jeweils gewünschte Transaktion auf der Eingabemaske geforderten Angaben über Datenübertragungsleitung via Internet einzufügen. Jedenfalls hat der Kunde bei Überweisungsaufträgen immer den Kundenidentifikator des Empfängers anzugeben. Macht der Kunde über diesen hinausgehende Angaben zum Empfänger, wie insbesondere zum Namen des Empfängers oder dem Verwendungszweck, sind diese nicht Teil des Kundenidentifikators, dienen daher lediglich zu Dokumentationszwecken und bleiben bei der Ausführung der Transaktion seitens der Bank unbeachtet. Sodann hat der Kunde die gewünschte Transaktion unter Verwendung der für die jeweilige Transaktion generierten TAN und anschließender Betätigung des für die Freigabe vorgesehenen Buttons abzuschließen.

4.3 Der Zeitpunkt, zu dem eine Transaktion via Internetbanking bei der Bank einlangt, gilt als

Eingangszeitpunkt. Geht eine Transaktion via Internetbanking nicht an einem Geschäftstag der Bank oder aber nach einem Zeitpunkt nahe am Ende eines Geschäftstages ein, so wird diese Transaktion so behandelt, als wäre sie erst am nächsten Geschäftstag eingegangen. Die Bank veröffentlicht diese Uhrzeiten in den „Informationen der Schoellerbank AG zu Zahlungsdienstleistungen für Verbraucher“, welche sie elektronisch auf ihrer Homepage bereithält oder in Schriftform dem Kunden auf dessen Verlangen in ihren Geschäftsstellen aushändigt oder postalisch übermittelt.

Der Kunde kann auch vorsehen, dass der Auftrag an einem in der Zukunft liegenden Datum (Terminauftrag) durchgeführt werden soll. Ist das bei einem Terminauftrag gewünschte Datum kein Geschäftstag der Bank, ist der Terminauftrag so zu behandeln, als sei er erst am darauffolgenden Geschäftstag eingegangen.

4.4 Im Rahmen des Internetbankings können zu einem Konto beliebig viele Überweisungsaufträge erteilt werden. Die Bank ist zur Durchführung eines Überweisungsauftrags nur dann verpflichtet, wenn dafür auf dem jeweiligen Konto des Kunden vollständige Deckung vorhanden ist. Der Kunde hat auch die Möglichkeit, mehrere Überweisungsaufträge zusammenzufassen und mit einer einzigen TAN freizugeben.

4.5 Allgemeines über Limits bei mobileTAN, Schoellerbank ID und bei cardTAN:

4.5.1 Beim Internetbanking können Transaktionslimits gesetzt werden.
Bei einem Transaktionslimit wird die Höhe jenes Betrages festgelegt, bis zu dem ein Überweisungsauftrag allein oder mehrere Überweisungsaufträge gemeinsam mit einer einzigen TAN erteilt werden können.

4.5.2 Ein Limit kann entweder von der Bank einseitig festgelegt (siehe Punkt 4.5.3) oder zwischen Bank und Kunde einvernehmlich vereinbart werden. In beiden Fällen handelt es sich um ein „bankseitiges Limit“.

4.5.3 Die Bank ist berechtigt, ein bankseitiges Limit ohne Mitwirkung des Kunden einzuführen oder herabzusetzen, wenn

- objektive Gründe im Zusammenhang mit der Sicherheit der persönlichen Identifikationsmerkmale oder der Systeme, für die sie benutzt werden können, dies rechtfertigen, oder
- der Verdacht einer Erteilung von nicht autorisierten Aufträgen oder der betrügerischen Verwendung der persönlichen Identifikationsmerkmale besteht. Die Bank wird den Kunden über eine solche Einführung oder Herabsetzung und die Gründe hierfür möglichst vor, spätestens aber unverzüglich nach der Einführung oder Herabsetzung in der mit ihm vereinbarten Form informieren.

4.6 Ein autorisierter, bei der Bank im Wege des Internetbankings eingegangener Überweisungsauftrag kann nicht mehr widerrufen werden. Der Widerruf eines bei der Bank eingelangten Terminauftrages ist bis zum Ende des Geschäftstages vor dem vereinbarten Durchführungstag direkt im Internetbanking unter Verwendung einer gültigen TAN möglich.

4.7 eps Online-Überweisung
Im Rahmen des Internetbankings können auch eps Online-Überweisungen erteilt werden. Bei der eps Online-Überweisung handelt es sich um ein standardisiertes, Bezahlverfahren bei Einkäufen im Internet und bei Inanspruchnahme von E-Government Dienstleistungen.

Der Kunde erhält dabei auf der Website des Internet-Shops bzw. auf der E-Government-Webseite, die jeweils mit einem entsprechenden Logo für eps („e-payment standard“) und Online-Überweisung gekennzeichnet sind, die Möglichkeit, sich unter Verwendung seines Benutzernamens/BK, seines Passworts und des jeweiligen Loginverfahrens direkt in das Internetbanking einzuloggen und die Bezahlung mittels Überweisungsauftrag vorzunehmen. Die Freigabe einer eps Online-Überweisung erfolgt wie die Freigabe jeder anderen Überweisung im Internetbanking unter Verwendung einer TAN (siehe Punkt 4.2). Im gesamten Ablauf der eps Online-Überweisung werden keine bankspezifischen Daten des Kunden von einer dritten Stelle abgefragt oder zwischengespeichert, da der Kunde sich dabei direkt auf der Website der Bank oder in der Banking-App der Bank in das Internetbanking einloggt und dort den Überweisungsauftrag freigibt. Im Rahmen der Abwicklung einer eps Online-Überweisung werden von der Bank auch keine bankspezifischen Daten des Käufers an den Händler übertragen. Mit Freigabe der eps Online-Überweisung durch den Kunden garantiert die Bank gegenüber dem Internet Händler bzw. der E-Government-Behörde die Ausführung der Überweisung, sodass der Kunde diese eps Online-Überweisung nicht widerrufen kann. Die eps Online-Überweisung ist lediglich ein Instrument, mit dem der Kunde eine Bezahlung im Internet durch einen Überweisungsauftrag im Internetbanking vornehmen kann. Die zwischen dem Kunden und dem Händler bestehende vertragliche Beziehung wird durch die Verwendung der eps Online-Überweisung nicht tangiert, und es sind deshalb gegenüber der Bank keine Einwendungen aus dem Grundgeschäft zulässig.

5. Legitimation
Bei sämtlichen Geschäftsfällen im Rahmen des Electronic Banking wird die Berechtigung zu deren Vornahme ausschließlich anhand der persönlichen Identifikations-merkmale geprüft.

~~**5. Legitimation**~~
~~Bei sämtlichen Geschäftsfällen im Rahmen des Electronic Banking wird die Berechtigung zu deren Vornahme ausschließlich anhand der persönlichen Identifikations-merkmale geprüft.~~

5. Kontoinformationsdienstleister und Zahlungs-auslösedienstleister
5.1 Der Kunde kann bestimmten Kontoinformations-dienstleistern und Zahlungsauslösedienstleistern Zugriff auf ein oder mehrere seiner zum Internetbanking berechtigten Zahlungskonten gewähren, indem der Kunde die Dienste dieser Dienstleister in Anspruch nimmt.

5.2 Kontoinformationsdienstleister bieten konsolidierte Informationen über ein oder mehrere Zahlungskonten eines Kontoinhabers an, die auch bei verschiedenen Kreditinstituten geführt werden können. Zahlungsauslösedienstleister lösen auf Antrag eines Kontoinhabers einen Zahlungsauftrag in Bezug auf ein anderes Zahlungskonto aus, welches auch bei einem anderen Kreditinstitut geführt werden kann.

5.3 Nimmt der Kunde die Dienste der Kontoinformationsdienstleister oder der Zahlungsauslöse-dienstleister in Anspruch, indem der Kunde diesen Dienstleistern Zugriff auf sein Zahlungskonto bzw. seine

Zahlungskonten gewährt, so ist die Bank im Sinne der Delegierten Verordnung (EU) 2018/389 zu technischen Regulierungsstandards für eine starke Kunden-authentifizierung und für sichere offene Standards für die Kommunikation verpflichtet, mit diesen Dienstleistern auf sichere Weise zu kommunizieren und diesen die erforderlichen Authentifizierungsverfahren zur Überprüfung der Identität des Kunden bereitzustellen.

6. Transaktionen über Electronic Banking

6. Transaktionen über Electronic Banking

Der Kunde erteilt der Schoellerbank seine Aufträge, indem er Daten in von der Schoellerbank festgelegten Formaten sendet. Fehlerhafte oder unvollständige Daten werden vom Rechenzentrum der Schoellerbank nicht oder nur teilweise bearbeitet. Für jeden Auftrag (z.B. Überweisungsauftrag, Anlage eines Dauerauftrages, Wertpapierauftrag) hat der Kunde nach Anmeldung zum Schoellerbank Electronic Banking, mit den entsprechenden Identifikationsmerkmalen die für die jeweils gewünschte Transaktion geforderten Daten durch Eingabe einer gültigen TAN freizugeben.

Bei Verwendung der digitalen Signatur erfolgt anstelle der Eingabe einer TAN die Freigabe der Transaktion durch Verwendung der entsprechenden Berechtigungskarte und der dazugehörigen Berechtigungsmerkmale (Signatur-PIN). Der Zeitpunkt, zu dem eine Transaktion via Electronic Banking bei der Schoellerbank eingeht, gilt als Eingangszeitpunkt. Geht diese Transaktion nicht an einem Geschäftstag der Schoellerbank ein, so wird diese Transaktion so behandelt, als wäre sie erst am nächsten Geschäftstag eingegangen.
Die Durchführung der Aufträge erfolgt in der Regel dann taggleich, wenn die Daten bis spätestens zu dem für die jeweilige Auftragsart gültigen, im Schalteraushang bekannt gegebenen, nahe dem Ende eines Geschäftstages gelegenen Eingangszeitpunkt eines Bankwerktages in der Schoellerbank zur Bearbeitung vorliegen. Erfolgt die Übertragung nach diesem Eingangszeitpunkt, kann die Durchführung auch erst am nächsten Bankwerktag vorgenommen werden. Für Zahlungen, deren Durchführungstag in der Zukunft liegt, ist der entsprechende Durchführungstag unbedingt anzugeben.

Allfällige Rückmeldungen der Schoellerbank nach Entgegennahme von Aufträgen bestätigen nur den Empfang der übermittelten Daten, nicht jedoch die Durchführung der erteilten Aufträge. Die Bearbeitung eines jeden Auftrages erfolgt im Rahmen der banküblichen Arbeitsabläufe.

Elektronische Überweisungsaufträge im Rahmen des Electronic Banking ermächtigen uns, die Konten gemäß dem Antragsformular im Rahmen von Guthaben bzw. Dispositionsrahmen zu belasten. Die Schoellerbank ist nicht verpflichtet Aufträge auszuführen, wenn entsprechende Guthaben oder Dispositionsrahmen auf dem Konto nicht vorhanden sind, kann jedoch Verfügungen über Electronic Banking auch bei mangelnden Guthaben im Rahmen der AGB ausführen und das Konto belasten.
Der Kunde kann dabei wählen, ob der Auftrag zum nächstmöglichen bankinternen Buchungslauf oder aber an einem in der Zukunft liegenden Datum (Terminauftrag) durchgeführt werden soll. Ist das bei einem Terminauftrag gewünschte Datum kein Geschäftstag der Schoellerbank, ist der Terminauftrag so zu behandeln, als sei er erst am darauffolgenden Geschäftstag eingegangen. Der Kunde hat auch die Möglichkeit, mehrere Überweisungsaufträge

Siehe Punkt 4. Transaktionen über Internetbanking

~~**6. Transaktionen über Electronic Banking**~~

~~Der Kunde erteilt der Schoellerbank seine Aufträge, indem er Daten in von der Schoellerbank festgelegten Formaten sendet. Fehlerhafte oder unvollständige Daten werden vom Rechenzentrum der Schoellerbank nicht oder nur teilweise bearbeitet. Für jeden Auftrag (z.B. Überweisungsauftrag, Anlage eines Dauerauftrages, Wertpapierauftrag) hat der Kunde nach Anmeldung zum Schoellerbank Electronic Banking, mit den entsprechenden Identifikationsmerkmalen die für die jeweils gewünschte Transaktion geforderten Daten durch Eingabe einer gültigen TAN freizugeben.~~

~~Bei Verwendung der digitalen Signatur erfolgt anstelle der Eingabe einer TAN die Freigabe der Transaktion durch Verwendung der entsprechenden Berechtigungskarte und der dazugehörigen Berechtigungsmerkmale (Signatur-PIN). Der Zeitpunkt, zu dem eine Transaktion via Electronic Banking bei der Schoellerbank eingeht, gilt als Eingangszeitpunkt. Geht diese Transaktion nicht an einem Geschäftstag der Schoellerbank ein, so wird diese Transaktion so behandelt, als wäre sie erst am nächsten Geschäftstag eingegangen.~~
~~Die Durchführung der Aufträge erfolgt in der Regel dann taggleich, wenn die Daten bis spätestens zu dem für die jeweilige Auftragsart gültigen, im Schalteraushang bekannt gegebenen, nahe dem Ende eines Geschäftstages gelegenen Eingangszeitpunkt eines Bankwerktages in der Schoellerbank zur Bearbeitung vorliegen. Erfolgt die Übertragung nach diesem Eingangszeitpunkt, kann die Durchführung auch erst am nächsten Bankwerktag vorgenommen werden. Für Zahlungen, deren Durchführungstag in der Zukunft liegt, ist der entsprechende Durchführungstag unbedingt anzugeben.~~

~~Allfällige Rückmeldungen der Schoellerbank nach Entgegennahme von Aufträgen bestätigen nur den Empfang der übermittelten Daten, nicht jedoch die Durchführung der erteilten Aufträge. Die Bearbeitung eines jeden Auftrages erfolgt im Rahmen der banküblichen Arbeitsabläufe.~~

~~Elektronische Überweisungsaufträge im Rahmen des Electronic Banking ermächtigen uns, die Konten gemäß dem Antragsformular im Rahmen von Guthaben bzw. Dispositionsrahmen zu belasten. Die Schoellerbank ist nicht verpflichtet Aufträge auszuführen, wenn entsprechende Guthaben oder Dispositionsrahmen auf dem Konto nicht vorhanden sind, kann jedoch Verfügungen über Electronic Banking auch bei mangelnden Guthaben im Rahmen der AGB ausführen und das Konto belasten.~~
~~Der Kunde kann dabei wählen, ob der Auftrag zum nächstmöglichen bankinternen Buchungslauf oder aber an einem in der Zukunft liegenden Datum (Terminauftrag) durchgeführt werden soll. Ist das bei einem Terminauftrag gewünschte Datum kein Geschäftstag der Schoellerbank, ist der Terminauftrag so zu behandeln, als sei er erst am darauf folgenden Geschäftstag eingegangen. Der Kunde hat auch die Möglichkeit, mehrere Überweisungsaufträge~~

PC282D-Gegenüberstellung 20200101

zusammenzufassen und mit einer einzigen TAN freizugeben.

Ein autorisierter, bei der Schoellerbank im Wege des Electronic Banking eingegangener Überweisungsauftrag kann nicht widerrufen werden. Der Widerruf eines Terminauftrages ist bis zum Ende des Geschäftstages vor dem vereinbarten Durchführungstag direkt im Electronic Banking unter Verwendung einer gültigen TAN möglich.

Die Schoellerbank ist berechtigt, Aufträge, die ihr im Rahmen einer Geschäftsverbindung mit einem Kunden, der nicht Verbraucher im Sinne des § 4 Z 20 Zahlungsdienstegesetz 2018 ist (nachfolgend kurz: Unternehmer) über Electronic Banking unter Verwendung der persönlichen Identifikationsmerkmale erteilt werden, auf dessen Rechnung durchzuführen, wenn sie ohne Verschulden zur Ansicht kommt, dass sie von diesem Kunden stammen und der unwirksame Auftrag nicht der Schoellerbank zurechenbar ist.

Das Schoellerbank Electronic Banking-System kennt keinen Unterschied zwischen Kontoinhaber und anderen legitimierten Teilnehmern. Der/Die Konto-/Depotinhaber übernimmt/übernehmen daher ausdrücklich die Haftung für allfällige Kontoüberziehungen durch andere legitimierte Teilnehmer und für Schäden, die durch deren sorgfaltswidriges Verhalten verursacht wurden.
Ist ein Teilnehmer auf dem Konto einzeln zeichnungsberechtigt, so ist er auch alleine befugt, Transaktionen für dieses Konto über Electronic Banking durchzuführen. Ist er kollektiv zeichnungsberechtigt, kann er Transaktionen über Electronic Banking nur mit einer berechtigten Person durchführen.

Ein nur von einem kollektiv zeichnungsberechtigten Verfüger mit seiner TAN erstgezeichneter Auftrag, der nicht binnen 28 Tagen vom zweiten kollektiv zeichnungsberechtigten Verfüger mittels seiner TAN gegengezeichnet und versandt wird, wird ohne weitere Kontoinformation seitens der Schoellerbank unwiderruflich und ohne Durchführung aus dem System gelöscht.

(siehe Punkt 10. Sorgfalt)

~~zusammenzufassen und mit einer einzigen TAN freizugeben.~~

~~Ein autorisierter, bei der Schoellerbank im Wege des Electronic Banking eingegangener Überweisungsauftrag kann nicht widerrufen werden. Der Widerruf eines Terminauftrages ist bis zum Ende des Geschäftstages vor dem vereinbarten Durchführungstag direkt im Electronic Banking unter Verwendung einer gültigen TAN möglich.~~

~~Die Schoellerbank ist berechtigt, Aufträge, die ihr im Rahmen einer Geschäftsverbindung mit einem Kunden, der nicht Verbraucher im Sinne des § 4 Z 20 Zahlungsdienstegesetz 2018 ist (nachfolgend kurz: Unternehmer) über Electronic Banking unter Verwendung der persönlichen Identifikationsmerkmale erteilt werden, auf dessen Rechnung durchzuführen, wenn sie ohne Verschulden zur Ansicht kommt, dass sie von diesem Kunden stammen und der unwirksame Auftrag nicht der Schoellerbank zurechenbar ist.~~

~~Das Schoellerbank Electronic Banking-System kennt keinen Unterschied zwischen Kontoinhaber und anderen legitimierten Teilnehmern. Der/Die Konto-/Depotinhaber übernimmt/übernehmen daher ausdrücklich die Haftung für allfällige Kontoüberziehungen durch andere legitimierte Teilnehmer und für Schäden, die durch deren sorgfaltswidriges Verhalten verursacht wurden.~~
~~Ist ein Teilnehmer auf dem Konto einzeln zeichnungsberechtigt, so ist er auch alleine befugt, Transaktionen für dieses Konto über Electronic Banking durchzuführen. Ist er kollektiv zeichnungsberechtigt, kann er Transaktionen über Electronic Banking nur mit einer berechtigten Person durchführen.~~

~~Ein nur von einem kollektiv zeichnungsberechtigten Verfüger mit seiner TAN erstgezeichneter Auftrag, der nicht binnen 28 Tagen vom zweiten kollektiv zeichnungsberechtigten Verfüger mittels seiner TAN gegengezeichnet und versandt wird, wird ohne weitere Kontoinformation seitens der Schoellerbank unwiderruflich und ohne Durchführung aus dem System gelöscht.~~

6. Sorgfalt

6.1 Der Kunde ist auch im eigenen Interesse verpflichtet, Passwort und TAN geheim zu halten und anderen Personen nicht offenzulegen (auch nicht den Mitarbeitern der Bank). Die biometrische Hinterlegung des Passworts (siehe Punkt 2.6) entbindet nicht von der Sorgfaltspflicht zur Geheimhaltung des Passworts und der TAN. Das Offenlegungsverbot des Passworts bzw. der TAN besteht nicht gegenüber Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern, deren Dienstleistungen der Kunde in Anspruch nimmt. Sobald der Kunde den Verdacht hat, dass eine andere Person Kenntnis seines Passworts hat oder eine nicht autorisierte Nutzung des Internetbankings erfolgt ist, hat er sein Passwort unverzüglich zu ändern. Aus Sicherheitsgründen wird dem Kunden empfohlen, sein Passwort regelmäßig (z.B. alle zwei Monate) selbstständig zu ändern. Die nicht autorisierte Nutzung des Internetbankings hat der Kunde unverzüglich der Internetbanking-Hotline (siehe Punkt 8.1) zu melden. Bei Diebstahl oder Verlust des Mobiltelefons zum Empfang der mobileTAN wird dem Kunden empfohlen, sein Mobiltelefon unverzüglich zu sperren.
6.2 Sollte beim Anmeldevorgang die URL nicht mit https://banking.schoellerbank.at/ beginnen oder sollte vom

Browser des Kunden das Schlosssymbol als Zeichen für eine verschlüsselte Übertragung der Daten nicht angezeigt werden, sind das Hinweise darauf, dass sich der Kunde nicht auf der Homepage der Bank befindet. Es besteht dann die Gefahr, dass es sich um eine von Unbekannten zu dem Zweck eingerichtete Website handelt, dem Kunden dessen persönliche Identifikationsmerkmale herauszulocken (Phishing). In diesem Fall empfiehlt die Bank den Anmeldevorgang abzubrechen und – sofern ein oder mehrere Identifikationsmerkmale auf jener Website bereits eingegeben wurden – unverzüglich die Internetbanking-Hotline (siehe Punkt 8.1) zu verständigen.

6.3 Bei der Nutzung des mobileTAN-Verfahrens oder der Schoellerbank ID App ist der Kunde verpflichtet, die in der Nachricht gemeinsam mit der mobileTAN übermittelten bzw. in der Schoellerbank ID App angezeigten Auftragsdaten (z. B. bei Zahlungsaufträgen IBAN des Empfängerkontos, Überweisungsbetrag) auf Übereinstimmung mit seinem Auftrag zu prüfen und die mobileTAN bzw. die in der Schoellerbank ID App angezeigte Zahl nur im Falle einer Übereinstimmung dieser Auftragsdaten zu verwenden. Bei der Nutzung des cardTAN-Verfahrens mit dem Modus „Flicker“ ist der Kunde verpflichtet, die übermittelten Transaktionsdaten (z.B. bei Zahlungsaufträgen IBAN des Empfängerkontos, Überweisungsbetrag) auf Übereinstimmung mit seinem Auftrag zu prüfen und die cardTAN nur im Falle einer Übereinstimmung dieser Transaktionsdaten zu verwenden. Bei der Nutzung des cardTAN-Verfahrens mit dem Modus „manueller Eingabe“ hat der Kunde die von ihm am cardTAN-Generator eingegebenen Transaktionsdaten auf Übereinstimmung mit seinem im Internetbanking erfassten Auftrag zu prüfen und die dafür erzeugte cardTAN nur im Falle einer Übereinstimmung dieser Transaktionsdaten zu verwenden.

6.4 Der Kunde ist verpflichtet bei der Nutzung von Internetbanking die in diesen Geschäftsbedingungen enthaltenen Bedingungen für die Nutzung einzuhalten und insbesondere bei der Erteilung von Aufträgen den Kundenidentifikator (siehe Punkt 4.2) korrekt anzugeben sowie dafür zu sorgen, dass er einen Überweisungsauftrag nur dann erteilt, wenn auf dem zu belastenden Konto eine zur Durchführung des Überweisungsauftrages ausreichende Kontodeckung vorhanden ist.

7. eps Online-Überweisung

7. eps Online-Überweisung

Im Rahmen von Online Banking können auch eps Online-Überweisungen erteilt werden. Bei der eps Online-Überweisung handelt es sich um ein standardisiertes, einfaches und sicheres Bezahlverfahren der österreichischen Banken für Einkäufe im Internet und bei Inanspruchnahme von E-Government- Dienstleistungen. Der Kunde erhält dabei auf der Website des Internet-Shops bzw. auf der E- Government-Website die Möglichkeit, sich unter Verwendung seiner Verfügernummer, seines Verfügernamens und PIN direkt in das Online Banking seiner Bank einzuloggen und die Bezahlung sodann mittels Überweisungsauftrag vorzunehmen. Die Freigabe einer eps Online-Überweisung erfolgt wie die Freigabe jeder anderen Überweisung im Online Banking durch Eingabe einer TAN. Der Bestellvorgang im Internet-Shop ist streng vom Bezahlvorgang im Online Banking getrennt.

Im gesamten Ablauf der eps Online-Überweisung werden keine bankspezifischen Daten des Kunden

Siehe Punkt 4.7. eps Online Überweisung

~~**7. eps Online-Überweisung**~~

~~Im Rahmen von Online Banking können auch eps Online-Überweisungen erteilt werden. Bei der eps Online-Überweisung handelt es sich um ein standardisiertes, einfaches und sicheres Bezahlverfahren der österreichischen Banken für Einkäufe im Internet und bei Inanspruchnahme von E-Government- Dienstleistungen. Der Kunde erhält dabei auf der Website des Internet-Shops bzw. auf der E- Government-Website die Möglichkeit, sich unter Verwendung seiner Verfügernummer, seines Verfügernamens und PIN direkt in das Online Banking seiner Bank einzuloggen und die Bezahlung sodann mittels Überweisungsauftrag vorzunehmen. Die Freigabe einer eps Online-Überweisung erfolgt wie die Freigabe jeder anderen Überweisung im Online Banking durch Eingabe einer TAN. Der Bestellvorgang im Internet-Shop ist streng vom Bezahlvorgang im Online Banking getrennt.~~

~~Im gesamten Ablauf der eps Online-Überweisung werden keine bankspezifischen Daten des Kunden~~

bekanntgegeben oder zwischengespeichert und auch keine bankspezifischen Daten des Käufers an den Händler übertragen. Mit Freigabe der eps Online-Überweisung durch den Kunden garantiert die Bank gegenüber dem Internet-Händler bzw. der E-Government-Behörde die Ausführung der Überweisung, sodass der Kunde diese eps Online-Überweisung nicht widerrufen kann.
Die eps Online-Überweisung ist lediglich ein Instrument, mit dem der Kunde eine Bezahlung im Internet durch einen Überweisungsauftrag im Online Banking vornehmen kann. Die zwischen dem Kunden und dem Händler bestehende vertragliche Beziehung wird durch die Verwendung der eps Online- Überweisung nicht tangiert, und es sind deshalb gegenüber der Schoellerbank keine Einwendungen aus dem Grundgeschäft zulässig.

~~bekanntgegeben oder zwischengespeichert und auch keine bankspezifischen Daten des Käufers an den Händler übertragen. Mit Freigabe der eps Online-Überweisung durch den Kunden garantiert die Bank gegenüber dem Internet-Händler bzw. der E-Government-Behörde die Ausführung der Überweisung, sodass der Kunde diese eps Online-Überweisung nicht widerrufen kann.~~
~~Die eps Online-Überweisung ist lediglich ein Instrument, mit dem der Kunde eine Bezahlung im Internet durch einen Überweisungsauftrag im Online Banking vornehmen kann. Die zwischen dem Kunden und dem Händler bestehende vertragliche Beziehung wird durch die Verwendung der eps Online- Überweisung nicht tangiert, und es sind deshalb gegenüber der Schoellerbank keine Einwendungen aus dem Grundgeschäft zulässig.~~

7. Berichtigung von nicht autorisierten Zahlungsvorgängen

Im Falle einer aufgrund eines nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorganges erfolgten Belastung kann der Kunde jedenfalls dann eine Berichtigung durch die Bank erwirken, wenn er die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorganges, jedoch spätestens 13 Monate nach dem Tag der Belastung hiervon unterrichtet hat, es sei denn, die Bank hat dem Kunden die Informationen über den jeweiligen Überweisungsauftrag bzw. über die jeweilige Zahlung, welche zulasten seines Kontos ausgeführt wurde (Referenz, Betrag, Währung, Entgelt, Zinsen, Wechselkurs, Wertstellung der Belastung), nicht in der mit ihm vereinbarten Weise mitgeteilt oder zugänglich gemacht. Andere Ansprüche des Kunden auf Berichtigung werden dadurch nicht ausgeschlossen. Im Falle eines nicht autorisierten Zahlungsvorganges wird die Bank dem Kunden den Betrag des nicht autorisierten Zahlungsvorgangs unverzüglich, auf jeden Fall spätestens bis zum Ende des folgenden Geschäftstags erstatten, nachdem sie von dem Zahlungsvorgang Kenntnis erhalten hat oder dieser ihr angezeigt wurde. Die Erstattung erfolgt dadurch, dass das belastete Konto wieder auf den Stand gebracht wird, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte, wobei der Betrag auf dem Zahlungskonto des Zahlers spätestens zum Tag der Kontobelastung wertzustellen ist. Hat die Bank der Finanzmarktaufsicht berechtigte Gründe für den Verdacht, dass ein betrügerisches Verhalten des Kunden vorliegt, schriftlich mitgeteilt, wird die Bank ihre Erstattungspflicht unverzüglich prüfen und erfüllen, wenn sich der Betrugsverdacht nicht bestätigt. Die Bank ist auch dann zur Erstattung eines nicht autorisierten Zahlungsvorgangs verpflichtet, wenn dieser über einen Zahlungsauslösedienstleister ausgelöst wurde.

8. App

8. App

Die Schoellerbank kann zur Nutzung elektronischer Dienste für ausgewählte Endgeräte Apps zur Verfügung stellen. Eine solche App muss vom Verfüger über den AppStore des jeweiligen Endgerätes separat installiert werden. Die im AppStore für die App hinterlegten Bestimmungen sind dabei zu beachten.

Ob eine App für ein bestimmtes Endgerät verwendet werden kann, ist abhängig von verschiedenen Parametern, z.B. Gerätemodell und Betriebssystemversion. Die Schoellerbank kann angesichts der Vielzahl der im Markt befindlichen Endgeräte und den Veränderungen dieser

Siehe 2.5 b) Schoellerbank ID App

~~**8. App**~~

~~Die Schoellerbank kann zur Nutzung elektronischer Dienste für ausgewählte Endgeräte Apps zur Verfügung stellen. Eine solche App muss vom Verfüger über den AppStore des jeweiligen Endgerätes separat installiert werden. Die im AppStore für die App hinterlegten Bestimmungen sind dabei zu beachten.~~

~~Ob eine App für ein bestimmtes Endgerät verwendet werden kann, ist abhängig von verschiedenen Parametern, z.B. Gerätemodell und Betriebssystemversion. Die Schoellerbank kann angesichts der Vielzahl der im Markt befindlichen Endgeräte und den Veränderungen dieser~~

Endgeräte aufgrund des technischen Fortschritts nicht sicherstellen, dass eine App (dauerhaft) auf einem Endgerät funktioniert. Ebenfalls kann die Schoellerbank keine Unterstützung bei der Installation oder Deinstallation der App auf einem speziellen Endgerät leisten.

~~Endgeräte aufgrund des technischen Fortschritts nicht sicherstellen, dass eine App (dauerhaft) auf einem Endgerät funktioniert. Ebenfalls kann die Schoellerbank keine Unterstützung bei der Installation oder Deinstallation der App auf einem speziellen Endgerät leisten.~~

Apps der Schoellerbank können dem Verfüger einen vereinfachten Login mit Hilfe der shortPIN ermöglichen (Gerätebindung in Kombination mit verfügerspezifischem vierstelligen PIN-Code). Nach dem Login mit der shortPIN bietet die App lediglich eingeschränkte Funktionen, insbesondere nur lesenden Zugriff auf Daten. Vor Zeichnung von Aufträgen muss die vollständige Authentifizierung mit den Zugangsmerkmalen des Verfügers erfolgen. Voraussetzung für die Nutzung der shortPIN ist, dass der Verfüger nach der Installation der App auf einem Endgerät eine Gerätebindung auf diesem Endgerät durchführt. Die Gerätebindung kann vom Verfüger über den dazugehörigen elektronischen Dienst gewartet werden, insbesondere kann die Gerätebindung hierüber gelöst werden.

~~Apps der Schoellerbank können dem Verfüger einen vereinfachten Login mit Hilfe der shortPIN ermöglichen (Gerätebindung in Kombination mit verfügerspezifischem vierstelligen PIN-Code). Nach dem Login mit der shortPIN bietet die App lediglich eingeschränkte Funktionen, insbesondere nur lesenden Zugriff auf Daten. Vor Zeichnung von Aufträgen muss die vollständige Authentifizierung mit den Zugangsmerkmalen des Verfügers erfolgen. Voraussetzung für die Nutzung der shortPIN ist, dass der Verfüger nach der Installation der App auf einem Endgerät eine Gerätebindung auf diesem Endgerät durchführt. Die Gerätebindung kann vom Verfüger über den dazugehörigen elektronischen Dienst gewartet werden, insbesondere kann die Gerätebindung hierüber gelöst werden.~~

Auf einigen Endgeräten kann der Verfüger zusätzlich zur shortPIN auch biometrische Verfahren nutzen, z.B. einen Fingerabdruck/Touch ID. Die Nutzung solcher biometrischer Verfahren hat den gleichen Zweck und führt zum gleichen Ergebnis wie die Eingabe einer shortPIN. Die Schoellerbank hat keinen Einfluss auf die Sicherheit und Zuverlässigkeit des biometrischen Verfahrens eines Endgerätes.

~~Auf einigen Endgeräten kann der Verfüger zusätzlich zur shortPIN auch biometrische Verfahren nutzen, z.B. einen Fingerabdruck/Touch ID. Die Nutzung solcher biometrischer Verfahren hat den gleichen Zweck und führt zum gleichen Ergebnis wie die Eingabe einer shortPIN. Die Schoellerbank hat keinen Einfluss auf die Sicherheit und Zuverlässigkeit des biometrischen Verfahrens eines Endgerätes.~~

Eine Gerätebindung und die anschließende Nutzung der shortPIN bzw. biometrischer Verfahren sollte der Verfüger nur für eigene Endgeräte durchführen. Der Verfüger hat dafür Sorge zu tragen, dass nur seine eigenen biometrischen Daten am Endgerät hinterlegt sind. Wenn der Verfüger ein Endgerät, auf dem eine App der Schoellerbank installiert wurde, dauerhaft weitergibt, insbesondere verkauft oder verschenkt, sollte der Verfüger die Gerätebindung lösen und alle Apps und Daten zu den elektronischen Diensten auf diesem Endgerät löschen, zum Beispiel durch das Zurücksetzen des Endgerätes in den Werkszustand entsprechend den Angaben des Herstellers.

~~Eine Gerätebindung und die anschließende Nutzung der shortPIN bzw. biometrischer Verfahren sollte der Verfüger nur für eigene Endgeräte durchführen. Der Verfüger hat dafür Sorge zu tragen, dass nur seine eigenen biometrischen Daten am Endgerät hinterlegt sind. Wenn der Verfüger ein Endgerät, auf dem eine App der Schoellerbank installiert wurde, dauerhaft weitergibt, insbesondere verkauft oder verschenkt, sollte der Verfüger die Gerätebindung lösen und alle Apps und Daten zu den elektronischen Diensten auf diesem Endgerät löschen, zum Beispiel durch das Zurücksetzen des Endgerätes in den Werkszustand entsprechend den Angaben des Herstellers.~~

Apps der Schoellerbank können Push-Nachrichten verwenden, wenn das Eingabegerät des Verfügers und der elektronische Dienst dies unterstützt und der Verfüger diese Funktion im elektronischen Dienst und in seinem Endgerät freigeschaltet hat. Über Push-Nachrichten kann sich der Verfüger über neue Mitteilungen in der App benachrichtigen lassen, auch wenn die App nicht im Vordergrund aktiv ist. Da die Zustellung von Push-Nachrichten von zahlreichen Faktoren abhängt, die nicht im Einflussbereich der Schoellerbank liegen, sind Push-Nachrichten lediglich eine Ergänzung der Mitteilungen innerhalb der App und kein garantierter Kommunikationskanal der Schoellerbank.

(siehe Punkt 13. Sperren)

~~Apps der Schoellerbank können Push-Nachrichten verwenden, wenn das Eingabegerät des Verfügers und der elektronische Dienst dies unterstützt und der Verfüger diese Funktion im elektronischen Dienst und in seinem Endgerät freigeschaltet hat. Über Push-Nachrichten kann sich der Verfüger über neue Mitteilungen in der App benachrichtigen lassen, auch wenn die App nicht im Vordergrund aktiv ist. Da die Zustellung von Push-Nachrichten von zahlreichen Faktoren abhängt, die nicht im Einflussbereich der Schoellerbank liegen, sind Push-Nachrichten lediglich eine Ergänzung der Mitteilungen innerhalb der App und kein garantierter Kommunikationskanal der Schoellerbank.~~

8. Sperren

8.1 Jeder Konto- bzw. Depotinhaber und jeder Zeichnungsberechtigte hat die Möglichkeit, seinen Benutzernamen wie folgt sperren zu lassen:

- jederzeit telefonisch bei der Internetbanking-Hotline der Bank, deren Telefonnummer auf der Homepage www.schoellerbank.at abrufbar ist, oder

- während der Öffnungszeiten der Bank persönlich oder schriftlich in jedem Standort der Bank. Eine innerhalb der Öffnungszeiten bei der Bank oder – zu welchem Zeitpunkt auch immer – bei der Internetbanking-Hotline veranlasste Sperre wird unmittelbar mit Einlangen des Sperrauftrags wirksam. Außerhalb der Öffnungszeiten bei der Bank schriftlich einlangende Sperraufträge werden unverzüglich nach Beginn der nächsten Öffnungszeit wirksam, oder
- jederzeit die Sperre im Internetbanking auch selbst unter dem Menüpunkt Sicherheit/Sperren online durchzuführen.

8.2 Die Bank ist berechtigt, einen Benutzernamen ohne Mitwirkung des Kunden zu sperren, wenn
- objektive Gründe im Zusammenhang mit der Sicherheit der persönlichen Identifikationsmerkmale oder der Systeme, für die sie benutzt werden können, dies rechtfertigen, oder
- der Verdacht einer Erteilung von nicht autorisierten Aufträgen oder der betrügerischen Verwendung der persönlichen Identifikationsmerkmale besteht.

Die Bank wird den Kunden über die Sperre und die Gründe hierfür – soweit dies nicht innerstaatliche oder gemeinschaftsrechtliche Rechtsvorschriften sowie gerichtliche oder verwaltungsbehördliche Anordnungen verletzen oder objektiven Sicherheitserwägungen zuwiderlaufen würde – möglichst vor, spätestens aber unverzüglich nach der Sperre in der mit ihm vereinbarten Form informieren.

8.3 Nach dreimaliger Falscheingabe der persönlichen Codes beim Login wird der Zugang zum Internetbanking temporär gesperrt, weitere Fehleingaben verlängern 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 Minuten 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 des persönlichen Codes ist der Zugang zum Internetbanking wiederhergestellt.

8.4 Der Kunde kann die Aufhebung der Sperre persönlich beantragen; dies kann auf jedem mit der Bank vereinbarten Kommunikationsweg geschehen (insbesondere über den Kundenbetreuer oder an einem Standort der Bank).

8.5 Die Bank ist berechtigt, einem Zahlungsauslösedienstleister oder einem Kontoinformationsdienstleister den Zugang zu einem zum Internetbanking berechtigten Zahlungskonto des Kunden zu verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Zahlungsauslösedienstleisters bzw. des Kontoinformationsdienstleisters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs dies rechtfertigen. Die Bank wird den Kunden – soweit eine Bekanntgabe der Sperre oder der Gründe für die Sperre nicht eine gerichtliche oder verwaltungsbehördliche Anordnung verletzen bzw. österreichischen oder

gemeinschaftsrechtlichen Rechtsnormen oder objektiven Sicherheitserwägungen zuwiderlaufen würde – von einer Sperre des Zugriffs durch einen Zahlungsauslöse-dienstleister bzw. Kontoinformationsdienstleister auf ein Zahlungskonto des Kunden und über deren Gründe in einer mit dem Kunden vereinbarten Kommunikationsform möglichst vor, spätestens aber unverzüglich nach der Sperre informieren.

9. Elektronische Wertpapieraufträge

9. Elektronische Wertpapieraufträge
Elektronische Wertpapieraufträge im Rahmen von Online Banking ermächtigen die Schoellerbank im Falle von Kaufaufträgen, die Konten gemäß dem „Antrag zur Teilnahme am Online Banking und zur Online-Abwicklung von Wertpapieraufträgen“ bzw. „Antrag zur Teilnahme am Online Banking inklusive Portfolioanalyse und zur Online-Abwicklung von Wertpapieraufträgen“ im Rahmen von Guthaben bzw. Dispositionsrahmen zu belasten. Die Schoellerbank ist berechtigt, Wertpapieraufträge ohne entsprechende Deckung nicht durchzuführen.

Erteilt der Kunde elektronische Wertpapieraufträge, weist die Schoellerbank darauf hin, dass sie nur als Vermittler und Depotbank tätig ist und die vom Kunden erteilten Aufträge nur dahin überprüft, ob die gewünschten Produkte im Hinblick auf die von ihm eingeholten Informationen zu seinen Kenntnissen und Erfahrungen im Anlagebereich für ihn angemessen sind. Eine Überprüfung im Hinblick auf seine Anlageziele und seine finanzielle Risikofähigkeit findet bei derartigen elektronischen Wertpapieraufträgen jedoch nicht statt. Entspricht der vom Kunden ohne vorgängige Beratung erteilte elektronische Wertpapierauftrag nicht seinen Kenntnissen und Erfahrungen im Anlagebereich, ist die Schoellerbank berechtigt, diesen nicht durchzuführen.

Über Online Banking können nur für einen von der Schoellerbank ausgewählten Kreis von Wertpapieren Aufträge erteilt werden. Die Schoellerbank behält sich vor, den Kreis der ausgewählten Wertpapiere zu ändern. Informationen über die jeweils zur Auftragserteilung über Online Banking freigeschalteten Wertpapiere erhält der Kunde bei seinem Berater.

Die Art der Orderweiterleitung mittels Online Banking erteilter Wertpapieraufträge unterscheidet sich nicht von der Weiterleitung von bei seinem Kundenberater erteilten Aufträgen. Die Art der Weiterleitung ist somit lediglich abhängig vom Wertpapier selbst bzw. dem Handelsplatz des Wertpapieres und erfolgt entweder direkt an die Börse/Kontrahent oder über bankinterne Systeme. Widerrufe von erteilten Aufträgen sind zwar grundsätzlich möglich, können aber nur berücksichtigt werden, wenn ein Auftrag nicht bereits ausgeführt wurde. Zur Vermeidung von Doppelausführungen hat sich der Kunde vor Erteilung eines erneuten Auftrages unbedingt bei seinem Berater zu informieren, ob ein Widerruf erfolgreich war.

Siehe B Besondere Bestimmungen zur Wertpapierfunktion

~~**9. Elektronische Wertpapieraufträge**~~
~~Elektronische Wertpapieraufträge im Rahmen von Online Banking ermächtigen die Schoellerbank im Falle von Kaufaufträgen, die Konten gemäß dem „Antrag zur Teilnahme am Online Banking und zur Online-Abwicklung von Wertpapieraufträgen“ bzw. „Antrag zur Teilnahme am Online Banking inklusive Portfolioanalyse und zur Online-Abwicklung von Wertpapieraufträgen“ im Rahmen von Guthaben bzw. Dispositionsrahmen zu belasten. Die Schoellerbank ist berechtigt, Wertpapieraufträge ohne entsprechende Deckung nicht durchzuführen.~~

~~Erteilt der Kunde elektronische Wertpapieraufträge, weist die Schoellerbank darauf hin, dass sie nur als Vermittler und Depotbank tätig ist und die vom Kunden erteilten Aufträge nur dahin überprüft, ob die gewünschten Produkte im Hinblick auf die von ihm eingeholten Informationen zu seinen Kenntnissen und Erfahrungen im Anlagebereich für ihn angemessen sind. Eine Überprüfung im Hinblick auf seine Anlageziele und seine finanzielle Risikofähigkeit findet bei derartigen elektronischen Wertpapieraufträgen jedoch nicht statt. Entspricht der vom Kunden ohne vorgängige Beratung erteilte elektronische Wertpapierauftrag nicht seinen Kenntnissen und Erfahrungen im Anlagebereich, ist die Schoellerbank berechtigt, diesen nicht durchzuführen.~~

~~Über Online Banking können nur für einen von der Schoellerbank ausgewählten Kreis von Wertpapieren Aufträge erteilt werden. Die Schoellerbank behält sich vor, den Kreis der ausgewählten Wertpapiere zu ändern. Informationen über die jeweils zur Auftragserteilung über Online Banking freigeschalteten Wertpapiere erhält der Kunde bei seinem Berater.~~

~~Die Art der Orderweiterleitung mittels Online Banking erteilter Wertpapieraufträge unterscheidet sich nicht von der Weiterleitung von bei seinem Kundenberater erteilten Aufträgen. Die Art der Weiterleitung ist somit lediglich abhängig vom Wertpapier selbst bzw. dem Handelsplatz des Wertpapieres und erfolgt entweder direkt an die Börse/Kontrahent oder über bankinterne Systeme. Widerrufe von erteilten Aufträgen sind zwar grundsätzlich möglich, können aber nur berücksichtigt werden, wenn ein Auftrag nicht bereits ausgeführt wurde. Zur Vermeidung von Doppelausführungen hat sich der Kunde vor Erteilung eines erneuten Auftrages unbedingt bei seinem Berater zu informieren, ob ein Widerruf erfolgreich war.~~

9. Erlöschen und Kündigung der Berechtigung
9.1 Bei Auflösung der Kontoverbindung erlöschen gleichzeitig alle Internetbanking-Berechtigungen für das betroffene Konto. Mit Wegfall eines Einzelzeichnungsrechts eines Konto- bzw. Depotinhabers oder Zeichnungsberechtigten zu einem Konto oder

PC282D-Gegenüberstellung 20200101

Wertpapierdepot erlischt die Möglichkeit zur Nutzung des Internetbankings zu diesem Konto oder Wertpapierdepot.

9.2 Jeder Kunde kann die Vereinbarung jederzeit unter Einhaltung einer Frist von einem Monat schriftlich kündigen. Jeder Konto- bzw. Depotinhaber hat die Möglichkeit, die Internetbanking-Berechtigung eines Zeichnungsberechtigten schriftlich oder persönlich an jedem Standort der Bank zu widerrufen.

9.3 Die Bank kann die Vereinbarung ohne Angabe von Gründen unter Einhaltung einer Frist von zwei Monaten jederzeit kündigen, wobei dem Konto- bzw. Depotinhaber die Kündigung in Papierform oder auf einem anderen vereinbarten dauerhaften Datenträger mitzuteilen ist.

9.4 Bei Vorliegen eines wichtigen Grundes sind der Kunde und die Bank berechtigt, die Vereinbarung mit sofortiger Wirkung zu kündigen. Ein wichtiger Grund kann insbesondere dann vorliegen, wenn der Kunde seine persönlichen Identifikationsmerkmale anderen Personen überlässt.

10. Sorgfalt

10. Sorgfalt

Warnhinweis: Electronic Banking wird über das Kommunikationsmedium Internet abgewickelt, welches ein offenes und allgemein zugängliches Medium ist. Unter Verwendung der persönlichen Identifikationsmerkmale eines Kunden kann auch ein unberechtigter Dritter in das Electronic Banking einsteigen und Dispositionen zu Lasten des Kontoinhabers vornehmen. Zur Vermeidung von Schäden bei den Transaktionen im Rahmen des Electronic Banking wird daher empfohlen, besonders sorgfältig vorzugehen.

Im Hinblick auf diese gebotene Sorgfalt ist der Kunde insbesondere verpflichtet, ab Erhalt seiner persönlichen Identifikationsmerkmale diese geheim zu halten und nicht an unbefugte Dritte weiterzugeben. Hat der Kunde den Verdacht, dass seine PIN anderen Personen bekannt geworden ist, hat er seine PIN unverzüglich zu ändern und den Verdacht der Electronic Banking Hotline (siehe Punkt 13.) zu melden. Dem Kunden wird empfohlen, die PIN regelmäßig selbständig zu ändern. Wir empfehlen diese Änderung mindestens alle 2 Monate durchzuführen.

Bei der Nutzung des mobileTAN-, cardTAN- oder tresorTAN-Verfahrens ist der Kunde verpflichtet, die gemeinsam mit der TAN übermittelten Auftragsdaten auf Übereinstimmung mit seinem Auftrag zu prüfen und die TAN nur im Falle einer Übereinstimmung dieser Auftragsdaten zu verwenden.

Siehe Punkt 6. Sorgfalt

~~**10. Sorgfalt**~~

~~Warnhinweis: Electronic Banking wird über das Kommunikationsmedium Internet abgewickelt, welches ein offenes und allgemein zugängliches Medium ist. Unter Verwendung der persönlichen Identifikationsmerkmale eines Kunden kann auch ein unberechtigter Dritter in das Electronic Banking einsteigen und Dispositionen zu Lasten des Kontoinhabers vornehmen. Zur Vermeidung von Schäden bei den Transaktionen im Rahmen des Electronic Banking wird daher empfohlen, besonders sorgfältig vorzugehen.~~

~~Im Hinblick auf diese gebotene Sorgfalt ist der Kunde insbesondere verpflichtet, ab Erhalt seiner persönlichen Identifikationsmerkmale diese geheim zu halten und nicht an unbefugte Dritte weiterzugeben. Hat der Kunde den Verdacht, dass seine PIN anderen Personen bekannt geworden ist, hat er seine PIN unverzüglich zu ändern und den Verdacht der Electronic Banking Hotline (siehe Punkt 13.) zu melden. Dem Kunden wird empfohlen, die PIN regelmäßig selbständig zu ändern. Wir empfehlen diese Änderung mindestens alle 2 Monate durchzuführen.~~

~~Bei der Nutzung des mobileTAN-, cardTAN- oder tresorTAN-Verfahrens ist der Kunde verpflichtet, die gemeinsam mit der TAN übermittelten Auftragsdaten auf Übereinstimmung mit seinem Auftrag zu prüfen und die TAN nur im Falle einer Übereinstimmung dieser Auftragsdaten zu verwenden.~~

10. Benachrichtigungs-Service

10.1 Der Kunde kann sich im Internetbanking für das kostenlose Benachrichtigungs-Service der Bank anmelden. Durch die Anmeldung des Kunden für das Benachrichtigungs-Service unter Mitteilungs-Einstellungen werden die im Rahmen der Anmeldung vom Kunden ausdrücklich ausgewählten kundenbezogenen Daten und Informationen (wie beispielsweise Benachrichtigung, wenn der Kontostand ein vom Kunden definiertes Limit unter- bzw. überschreitet, Kurs-Alarme) an die vom Kunden angegebene E-Mail-Adresse oder einen anderen mit dem Kunden vereinbarten Kommunikationskanal übermittelt.

10.2 Das Benachrichtigungs-Service kann vom Kunden im Internetbanking jederzeit aktiviert bzw. deaktiviert werden. Die Mitteilungs-Einstellungen (Kommunikationskanal sowie Ereignisse, die eine Benachrichtigung an den Kunden auslösen) können vom Kunden jederzeit abgeändert werden.

11. Ablehnung von Überweisungsaufträgen

Die Schoellerbank darf die Durchführung eines vom Kunden über Electronic Banking wirksam erteilten Überweisungsauftrages nur dann ablehnen, wenn

- der Kundenidentifikator nicht oder nur unvollständig angegeben wurde oder
- eine für die Durchführung des Überweisungsauftrages erforderliche Kontodeckung nicht vorhanden ist oder
- die Ausführung gegen eine innerstaatliche oder gemeinschaftliche Regelung oder gegen eine gerichtliche Anordnung verstößt oder
- die Schoellerbank ihre Sorgfaltspflichten gem. § 6 Finanzmarkt-Geldwäschegesetz nicht erfüllen kann oder
- der Verdacht besteht, dass die Ausführung des Auftrages eine strafbare Handlung darstellen würde.

Die Schoellerbank wird dem Kunden die Ablehnung eines Überweisungsauftrages so rasch wie möglich unter Angabe einer Möglichkeit der Verbesserung des Überweisungsauftrages in einer mit dem Kunden vereinbarten Form mitteilen oder zugänglich machen. Die Angabe eines Grundes für die Ablehnung wird nur erfolgen, sofern dies nicht einen Verstoß gegen innerstaatliche oder gemeinschaftsrechtliche Regelungen bzw. eine gerichtliche oder verwaltungsbehördliche Anordnung darstellen würde.

(siehe Punkt 21. Änderung der Geschäftsbedingungen)

~~**11. Ablehnung von Überweisungsaufträgen**~~

~~Die Schoellerbank darf die Durchführung eines vom Kunden über Electronic Banking wirksam erteilten Überweisungsauftrages nur dann ablehnen, wenn~~

- ~~der Kundenidentifikator nicht oder nur unvollständig angegeben wurde oder~~
- ~~eine für die Durchführung des Überweisungsauftrages erforderliche Kontodeckung nicht vorhanden ist oder~~
- ~~die Ausführung gegen eine innerstaatliche oder gemeinschaftliche Regelung oder gegen eine gerichtliche Anordnung verstößt oder~~
- ~~die Schoellerbank ihre Sorgfaltspflichten gem. § 6 Finanzmarkt-Geldwäschegesetz nicht erfüllen kann oder~~
- ~~der Verdacht besteht, dass die Ausführung des Auftrages eine strafbare Handlung darstellen würde.~~

~~Die Schoellerbank wird dem Kunden die Ablehnung eines Überweisungsauftrages so rasch wie möglich unter Angabe einer Möglichkeit der Verbesserung des Überweisungsauftrages in einer mit dem Kunden vereinbarten Form mitteilen oder zugänglich machen. Die Angabe eines Grundes für die Ablehnung wird nur erfolgen, sofern dies nicht einen Verstoß gegen innerstaatliche oder gemeinschaftsrechtliche Regelungen bzw. eine gerichtliche oder verwaltungsbehördliche Anordnung darstellen würde.~~

11 Änderung der Geschäftsbedingungen

11.1 Änderungen dieser Geschäftsbedingungen werden dem Kunden von der Bank spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Inkrafttretens unter Hinweis auf die betroffenen Bestimmungen angeboten. Die Zustimmung des Kunden gilt als erteilt, wenn bei der Bank vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens kein Widerspruch des Kunden einlangt. Darauf wird die Bank den Kunden im Änderungsangebot hinweisen. Das Änderungsangebot ist dem Kunden mitzuteilen. Außerdem wird die Bank eine Gegenüberstellung über die von der Änderung der Geschäftsbedingungen betroffenen Bestimmungen sowie die vollständige Fassung der neuen Geschäftsbedingungen auf ihrer Homepage veröffentlichen und diese in Schriftform dem Kunden auf dessen Verlangen an ihren Standorten aushändigen oder postalisch übermitteln. Die Bank wird den Kunden mit der Mitteilung über die angebotene Änderung auf diese Möglichkeit hinweisen.

11.1a Die Mitteilung über die angebotene Änderung gemäß Punkt 11.1 erfolgt entweder per Post an die letzte vom Kunden bekannt gegebene Anschrift (s. auch Z 11 Abs. 2 der Allgemeinen Geschäftsbedingungen der Bank) oder in elektronischer Form über Mitteilungen im Internetbanking. Diese elektronische Mitteilung erfolgt derart, dass die Bank das Änderungsangebot nicht mehr einseitig abändern kann und der Kunde die Möglichkeit hat, die Mitteilung bei sich abzuspeichern und auszudrucken. Erfolgt eine solche elektronische Mitteilung über das Internetbanking, wird die Bank den Kunden überdies gleichzeitig davon in Kenntnis setzen, dass das Änderungsangebot unter Mitteilungen im Internetbanking verfügbar und abfragbar ist. Dies geschieht

durch Übersenden eines separaten E-Mails an die vom Kunden zuletzt bekannt gegebene E-Mail-Adresse oder einen anderen mit dem Kunden vereinbarten Kommunikationskanal.

11.1b Gegenüber einem Unternehmer ist es ausreichend, das Änderungsangebot spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens der Änderungen über Mitteilungen des Internetbankings zuzustellen oder auf eine andere, mit dem Unternehmer vereinbarte Weise zum Abruf bereitzuhalten.

11.2 Im Falle einer solchen beabsichtigten Änderung der Geschäftsbedingungen hat der Kunde, der Verbraucher ist, das Recht, seine Rahmenverträge für Zahlungsdienstleistungen, insbesondere diese Vereinbarung oder den Girokontovertrag, vor Inkrafttreten der Änderung kostenlos fristlos zu kündigen. Darauf wird die Bank im Änderungsanbot hinweisen.

11.3 Die Punkte 11.1 bis 11.2 gelten auch für Änderungen der Vereinbarung gemäß Punkt 1.2, in der die Geltung dieser Geschäftsbedingungen zwischen Kunde und Bank vereinbart worden ist.

11.4 Die vorstehenden Punkte 11.1 bis 11.3 finden auf die Änderung der Leistungen der Bank und der Entgelte des Kunden keine Anwendung.

12. Berichtigung von nicht autorisierten Zahlungs- vorgängen

Auf Z16(2) der Allgemeinen Geschäftsbedingungen der Schoellerbank wird hingewiesen. Ist der Kunde Unternehmer, verkürzt sich die dort angesprochene Frist von 13 Monaten auf 3 Monate.

~~**12. Berichtigung von nicht autorisierten Zahlungs- vorgängen**~~

~~Auf Z16(2) der Allgemeinen Geschäftsbedingungen der Schoellerbank wird hingewiesen. Ist der Kunde Unternehmer, verkürzt sich die dort angesprochene Frist von 13 Monaten auf 3 Monate.~~

13. Sperren

Den Verlust, Diebstahl oder missbräuchliche Verwendung der persönlichen Identifikationsmerkmale (Verfügernummer, PIN) oder die sonstige nicht autorisierte Nutzung des Electronic Banking hat der Kunde unverzüglich nach Feststellung der Schoellerbank mitzuteilen.

Jeder Kontoinhaber und jeder Zeichnungsberechtigte hat die Möglichkeit eine Sperre wie folgt zu veranlassen:
• jederzeit telefonisch bei der Electronic Banking Hotline 0800/692265, aus dem Ausland unter +43/1/53471-1428, per Telefax +43/1/53471-1619 oder per e-Mail: banking@schoellerbank.at, oder
• während der Öffnungszeiten der Schoellerbank persönlich bei seinem Berater oder schriftlich in jedem Standort der Schoellerbank.

Der Kunde kann die Sperre der PIN im Schoellerbank Electronic Banking auch selbst online vornehmen. Im Falle der viermaligen aufeinander folgenden Falscheingabe der PIN bzw. der TAN wird die Verfügernummer unmittelbar nach der vierten Falscheingabe automatisch gesperrt.

Bei Verlust oder Diebstahl einer Signaturkarte, oder wenn der Verdacht besteht, dass die Geheimhaltungs-PIN nicht mehr sicher ist, muss das betroffene Zertifikat beim Widerrufsdienst der A- Trust unverzüglich widerrufen werden.

Siehe Punkt 8. Sperren

~~**13. Sperren**~~

~~Den Verlust, Diebstahl oder missbräuchliche Verwendung der persönlichen Identifikationsmerkmale (Verfügernummer, PIN) oder die sonstige nicht autorisierte Nutzung des Electronic Banking hat der Kunde unverzüglich nach Feststellung der Schoellerbank mitzuteilen.~~

~~Jeder Kontoinhaber und jeder Zeichnungsberechtigte hat die Möglichkeit eine Sperre wie folgt zu veranlassen:~~
~~• jederzeit telefonisch bei der Electronic Banking Hotline 0800/692265, aus dem Ausland unter +43/1/53471-1428, per Telefax +43/1/53471-1619 oder per e-Mail: banking@schoellerbank.at, oder~~
~~• während der Öffnungszeiten der Schoellerbank persönlich bei seinem Berater oder schriftlich in jedem Standort der Schoellerbank.~~

~~Der Kunde kann die Sperre der PIN im Schoellerbank Electronic Banking auch selbst online vornehmen. Im Falle der viermaligen aufeinander folgenden Falscheingabe der PIN bzw. der TAN wird die Verfügernummer unmittelbar nach der vierten Falscheingabe automatisch gesperrt.~~

~~Bei Verlust oder Diebstahl einer Signaturkarte, oder wenn der Verdacht besteht, dass die Geheimhaltungs-PIN nicht mehr sicher ist, muss das betroffene Zertifikat beim Widerrufsdienst der A- Trust unverzüglich widerrufen werden.~~

Eine innerhalb der Öffnungszeiten bei der Schoellerbank oder – zu welchem Zeitpunkt auch immer – bei der Electronic Banking-Hotline veranlasste Sperre wird unmittelbar mit Einlangen des Sperrauftrages wirksam. Außerhalb der Öffnungszeiten bei der Schoellerbank schriftlich einlangende Sperraufträge werden unverzüglich, spätestens eine Stunde nach Beginn der nächsten Öffnungszeit, wirksam.

~~Eine innerhalb der Öffnungszeiten bei der Schoellerbank oder – zu welchem Zeitpunkt auch immer – bei der Electronic Banking-Hotline veranlasste Sperre wird unmittelbar mit Einlangen des Sperrauftrages wirksam. Außerhalb der Öffnungszeiten bei der Schoellerbank schriftlich einlangende Sperraufträge werden unverzüglich, spätestens eine Stunde nach Beginn der nächsten Öffnungszeit, wirksam.~~

Die Schoellerbank ist berechtigt, eine Verfügernummer ohne Mitwirkung des Kunden zu sperren, wenn

- objektive Gründe im Zusammenhang mit der Sicherheit der persönlichen Identifikationsmerkmale oder der Systeme, für die sie benutzt werden können, dies rechtfertigen,
- der Verdacht einer Erteilung von nicht autorisierten Aufträgen oder der betrügerischen Verwendung der persönlichen Identifikationsmerkmale besteht,
- ein beträchtlich erhöhtes Risiko besteht, dass der Kontoinhaber seinen gegenüber der Schoellerbank aus der Verwendung der persönlichen Identifikationsmerkmalen entstehenden Zahlungsverpflichtungen nicht nachkommen kann.

~~Die Schoellerbank ist berechtigt, eine Verfügernummer ohne Mitwirkung des Kunden zu sperren, wenn~~

- ~~objektive Gründe im Zusammenhang mit der Sicherheit der persönlichen Identifikationsmerkmale oder der Systeme, für die sie benutzt werden können, dies rechtfertigen,~~
- ~~der Verdacht einer Erteilung von nicht autorisierten Aufträgen oder der betrügerischen Verwendung der persönlichen Identifikationsmerkmale besteht,~~
- ~~ein beträchtlich erhöhtes Risiko besteht, dass der Kontoinhaber seinen gegenüber der Schoellerbank aus der Verwendung der persönlichen Identifikationsmerkmalen entstehenden Zahlungsverpflichtungen nicht nachkommen kann.~~

Die Schoellerbank wird den Kunden über die Sperre und die Gründe hierfür – soweit dies nicht innerstaatliche oder gemeinschaftsrechtliche Rechtsvorschriften sowie gerichtliche oder verwaltungsbehördliche Anordnungen verletzen oder objektiven Sicherheitserwägungen zuwiderlaufen würde – möglichst vor, spätestens aber unverzüglich nach der Sperre in der mit ihm vereinbarten Form informieren.

~~Die Schoellerbank wird den Kunden über die Sperre und die Gründe hierfür – soweit dies nicht innerstaatliche oder gemeinschaftsrechtliche Rechtsvorschriften sowie gerichtliche oder verwaltungsbehördliche Anordnungen verletzen oder objektiven Sicherheitserwägungen zuwiderlaufen würde – möglichst vor, spätestens aber unverzüglich nach der Sperre in der mit ihm vereinbarten Form informieren.~~

Die Aufhebung einer Sperre kann nur durch den Kunden persönlich oder über ausdrücklichen, schriftlichen Auftrag – brieflich mit eigenhändiger Unterschrift bzw. firmenmäßiger Fertigung des Kunden – bei der Schoellerbank erfolgen.

~~Die Aufhebung einer Sperre kann nur durch den Kunden persönlich oder über ausdrücklichen, schriftlichen Auftrag – brieflich mit eigenhändiger Unterschrift bzw. firmenmäßiger Fertigung des Kunden – bei der Schoellerbank erfolgen.~~

14. Informationen über einzelne Zahlungsvorgänge (Kontoauszüge)

Die Informationen über einzelne Zahlungsvorgänge (Kontoauszüge) werden tagesaktuell von der Schoellerbank zur Abrufung durch den Kunden in seinem elektronischen Postfach im PDF-Format bereitgehalten. Die Kontoauszüge sind mit ihrer Abrufung durch den Kunden zugestellt. Dem Kunden ist bekannt, dass Kontoauszüge wichtige Mitteilungen beinhalten und seine Einwendungen bzw. Erklärungen innerhalb bestimmter Frist notwendig machen können. Er wird daher die Informationen aus dem elektronischen Postfach regelmäßig, zumindest 1x monatlich, abrufen. Der Kunde wird die Schoellerbank davon verständigen, wenn er längere Zeit an der Abrufung der Kontoauszüge in seinem elektronischen Postfach gehindert sein sollte. Für Schäden, die dem Kunden aus der unterlassenen, verspäteten oder unsachgemäßen Abrufung der Informationen entstehen, haftet die Schoellerbank nicht.
Zusätzlich kann der Kunde verlangen, dass ihm die Informationen 1x monatlich gegen Ersatz der Portospesen übermittelt werden.

~~**14. Informationen über einzelne Zahlungsvorgänge (Kontoauszüge)**~~

~~Die Informationen über einzelne Zahlungsvorgänge (Kontoauszüge) werden tagesaktuell von der Schoellerbank zur Abrufung durch den Kunden in seinem elektronischen Postfach im PDF-Format bereitgehalten. Die Kontoauszüge sind mit ihrer Abrufung durch den Kunden zugestellt. Dem Kunden ist bekannt, dass Kontoauszüge wichtige Mitteilungen beinhalten und seine Einwendungen bzw. Erklärungen innerhalb bestimmter Frist notwendig machen können. Er wird daher die Informationen aus dem elektronischen Postfach regelmäßig, zumindest 1x monatlich, abrufen. Der Kunde wird die Schoellerbank davon verständigen, wenn er längere Zeit an der Abrufung der Kontoauszüge in seinem elektronischen Postfach gehindert sein sollte. Für Schäden, die dem Kunden aus der unterlassenen, verspäteten oder unsachgemäßen Abrufung der Informationen entstehen, haftet die Schoellerbank nicht.~~
~~Zusätzlich kann der Kunde verlangen, dass ihm die Informationen 1x monatlich gegen Ersatz der Portospesen übermittelt werden.~~

15. Erlöschen und Kündigung der Vereinbarung

Bei Auflösung der Kontoverbindung erlöschen gleichzeitig alle Electronic Banking-Berechtigungen für das betroffene Konto. Die Electronic Banking-Berechtigung eines Kontoinhabers oder Zeichnungsberechtigten erlischt

~~**15. Erlöschen und Kündigung der Vereinbarung**~~

~~Bei Auflösung der Kontoverbindung erlöschen gleichzeitig alle Electronic Banking-Berechtigungen für das betroffene Konto. Die Electronic Banking-Berechtigung eines Kontoinhabers oder Zeichnungsberechtigten erlischt~~

ebenfalls bei Wegfall seiner Einzelverfügungsberechtigung für das betroffene Konto.

Jeder Kunde kann die Vereinbarung jederzeit unter Einhaltung einer Frist von einem Monat schriftlich kündigen. Jeder Kontoinhaber hat die Möglichkeit, die Electronic Banking-Berechtigung eines Zeichnungsberechtigten schriftlich oder persönlich in jedem Standort der Schoellerbank zu widerrufen.

Die Schoellerbank kann die Vereinbarung ohne Angabe von Gründen unter Einhaltung einer Frist von 2 Monaten jederzeit kündigen, wobei dem Kontoinhaber die Kündigung in Papierform oder auf einem anderen vereinbarten dauerhaften Datenträger mitzuteilen ist.

Bei Vorliegen eines wichtigen Grundes sind der Kunde und die Schoellerbank berechtigt, die Vereinbarung mit sofortiger Wirkung zu kündigen. Als wichtiger Grund gilt insbesondere, wenn der Kunde seine persönlichen Identifikationsmerkmale anderen Personen überlässt.

16. Haftung

a) Haftung bei elektronischen Überweisungsaufträgen
Handelt es sich beim Kunden nicht um einen Verbraucher gemäß § 4 Z 20 ZaDiG 2018, ist er bei nicht autorisierten Zahlungsvorgängen, die auf der Nutzung eines verlorenen oder gestohlenen Zahlungsinstruments oder auf der missbräuchlichen Verwendung eines Zahlungsinstruments beruhen, auch bei leicht fahrlässiger Verletzung der in § 63 ZaDiG 2018 genannten Pflichten und Bedingungen der Schoellerbank zum Ersatz des gesamten Schadens verpflichtet. § 68 Abs 2 Z 1, Abs 4, Abs 5 und Abs 6 ZaDiG 2018 gelten nicht.

b) Haftung bei elektronischen Wertpapieraufträgen
Beruht ein elektronischer Wertpapierauftrag auf der missbräuchlichen Verwendung der persönlichen Identifikationsmerkmale des Kunden, trägt der Kunde alle daraus entstehenden Folgen und Nachteile, wenn er die Verwendung der persönlichen Identifikationsmerkmale durch Dritte fahrlässig ermöglicht hat. Der Kunde ist verpflichtet, einen der Schoellerbank in diesem Fall entstehenden Schaden zu ersetzen.

(Siehe Punkt 9. Elektronische Wertpapieraufträge)

~~ebenfalls bei Wegfall seiner Einzelverfügungsberechtigung für das betroffene Konto.~~

~~Jeder Kunde kann die Vereinbarung jederzeit unter Einhaltung einer Frist von einem Monat schriftlich kündigen. Jeder Kontoinhaber hat die Möglichkeit, die Electronic Banking-Berechtigung eines Zeichnungsberechtigten schriftlich oder persönlich in jedem Standort der Schoellerbank zu widerrufen.~~

~~Die Schoellerbank kann die Vereinbarung ohne Angabe von Gründen unter Einhaltung einer Frist von 2 Monaten jederzeit kündigen, wobei dem Kontoinhaber die Kündigung in Papierform oder auf einem anderen vereinbarten dauerhaften Datenträger mitzuteilen ist.~~

~~Bei Vorliegen eines wichtigen Grundes sind der Kunde und die Schoellerbank berechtigt, die Vereinbarung mit sofortiger Wirkung zu kündigen. Als wichtiger Grund gilt insbesondere, wenn der Kunde seine persönlichen Identifikationsmerkmale anderen Personen überlässt.~~

~~**16. Haftung**~~

~~a) Haftung bei elektronischen Überweisungsaufträgen~~
~~Handelt es sich beim Kunden nicht um einen Verbraucher gemäß § 4 Z 20 ZaDiG 2018, ist er bei nicht autorisierten Zahlungsvorgängen, die auf der Nutzung eines verlorenen oder gestohlenen Zahlungsinstruments oder auf der missbräuchlichen Verwendung eines Zahlungsinstruments beruhen, auch bei leicht fahrlässiger Verletzung der in § 63 ZaDiG 2018 genannten Pflichten und Bedingungen der Schoellerbank zum Ersatz des gesamten Schadens verpflichtet. § 68 Abs 2 Z 1, Abs 4, Abs 5 und Abs 6 ZaDiG 2018 gelten nicht.~~
~~b) Haftung bei elektronischen Wertpapieraufträgen~~
~~Beruht ein elektronischer Wertpapierauftrag auf der missbräuchlichen Verwendung der persönlichen Identifikationsmerkmale des Kunden, trägt der Kunde alle daraus entstehenden Folgen und Nachteile, wenn er die Verwendung der persönlichen Identifikationsmerkmale durch Dritte fahrlässig ermöglicht hat. Der Kunde ist verpflichtet, einen der Schoellerbank in diesem Fall entstehenden Schaden zu ersetzen.~~

B Besondere Bestimmungen zur Wertpapierfunktion

1. Allgemein

Über Internetbanking ist der Kauf und Verkauf von Aktien, Optionsscheinen, Anleihen, Indexzertifikaten an ausgewählten Börsen sowie von der Bank ausgewählten in- und ausländischen Fonds möglich. Die aktuellen Börsenplätze, an denen über Internetbanking gehandelt werden kann, sowie die Wertpapierarten, die an den infrage kommenden Börsen über Internetbanking gehandelt werden können, sind der „Best Execution Policy“ zu entnehmen. Diese kann auf der Website der Bank unter www.schoellerbank.at eingesehen bzw. in einer Filiale der Bank erfragt werden.

2. Auftragerteilung und Nutzungszeiten

2.1 Die Auftragserteilung ist über Internetbanking grundsätzlich 24 Stunden am Tag und 7 Tage die Woche möglich (siehe Teil A, Punkt 4.1).

2.2 Auf diese Weise können Kauf- und Verkaufsaufträge zu einzelnen Wertpapierpositionen beim Internetbanking auch taggleich erteilt werden (Intraday-Handel).

2.3 Der Verkauf verpfändeter oder aus sonstigem Grund von der Bank gesperrt zu haltender, auf dem/den angegebenen Wertpapierdepot(s) erliegender Werte ist im Rahmen des Internetbankings nicht möglich.

2.4 Der Kunde erhält von der Bank rechtsverbindliche Bestätigungen über die Durchführung der erteilten Aufträge sowie die Abrechnung auf dem für Kontopost vereinbarten Versandweg. Eine elektronische Auftragsbestätigung gilt daher nur als Bestätigung der Übernahme des Auftrags zur Bearbeitung durch die Bank, nicht jedoch als Ausführungsbestätigung oder Abrechnung.

2.5 Die Erteilung eines Kaufauftrags im Rahmen des Internetbankings ist nur so weit zulässig, als zum Zeitpunkt der Ordererteilung auf dem für den Kaufauftrag gewählten Verrechnungskonto eine für die Ausführung des Auftrags notwendige Deckung (Guthaben oder vereinbarter Überziehungsrahmen) vorhanden ist.

2.6 Über die Handelszeiten zum Zeitpunkt der Auftragserteilung und die Usancen der jeweiligen Börse hat sich der Kunde selbstständig zu informieren. Die Bank haftet nicht für Schäden, die dem Kunden daraus entstehen, dass sein im Internetbanking erteilter Auftrag nicht mit den Handelsusancen der gewünschten Börse übereinstimmt. Entspricht der vom Kunden ohne vorgängige Beratung erteilte elektronische Wertpapierauftrag nicht seinen Kenntnissen und Erfahrungen im Anlagebereich, ist die Bank berechtigt, diesen nicht durchzuführen.

3. Pfandrecht

Die auf dem/den für Internetbanking gewidmeten Wertpapierdepot(s) verbuchten Wertpapiere sowie die aus diesen Wertpapieren resultierenden Zins-, Tilgungs- und Verkaufserlöse unterliegen für alle der Bank zustehenden Forderungen aus der Geschäftsbeziehung dem Pfandrecht nach Z 49 ff. der Allgemeinen Geschäftsbedingungen der Schoellerbank AG. Falls die Kurswerte der auf dem/den gewidmeten Wertpapierdepot(s) jeweils erliegenden Werte soweit absinken sollten, dass eine Aushaftung auf dem/den dazugehörigen Verrechnungskonto/-konten nicht mehr gedeckt ist, verpflichtet sich der Kunde als Konto- bzw. Depotinhaber, innerhalb der von der Bank gesetzten Frist entweder weitere der Bank als Pfand genehme Wertpapiere in entsprechender Höhe zu übergeben oder die Aushaftung in dem Maße abzudecken, dass eine ausreichende Besicherung wiederhergestellt wird. Im Rahmen dieses Pfandrechts nicht benötigte Deckungswerte bleiben im Einvernehmen mit der Bank und unter Absprache mit dem jeweiligen Kundenbetreuer zur freien Verfügung des Kunden. Ausdrücklich festgehalten wird das Recht der Bank, im Zusammenhang mit dem Pfandrecht Depotwerte zu sperren, soweit dies zur Sicherstellung von Forderungen aus der Depotführung oder aus der sonstigen Geschäftsbeziehung notwendig ist. Die Bank ist berechtigt, die verpfändeten bzw. der Depotsperre unterliegenden Wertpapiere im Sinne der Allgemeinen Geschäftsbedingungen der Schoellerbank AG ganz oder teilweise zu veräußern, wenn die oben erwähnte Nachschussleistung bzw. Abdeckung nicht erbracht wird oder eine von ihr geltend gemachte Forderung aus der Geschäftsbeziehung (insbesondere auch aus der Depotführung) nicht fristgerecht beglichen wird.

17. Erlaubte Nutzung des Electronic Banking
Der Kunde ist berechtigt, die Software via Web-Browser für die beabsichtigten Zwecke gemäß dieser Vereinbarung zu nutzen. Er darf das Schoellerbank Electronic Banking für seine privaten Zwecke unbeschränkt nutzen, die Reproduktion, der Verkauf oder die sonstige Weitergabe der über das Schoellerbank Electronic Banking erhältlichen Informationen und Dienstleistungen sowie gewerbliche Nutzung in welcher Form immer ist an unsere ausdrückliche schriftliche Zustimmung gebunden. Wir weisen ausdrücklich auf das Urheberrecht der Schoellerbank in Hinblick auf das Layout, Grafiken, HTML bzw. sonstige Seitenelemente hin.

18. Schoellerbank Business Banking (HBP)
Diese Bedingungen regeln den Erwerb des einfachen, nicht übertragbaren Nutzungsrechtes des Software-produkts „Schoellerbank Business Banking (HBP)“ sowie dessen Anwendung für bei der Schoellerbank geführte Konten/Depots im jeweils vereinbarten Umfang.

Schoellerbank Business Banking entspricht grundsätzlich dem so genannten „Multi Bank Standard“, der es dem Kunden ermöglicht, mit einem Softwareprodukt alle Kontoverbindungen in Österreich zu bedienen, welche MBS unterstützen.

~~**17. Erlaubte Nutzung des Electronic Banking**~~
~~Der Kunde ist berechtigt, die Software via Web-Browser für die beabsichtigten Zwecke gemäß dieser Vereinbarung zu nutzen. Er darf das Schoellerbank Electronic Banking für seine privaten Zwecke unbeschränkt nutzen, die Reproduktion, der Verkauf oder die sonstige Weitergabe der über das Schoellerbank Electronic Banking erhältlichen Informationen und Dienstleistungen sowie gewerbliche Nutzung in welcher Form immer ist an unsere ausdrückliche schriftliche Zustimmung gebunden. Wir weisen ausdrücklich auf das Urheberrecht der Schoellerbank in Hinblick auf das Layout, Grafiken, HTML bzw. sonstige Seitenelemente hin.~~

~~**18. Schoellerbank Business Banking (HBP)**~~
~~Diese Bedingungen regeln den Erwerb des einfachen, nicht übertragbaren Nutzungsrechtes des Software-produkts „Schoellerbank Business Banking (HBP)“ sowie dessen Anwendung für bei der Schoellerbank geführte Konten/Depots im jeweils vereinbarten Umfang.~~

~~Schoellerbank Business Banking entspricht grundsätzlich dem so genannten „Multi Bank Standard“, der es dem Kunden ermöglicht, mit einem Softwareprodukt alle Kontoverbindungen in Österreich zu bedienen, welche MBS unterstützen.~~

C Besondere Bedingungen Schoellerbank Business Banking und Multi Bank Standard Service (MBS-Service)
Diese besonderen Bedingungen gelten nur für Unternehmer.
Für die Bankprodukte Schoellerbank Business Banking (HBP) und Multi Bank Standard Service (MBS-Service) gilt Teil A dieser Bedingungen im folgenden Ausmaß: Die Authentifizierung kann mittels mobileTAN und cardTAN erfolgen (Punkt 2.5.a und 2.5.c). Weiters gelten die Punkte 6 (Sorgfalt), 7 (Berichtigung von nicht autorisierten Zahlungsvorgängen), 8 (Sperren), 9 (Erlöschen und Kündigung der Berechtigung) und 11 (Änderungen der Geschäftsbedingungen). Die anderen Absätze sind für die nachfolgenden Bankprodukte nicht anwendbar.

1. Schoellerbank Business Banking (HBP)
1.1 Zugang zum Schoellerbank Business Banking
Verfügernummer: Der Kunde erhält von der Schoellerbank AG eine Verfügernummer, anhand derer die Schoellerbank AG einen Kunden zu den zum Schoellerbank Business Banking berechtigten Konten zuordnen kann. Sie besteht aus einem mehrstelligen Zahlencode und wird bei Ausstellung vom System vergeben. Die Verfügernummer kann vom Kunden nicht geändert werden.

Verfügername: Der Verfügername muss vom Kunden im Rahmen des Ersteinstiegs im Schoellerbank Business Banking festgelegt werden. Der Verfügername kann jederzeit und sofort unter Verwendung einer TAN geändert werden.

Passwort (=PIN/Persönliche Identifikationsnummer): Das Passwort dient zur Legitimierung des Kunden beim Electronic Banking und ist die Voraussetzung dafür, dass der Kunde über Schoellerbank Business Banking Aufträge erteilen bzw. Daten und Informationen abfragen kann. Die PIN besteht aus einer 16-stelligen Zahlen-/Buchstabenkette. Diese Erst-PIN muss im Rahmen des Ersteinstiegs zum gewählten Electronic Banking Produkt vom Kunden

abgeändert werden. Die PIN kann jederzeit und sofort wirksam unter Verwendung einer TAN geändert werden. Eine neue Erst-PIN kann der Kunde telefonisch bei seinem Kundenbetreuer beantragen.

1.2 Abwicklung

Zusätzlich zu den persönlichen Berechtigungsmerkmalen, wie im Punkt 1.1. beschrieben, sind seitens jedes berechtigten Teilnehmers am Schoellerbank Business Banking folgende Merkmale selbst zu definieren:
Benutzername (Useridentifikation zum Einstieg in das Schoellerbank Business Banking) und Passwort (vom nutzungsberechtigten Teilnehmer jederzeit abänderbar). Bei diesen Merkmalen „Benutzername und Passwort" handelt es sich um – im Schoellerbank Business Banking – lokal gespeicherte Zugangsdaten für die Anmeldung am Programm und nicht um die in Punkt 1.1. beschriebenen persönlichen Berechtigungsmerkmale. Diese Merkmale dienen der internen Sicherheit des Kunden und sind unabhängig von den von der Bank vergebenen persönlichen Berechtigungsmerkmalen.

1.3 Zugangsvoraussetzungen

Eine Berechtigung zur Nutzung von Schoellerbank Business Banking wird mittels Teilnahmevereinbarung „Antrag zur Teilnahme am Schoellerbank Business Banking" begründet. Der Kunde erhält seine Zugangsdaten (Verfügernummer und persönliche Identifikationsnummer=PIN) zum Schoellerbank Business Banking postalisch oder persönlich per Brief. Die Kommunikation kann nur dann erfolgreich durchgeführt werden, wenn die von der Bank vergebenen (Verfügernummer und persönliche Identifikations-nummer=PIN) und die vom Kunden zu definierenden Zugangsdaten (Verfügername) korrekt eingegeben wurden. Die von der Bank vergebene PIN ist bei Erstanmeldung zu ändern.

Vertragsgegenstand ist der Erwerb des einfachen, nicht übertragbaren Nutzungsrechtes am Softwareprodukt „Schoellerbank Business Banking" sowie dessen Anwendung für bei der Bank geführte Konten/Depots im jeweils vereinbarten Umfang. Schoellerbank Business Banking entspricht grundsätzlich dem so genannten „Multi Bank Standard", der es dem Kunden ermöglicht, mit einem Softwareprodukt alle Kontoverbindungen in Österreich zu bedienen, welche MBS unterstützen.

Dem Kunden ist es nicht erlaubt, die Schoellerbank Business Banking-Software zu kopieren und an Dritte weiterzugeben. Davon ausgenommen ist die Herstellung einer Sicherungskopie zur Förderung der Betriebs-sicherheit. Das geistige Eigentum an Software und Dokumentation und die damit verbundenen Rechte bleiben bei der Schoellerbank. Die Schoellerbank übernimmt keine Garantie für die fehlerfreie Funktion der Programme. Installation und Gebrauch erfolgen immer auf eigenes Risiko.

Dem Kunden ist es nicht erlaubt, die Schoellerbank Business Banking-Software zu kopieren und an Dritte weiterzugeben. Davon ausgenommen ist die Herstellung einer Sicherungskopie zur Förderung der Betriebssicherheit. Das geistige Eigentum an Software und Dokumentation und die damit verbundenen Rechte bleiben bei der Schoellerbank. Die ~~Schoellerbank~~ Bank übernimmt keine Garantie für die fehlerfreie Funktion der Programme. Installation und Gebrauch erfolgen immer auf eigenes Risiko.

1.4 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 Programm-oberfläche durchzuführen. Programmänderungen und -erweiterungen werden vollautomatisch bei der Kommunikation mit der Schoellerbank AG übermittelt. Der Kunde ist verpflichtet, für eine ordnungsgemäße Installation

19. Aktualisierungen und technische Anpassungen / MBS

Die Schoellerbank ist jederzeit berechtigt, entsprechend dem technischen Fortschritt und allenfalls zusätzlichen Sicherheitsmaßnahmen, Updates und Abänderungen im Datenübertragungsbereich oder an der Programmoberfläche durchzuführen. Programmänderungen und -erweiterungen werden vollautomatisch bei der Kommunikation mit der Schoellerbank übermittelt. Der Kunde ist verpflichtet, für eine ordnungsgemäße Installation von Programmupdates zu sorgen. Darüber hinaus ist die Schoellerbank auch zur Erweiterung des Funktionsumfanges des Electronic Banking insoweit berechtigt, als dadurch dem Kunden keine zusätzlichen Kosten oder Verpflichtungen erwachsen.

~~**19. Aktualisierungen und technische Anpassungen / MBS**~~

~~Die Schoellerbank ist jederzeit berechtigt, entsprechend dem technischen Fortschritt und allenfalls zusätzlichen Sicherheitsmaßnahmen, Updates und Abänderungen im Datenübertragungsbereich oder an der Programmoberfläche durchzuführen. Programmänderungen und -erweiterungen werden vollautomatisch bei der Kommunikation mit der Schoellerbank übermittelt. Der Kunde ist verpflichtet, für eine ordnungsgemäße Installation von Programmupdates zu sorgen. Darüber hinaus ist die Schoellerbank auch zur Erweiterung des Funktionsumfanges des Electronic Banking insoweit berechtigt, als dadurch dem Kunden keine zusätzlichen Kosten oder Verpflichtungen erwachsen.~~

von Programmupdates zu sorgen. Darüber hinaus ist die Bank auch zur Erweiterung des Funktionsumfanges des Electronic Banking insoweit berechtigt, als dadurch dem Kunden keine zusätzlichen Kosten oder Verpflichtungen erwachsen.

Für Schoellerbank Business Banking muss seitens des Kunden gewährleistet sein, dass ein ungehinderter Datentransfer über die URL hob.banking.co.at nicht durch z.B. eine Firewall behindert wird. Weiters werden die Ports 3048, 443 und 80 benötigt. Technischer Support erfolgt ausschließlich für die aktuelle Version. Schoellerbank Business Banking unterstützt den MBS-Standard.

Multi Bank Standard Service (MBS-Service) bietet als sektorübergreifende Softwarelösung die Möglichkeit, mit einem einzigen Programm mehrere Kontoverbindungen bei unterschiedlichen Banken anzusprechen.

1. Digitale Signatur

Die Freigabe einer Transaktion kann auch durch Verwendung mittels qualifizierter digitaler Signatur erfolgen (z.B. Bürgerkartenfunktion auf der e-card, a.sign premium).

Zu Kontrollzwecken werden auch die Angaben über die durchzuführenden Aufträge angezeigt. Bei Überweisungsaufträgen werden insbesondere Empfänger-IBAN und Betrag oder ein Referenzcode und Kontrollwert (Summe aller Aufträge) angeführt. Der Kunde ist verpflichtet, diese auf Übereinstimmung mit den eingegebenen Aufträgen zu prüfen. Die Signatur-PIN darf nur bei Übereinstimmung eingegeben werden.

Dieses Signaturverfahren ist keine Anwendung der Bank. Eine Sperre bzw. ein Widerruf des Zertifikats ist beim Zertifikatsanbieter zu veranlassen.

2. Nutzung über andere Software-Produkte (MBS-Service)

Kunden haben die Möglichkeit, MBS auch über Softwareprodukte anderer Banken (z.B. Business Line, ELBA Business etc.), mit denen eine Verbindung zum Bankrechner der Schoellerbank AG hergestellt werden kann, zu nutzen. Abhängig von der Berechtigungsverwaltung dieser Softwareprodukte kann der Verfüger, sowie allfällige von diesem 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 gestellt hat.

Für Schoellerbank Business Banking muss seitens des Kunden gewährleistet sein, dass ein ungehinderter Datentransfer über die URL hob.banking.co.at nicht durch z.B. eine Firewall behindert wird. Weiters werden die Ports 3048, 443 und 80 benötigt. Technischer Support erfolgt ausschließlich für die aktuelle Version. Schoellerbank Business Banking unterstützt den MBS-Standard.

~~Für Schoellerbank Business Banking muss seitens des Kunden gewährleistet sein, dass ein ungehinderter Datentransfer über die URL hob.banking.co.at nicht durch z.B. eine Firewall behindert wird. Weiters werden die Ports 3048, 443 und 80 benötigt. Technischer Support erfolgt ausschließlich für die aktuelle Version. Schoellerbank Business Banking unterstützt den MBS-Standard.~~

Multi Bank Standard Service (MBS-Service) bietet als sektorübergreifende Softwarelösung die Möglichkeit, mit einem einzigen Programm mehrere Kontoverbindungen bei unterschiedlichen Banken anzusprechen.

~~Multi Bank Standard Service (MBS-Service) bietet als sektorübergreifende Softwarelösung die Möglichkeit, mit einem einzigen Programm mehrere Kontoverbindungen bei unterschiedlichen Banken anzusprechen.~~

Kunden haben die Möglichkeit, MBS auch über Softwareprodukte anderer Banken, mit denen eine Verbindung zum Bankrechner der Schoellerbank hergestellt werden kann, zu nutzen. Abhängig von der Berechtigungsverwaltung dieser Softwareprodukte kann der Verfüger, sowie allfällige von diesem 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 gestellt hat.

~~Kunden haben die Möglichkeit, MBS auch über Softwareprodukte anderer Banken, mit denen eine Verbindung zum Bankrechner der Schoellerbank hergestellt werden kann, zu nutzen. Abhängig von der Berechtigungsverwaltung dieser Softwareprodukte kann der Verfüger, sowie allfällige von diesem 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 gestellt hat.~~

20. Entgelte

Die geltenden Gebühren für das Schoellerbank Electronic Banking werden separat bzw. durch Preisaushang mitgeteilt. Auf Z 43 - 46 der Allgemeinen Geschäftsbedingungen der Schoellerbank wird hingewiesen. Der Kunde erhält den Preisaushang sowie die Allgemeinen Geschäftsbedingungen der Schoellerbank gleichzeitig mit gegenständlichen "Bedingungen zur Teilnahme am Electronic Banking": Wird zum Zeitpunkt der Unterfertigung des Antrages zur Teilnahme am Schoellerbank Online Banking, Business Banking bzw. MBS-Service kein gesondertes Entgelt für die Inanspruchnahme von Schoellerbank Electronic Banking verrechnet, ist die Schoellerbank AG berechtigt, nach entsprechender Ankündigung ein Entgelt zu verrechnen.

~~**20. Entgelte**~~

~~Die geltenden Gebühren für das Schoellerbank Electronic Banking werden separat bzw. durch Preisaushang mitgeteilt. Auf Z 43 - 46 der Allgemeinen Geschäftsbedingungen der Schoellerbank wird hingewiesen. Der Kunde erhält den Preisaushang sowie die Allgemeinen Geschäftsbedingungen der Schoellerbank gleichzeitig mit gegenständlichen "Bedingungen zur Teilnahme am Electronic Banking": Wird zum Zeitpunkt der Unterfertigung des Antrages zur Teilnahme am Schoellerbank Online Banking, Business Banking bzw. MBS-Service kein gesondertes Entgelt für die Inanspruchnahme von Schoellerbank Electronic Banking verrechnet, ist die Schoellerbank AG berechtigt, nach entsprechender Ankündigung ein Entgelt zu verrechnen.~~

Die dem Kunden vom Netzwerkanbieter angelasteten Telefongebühren und Entgelte gehen zu Lasten des Kunden. Nicht berührt werden weiters die Entgelte im Zusammenhang mit der Kontoführung. Der Kunde erteilt der Schoellerbank die Ermächtigung, die jeweils anfallenden Gebühren seinem Konto anzulasten.

~~Die dem Kunden vom Netzwerkanbieter angelasteten Telefongebühren und Entgelte gehen zu Lasten des Kunden. Nicht berührt werden weiters die Entgelte im Zusammenhang mit der Kontoführung. Der Kunde erteilt der Schoellerbank die Ermächtigung, die jeweils anfallenden Gebühren seinem Konto anzulasten.~~

21. Änderung der Geschäftsbedingungen

Änderungen dieser Geschäftsbedingungen erlangen nach Ablauf von 2 Monaten ab der Verständigung des Kunden Rechtsgültigkeit für alle gegenwärtigen und künftigen Nutzungen des Electronic Banking, sofern nicht bis dahin ein schriftlicher Widerspruch des Kunden bei der Schoellerbank einlangt. Die Verständigung des Kunden kann in jeder Form erfolgen, die mit ihm im Rahmen der Geschäftsverbindung vereinbart worden ist (insbesondere schriftlich durch Benachrichtigung auf einem Kontoauszug oder elektronisch im Rahmen des Electronic Banking). Eine mit dem Kunden getroffene Vereinbarung über den Zugang von Erklärungen der Schoellerbank gilt auch für die Verständigung von Änderungen dieser Geschäfts-bedingungen.

Die Schoellerbank wird den Kunden anlässlich der Benachrichtigung auf die Tatsache der Änderung dieser

Siehe Punkt 11. Änderung der Geschäftsbedingungen

~~**21. Änderung der Geschäftsbedingungen**~~

~~Änderungen dieser Geschäftsbedingungen erlangen nach Ablauf von 2 Monaten ab der Verständigung des Kunden Rechtsgültigkeit für alle gegenwärtigen und künftigen Nutzungen des Electronic Banking, sofern nicht bis dahin ein schriftlicher Widerspruch des Kunden bei der Schoellerbank einlangt. Die Verständigung des Kunden kann in jeder Form erfolgen, die mit ihm im Rahmen der Geschäftsverbindung vereinbart worden ist (insbesondere schriftlich durch Benachrichtigung auf einem Kontoauszug oder elektronisch im Rahmen des Electronic Banking). Eine mit dem Kunden getroffene Vereinbarung über den Zugang von Erklärungen der Schoellerbank gilt auch für die Verständigung von Änderungen dieser Geschäfts-bedingungen.~~

~~Die Schoellerbank wird den Kunden anlässlich der Benachrichtigung auf die Tatsache der Änderung dieser~~

PC282D-Gegenüberstellung 20200101

Geschäftsbedingungen aufmerksam machen und ausdrücklich darauf hinweisen, dass sein Stillschweigen nach Ablauf von 2 Monaten ab Verständigung als Zustimmung zur Änderung gilt und dass er das Recht hat, die Vereinbarung vor dem Inkrafttreten der Änderung kostenlos, fristlos zu kündigen.

~~Geschäftsbedingungen aufmerksam machen und ausdrücklich darauf hinweisen, dass sein Stillschweigen nach Ablauf von 2 Monaten ab Verständigung als Zustimmung zur Änderung gilt und dass er das Recht hat, die Vereinbarung vor dem Inkrafttreten der Änderung kostenlos, fristlos zu kündigen.~~

Sofern es sich um Entgeltsänderungen gegenüber Verbrauchern handelt, darf die Schoellerbank eine Anpassung entsprechend der Entwicklung des von der Statistik Austria veröffentlichten nationalen Verbraucherpreisindex 2000 vornehmen (Erhöhung oder Senkung), wobei jeweils eine kaufmännische Rundung auf ganze Cent erfolgt. Erfolgt bei Erhöhung des Index keine Anhebung der Entgelte aus welchen Gründen immer, so ist dadurch das Recht auf Anhebung in den Folgejahren nicht verloren gegangen. Der Kunde hat das Recht, den Rahmenvertrag bis zum Inkrafttreten der Änderung kostenlos, fristlos zu kündigen. Auch darauf wird das Kreditinstitut den Kunden, der Verbraucher ist, in der Mitteilung über das Änderungsangebot hinweisen.

~~Sofern es sich um Entgeltsänderungen gegenüber Verbrauchern handelt, darf die Schoellerbank eine Anpassung entsprechend der Entwicklung des von der Statistik Austria veröffentlichten nationalen Verbraucherpreisindex 2000 vornehmen (Erhöhung oder Senkung), wobei jeweils eine kaufmännische Rundung auf ganze Cent erfolgt. Erfolgt bei Erhöhung des Index keine Anhebung der Entgelte aus welchen Gründen immer, so ist dadurch das Recht auf Anhebung in den Folgejahren nicht verloren gegangen. Der Kunde hat das Recht, den Rahmenvertrag bis zum Inkrafttreten der Änderung kostenlos, fristlos zu kündigen. Auch darauf wird das Kreditinstitut den Kunden, der Verbraucher ist, in der Mitteilung über das Änderungsangebot hinweisen.~~

Sofern es sich um Entgelts- und Leistungsänderungen gegenüber Unternehmern handelt, gilt Ziffer 43 der Allgemeinen Geschäftsbedingungen der Schoellerbank.

~~Sofern es sich um Entgelts- und Leistungsänderungen gegenüber Unternehmern handelt, gilt Ziffer 43 der Allgemeinen Geschäftsbedingungen der Schoellerbank.~~

Hauptleistungen der Schoellerbank können nicht auf diese Weise geändert werden.

~~Hauptleistungen der Schoellerbank können nicht auf diese Weise geändert werden.~~

Anhang zu den Geschäftsbedingungen zum Electronic Banking

Empfehlung der Bank zur Sicherheit im Internet und Nutzung des Electronic Banking:

1. Electronic Banking wird über das Kommunikationsmedium Internet abgewickelt, welches ein offenes und allgemein zugängliches Medium ist. Unter Verwendung der persönlichen Identifikationsmerkmale des Kunden kann auch ein unberechtigter Dritter in das Internetbanking einsteigen und Dispositionen zulasten des Konto- bzw. Depotinhabers vornehmen. Die Bank informiert auf ihrer Homepage www.schoellerbank.at und direkt im Internetbanking regelmäßig über aktuelle Gefahren im Internet und gibt dort auch konkrete Empfehlungen und Sicherheitshinweise, wie das Verhalten bei der Nutzung des Internetbanking im Hinblick auf diese Gefahren risikominimierend angepasst werden kann. Zur Vermeidung von Schäden bei den Transaktionen im Rahmen des Internetbankings wird dem Kunden empfohlen, besonders sorgfältig vorzugehen.

2. Die Bank führt umfangreiche Maßnahmen zur Absicherung der im Electronic Banking übermittelten und bankseitig verarbeiteten Daten durch und trifft umfassende Sicherheitsvorkehrungen, die einen Schutz gegen Angriffe bei der Übertragung der Daten über das Internet oder bei der Verarbeitung auf dem Bankserver bieten. Damit die vorgesehenen Sicherheitsmaßnahmen nicht gefährdet werden, empfiehlt die Bank jedem Kunden auch in eigenem Interesse seinerseits technische Vorkehrungen zum Schutz der von ihm eingesetzten Systeme und des PCs zu treffen. Die Bank informiert auf ihrer Homepage und im Internetbanking über mögliche Gefahren sowie die gebotenen und empfehlenswerten Sicherheitsmaßnahmen zum Schutz der Systeme und des PCs des Kunden.