

SONDERBEDINGUNGEN FÜR DAS ONLINE-BANKING

Die nachfolgenden „Sonderbedingungen für das Online-Banking“ gelten nur bei Eintritt eines Kündigungsereignisses der Geschäftsbeziehung, wie es zwischen CHECK24 und Multitude Bank p.l.c. festgelegt wurde, oder eines Übertragungsereignisses, wie es in Klausel 9(6) der Allgemeinen Geschäftsbedingungen beschrieben ist.

INHALTSVERZEICHNIS

- 1. Leistungsangebot**
- 2. Voraussetzungen zur Nutzung des Online-Banking**
 - 2.1 Personalisierte Sicherheitsmerkmale
 - 2.2 Authentifizierungsinstrumente
- 3. Zugang zum Online-Banking**
- 4. Online-Banking-Aufträge**
 - 4.1 Auftragserteilung und Autorisierung
 - 4.2 Widerruf von Aufträgen
- 5. Bearbeitung von Online-Banking-Aufträgen durch die Bank**
- 6. Information des Kontoinhabers über Online-Banking-Verfügungen**
- 7. Sorgfaltspflichten des Teilnehmers**
 - 7.1 Technische Verbindung zum Online-Banking
 - 7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente
 - 7.3 Sicherheit des Kundensystems
 - 7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten
- 8. Anzeige- und Unterrichtungspflichten**
 - 8.1 Sperranzeige
 - 8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge
- 9. Nutzungssperre**
 - 9.1 Sperre auf Veranlassung des Teilnehmers
 - 9.2 Sperre auf Veranlassung der Bank
 - 9.3 Aufhebung der Sperre
 - 9.4 Automatische Sperrung eines chipbasierten Authentifizierungsinstrumentes
- 10. Haftung**
 - 10.1 Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung
 - 10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstrumentes
 - 10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge der Sperranzeige
 - 10.2.2 Haftung der Bank ab der Sperranzeige
 - 10.2.3 Haftungsausschluss
- 11. Speicherung von Teilnehmerdaten**
- 12. Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit**
- 13. Kommunikation mit der Bank**
 - 13.1 Das elektronische Postfach
 - 13.2 Verzicht auf papierhafte Zustellung
 - 13.3 Übermittlung von Konto- und Kundendokumenten und Mitwirkungspflicht des Teilnehmers
 - 13.4 Zugang
 - 13.5 Speicherung der Dokumente
- 14. Geschäftsbedingungen**

SONDERBEDINGUNGEN FÜR DAS ONLINE-BANKING

1. Leistungsangebot

(1) Der Kontoinhaber kann Bankgeschäfte mittels Online-Banking in dem von der Multitude Bank p.l.c. (im Folgenden „Bank“ genannt) angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank zum Konto und/oder zu Kontobewegungen mittels Online-Banking abrufen.

(2) Kontoinhaber werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Das Tagesgeldkonto und das Festgeldkonto werden im Folgenden einheitlich als „Konto“ bezeichnet.

(3) Die Bank ist berechtigt, dem Teilnehmer die Änderungen ihrer Geschäftsbedingungen auf elektronischem Weg anzuzeigen und zum Abruf bereitzustellen. Hinsichtlich der Voraussetzungen für das Wirksamwerden von Änderungen gilt Nr. 1 Absatz 2 der Allgemeinen Geschäftsbedingungen.

(4) Zur Nutzung des Online-Banking gelten die mit der Bank gesondert vereinbarten Verfügungslimits. Eine Änderung dieser Limite kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

2. Voraussetzungen zur Nutzung des Online-Banking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels Online-Banking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (vgl. Nummer 3) und Aufträge zu autorisieren (vgl. Nummer 4).

Im Falle mehrerer Teilnehmer (im Falle von Gemeinschaftskonten) werden für jeden Teilnehmer gesondert Personalisierte Sicherheitsmerkmale und Authentifizierungsinstrumente erstellt.

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind:

- die persönliche Identifikationsnummer (PIN) und
- einmal verwendbare Transaktionsnummern (TAN).

2.2 Authentifizierungsinstrumente

Die TAN kann dem Teilnehmer ausschließlich auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:

- mittels eines mobilen Endgerätes (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),

3. Zugang zum Online-Banking

Der Teilnehmer erhält Zugang zum Online-Banking, wenn

- der Teilnehmer die Kontonummer oder seine individuelle Kundenkennung und seine PIN übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (vgl. Nummern 8.1 und 9) vorliegt.

Nach Gewährung des Zugangs zum Online-Banking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

Tritt einer der Umstände ein, die außerhalb der angemessenen Kontrolle der Bank gemäß Klausel 9 Abs. 6 der Allgemeinen Geschäftsbedingungen liegen, so ist der Kunde berechtigt und die Bank räumt dem Kunden das Recht ein, weiterhin über die Multitude Banking App Zugang zum Online-Banking zu haben, vorbehaltlich der Bedingungen des gleichen Abschnitts 9 Abs. 6 der Allgemeinen Geschäftsbedingungen.

4. Online-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Online-Banking-Aufträge (z. B. Überweisungen an das Referenzkonto) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (TAN) autorisieren und der Bank mittels Online-Banking übermitteln. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags. Schriftliche Aufträge oder Aufträge in anderer Weise als über das Online-Banking werden von der Bank nicht akzeptiert.

SONDERBEDINGUNGEN FÜR DAS ONLINE-BANKING

4.2 Widerruf von Aufträgen

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

5. Bearbeitung von Online-Banking-Aufträgen durch die Bank

(1) Die Bearbeitung der Online-Banking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Online-Banking-Seite der Bank gemäß den im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank angegebenen oder im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß dem „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat sich mit dem Personalisierten Sicherheitsmerkmal autorisiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Sonderbedingungen für den Überweisungsverkehr) liegen vor.

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

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

6. Information des Kontoinhabers über Online-Banking-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über seine mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg und gemäß den für den Auftrag geltenden Bedingungen.

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum Online-Banking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online-Banking nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle (z. B. Internetadresse) herzustellen.

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer hat

- seine Personalisierten Sicherheitsmerkmale (vgl. Nummer 2.1) geheim zu halten und nur im Rahmen einer Auftragserteilung über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument (vgl. Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen Personalisierten Sicherheitsmerkmal das Online-Banking-Verfahren missbräuchlich nutzen.

(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

SONDERBEDINGUNGEN FÜR DAS ONLINE-BANKING

- Das Personalisierte Sicherheitsmerkmal (PIN und TAN) darf nicht elektronisch gespeichert werden (z. B. im Kundensystem).
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das Personalisierte Sicherheitssystem darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf Online-Händlerseiten).
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die PIN darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer darf nicht mehr als eine mobile TAN verwenden, um einen Auftrag zu autorisieren.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon) nicht für das Online-Banking genutzt werden.

7.3 Sicherheit des Kundensystems

Der Teilnehmer muss die Sicherheitshinweise der Bank zum Online-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten. Insbesondere muss der Teilnehmer geeignete, dem aktuellen Sicherheitsstandard entsprechende Hard- und Software und marktübliche Sicherheitsvorkehrungen zum Schutz gegen Viren und Missbrauch verwenden.

7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem Online-Banking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z. B. Mobiltelefon) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines Persönlichen Sicherheitsmerkmals fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über gesondert mitgeteilte Kontaktdaten aufgeben.

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

(3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt

- den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder
 - das Authentifizierungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet,
- muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

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

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1,

- den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Bank

SONDERBEDINGUNGEN FÜR DAS ONLINE-BANKING

(1) Die Bank darf den Online-Banking-Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.

(2) Die Bank wird das Konto sperren und die Gründe nach Möglichkeit vor der Sperre angeben, aber sie wird die Gründe spätestens unmittelbar nach der Sperre angeben.

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal bzw. das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Teilnehmer unverzüglich.

9.4 Automatische Blockierung mit einem Chip-basierten Authentifizierungswerkzeug

(1) Die Chipkarte mit Signaturfunktion deaktiviert sich selbst, wenn der Verwendungscodes für die elektronische Signatur dreimal hintereinander falsch eingegeben wird.

(2) Ein TAN-Generator, der die Eingabe eines eigenen Verwendungscodes des Teilnehmers erfordert, kann sich bei dreimaliger Falscheingabe in Folge selbst sperren.

(3) Die in den Absätzen 1 und 2 genannten Authentifizierungsinstrumente können dann nicht mehr für das Online-Banking verwendet werden. Der Teilnehmer kann sich in diesem Zusammenhang mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wieder herzustellen.

10. Haftung

10.1 Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung

Die Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr).

10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob dem Teilnehmer an dem Verlust, Diebstahl oder sonstigem Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen, gestohlen oder sonst abhandengekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der Personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

(3) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 2 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(4) Kommt es zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, bevor die Sperre möglich war, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere dann vorliegen, wenn er

- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (vgl. Nummer 8.1 Absatz 1),

SONDERBEDINGUNGEN FÜR DAS ONLINE-BANKING

- das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (vgl. Nummer 7.2. Absatz 1, 3. Spiegelstrich),
- sein Personalisiertes Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (vgl. Nummer 7.2 Absatz 1, 2. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (vgl. Nummer 7.2 Absatz 2, 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (vgl. Nummer 7.2. Absatz 2, 4. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (vgl. Nummer 7.2. Absatz 2, 5. Spiegelstrich),
- mehr als eine TAN für einen Auftrag autorisiert (vgl. Punkt 7.2, Absatz 2, 6. Spiegelstrich),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon) auch für das Online-Banking nutzt (vgl. Nummer 7.2 Absatz 2, 7. Spiegelstrich).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

10.2.2 Haftung der Bank ab der Sperranzeige

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

10.2.3 Haftungsausschluss

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

Haftungsansprüche von Kunden, die am Zugang zum Online-Banking gehindert wurden, sind ebenfalls ausgeschlossen, wenn die Umstände, die solche Ansprüche begründen, nach den einschlägigen Bestimmungen der Klausel 10 der Allgemeinen Geschäftsbedingungen außerhalb der angemessenen Kontrolle der Bank liegen.

11. Speicherung von Teilnehmerdaten

Aufgrund gesetzlicher Vorschriften werden die Teilnehmerdaten zum Zwecke der Vertragsdurchführung von der Bank gespeichert.

12. Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit

Für die Beilegung von Streitigkeiten mit der Bank kann sich der Teilnehmer an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.

13. Kommunikation mit der Bank

13.1 Das elektronische Postfach

Im Rahmen der Geschäftsbeziehung zwischen der Bank und dem Teilnehmer gilt das elektronische Postfach (Online-Banking-Postfach) als Kanal, über den der Teilnehmer der Bank Dokumente (z. B. Kontoauszüge, Rechnungsabschlüsse und sonstige Informationen) in elektronischer Form bereitstellen kann. Ausgenommen sind Dokumente, bei denen die Schriftform vorgeschrieben ist. Mit der Anmeldung zum Online-Banking werden dem Teilnehmer Dokumente und Mitteilungen zu gegenwärtigen und künftigen Konten in das elektronische Postfach eingestellt. Möchte der Teilnehmer das elektronische Postfach für bestimmte Konten nicht nutzen, kann die Bank diese Konten für einen anderen Versandkanal zulassen. Diese Nutzung der anderen Kanäle ist kostenpflichtig.

13.2 Verzicht auf papierhafte Zustellung

Mit der Einrichtung des elektronischen Postfachs verzichtet der Kunde nach Maßgabe dieser Bedingungen ausdrücklich auf den postalischen Versand der in das Postfach einzustellenden Mitteilungen. Die Bank ist jedoch berechtigt, dem Teilnehmer

SONDERBEDINGUNGEN FÜR DAS ONLINE-BANKING

Dokumente in Papierform auf dem Postweg zu übersenden, z. B. um gesetzliche Pflichten zu erfüllen oder, wenn sie dies – auch unter Abwägung der Interessen des Kunden – für zweckmäßig erachtet.

13.3 Übermittlung von Konto- und Kundendokumenten und Mitwirkungspflicht des Teilnehmers

Die Bank stellt dem Kunden Mitteilungen, die den Geschäftsverkehr mit der Bank betreffen, elektronisch als Datei zur Verfügung; dies gilt auch für Anlagen. Der Teilnehmer ist verpflichtet, seine Dokumente aus dem elektronischen Postfach regelmäßig abzurufen sowie diese unverzüglich auf Richtigkeit und Vollständigkeit hin zu prüfen sowie etwaige Einwendungen unverzüglich zu erheben.

13.4 Zugang

Die Mitteilungen der Bank an das elektronische Postfach gelten mit der Einstellung und der Möglichkeit zum Abruf durch den Teilnehmer als zugegangen.

13.5 Speicherung der Dokumente

Die Bank speichert die im elektronischen Postfach hinterlegten Informationen im Rahmen der gesetzlichen Aufbewahrungsfristen. Nach Ablauf dieser Frist kann die Bank die entsprechenden Informationen aus dem elektronischen Postfach löschen, ohne dass der Teilnehmer hierzu eine gesonderte Mitteilung erhält.

14. Geschäftsbedingungen

Die Allgemeinen Geschäftsbedingungen und die jeweiligen Sonderbedingungen zu den Produkten gelten ergänzend zu diesen Sonderbedingungen.