

# Vereinbarung über die Nutzung des Online-Bankings mit PIN und iTAN (Online-Banking) und Telefon-Bank-Service (TBS)

Kundennummer \_\_\_\_\_

Antragsteller

Herr

Frau

Anredezusätze \_\_\_\_\_

Name, Vorname \_\_\_\_\_

Straße, Hausnummer \_\_\_\_\_

Postleitzahl, Ort \_\_\_\_\_

Der genannte Antragsteller vereinbart mit der Bank für die elektronische Datenübermittlung im Wege des Online-Banking-Dialogs mit PIN und iTAN (Online-Banking) und für die Teilnahme am Telefon-Bank-Service Folgendes:

## 1. Vertragsgegenstand

Der Konto-/Depotinhaber sowie etwaige mit separater Konto-/Depotvollmacht Bevollmächtigte (im Folgenden einheitlich „Teilnehmer“ genannt) sind zu den nachfolgend aufgeführten Bedingungen, soweit sie auf Online-Banking anwendbar sind, zur Inanspruchnahme des Online-Bankings in dem von der Bank angebotenen Umfang berechtigt. Die Online-Nutzung bezieht sich auf alle derzeit und zukünftig bei der Augsburger Aktienbank geführten Konten und Depots.

Des Weiteren vereinbart der Antragsteller gleichzeitig die Nutzung des Telefon-Bank-Service (TBS) zu den nachfolgend aufgeführten Bedingungen, soweit sie auf Telefon-Bank-Service anwendbar sind.

## 2. Zugangsvoraussetzungen

Die Teilnahme am TBS und Online-Banking steht Inhabern von Einzelkonten/-depots (Privatpersonen sowie Einzelkaufleuten), Inhabern von Gemeinschaftskonten/-depots mit Einzelverfügungsberechtigung (Oder-Konten/-Depots) sowie Konto-/Depot-Bevollmächtigten zur Verfügung. Die Vereinbarung gilt für alle vorhandenen sowie zukünftigen Konten/Depots.

Das gegenwärtige Leistungsangebot und die derzeit möglichen Verfügungen und weitere Erläuterungen beim Online-Banking und Telefon-Bank-Service sind in den beiliegenden Bedingungen für das Online-Banking und den Telefon-Bank-Service, die wesentlicher Vertragsbestandteil werden, dargestellt.

Die Augsburger Aktienbank AG ist unter dem folgenden Kommunikationszugang per Online-Banking erreichbar: <https://akp.aab.de>

Zur Abwicklung von Bankgeschäften per Online-Banking benötigt der Teilnehmer die in den Bedingungen für das Online-Banking vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente. Es besteht unter anderem die Gefahr, dass die Personalisierten Sicherheitsmerkmale Unbefugten zugänglich werden, wenn im Internet die Bankadresse nicht direkt angegeben wird (z. B. bei Links). Daher sind Bankgeschäfte nur unter vorbenanntem direktem Kommunikationszugang zu tätigen (siehe auch Ziffer 7.2 der Bedingungen für das Online-Banking).

## 3. Sperranzeige des Teilnehmers

Die Sperranzeige nach Nr. 8. 1 der Bedingungen für das Online-Banking kann der Teilnehmer unter der Telefonnummer 08 21.50 15-554 der Bank jederzeit mitteilen.

## 4. Einbeziehung der Bedingungen

Für die Teilnahme am Online-Banking gelten die „Bedingungen für das Online-Banking“. Für die Teilnahme am Telefon-Bank-Service gelten die „Bedingungen für den Telefon-Bank-Service“. Ergänzend gelten jeweils die Allgemeinen Geschäftsbedingungen sowie die Sonderbedingungen der Bank.

## 5. PIN-/iTAN-Versand

Alle PIN-/iTAN-Briefe werden standardmäßig an die bei der Augsburger Aktienbank AG hinterlegte Versandadresse verschickt. Ist keine Versandadresse gespeichert, werden die Briefe an die Meldeadresse verschickt. Die Meldeadresse ist die im Konto-/Depoteröffnungsantrag vom Konto-/Depotinhaber angegebene Adresse. Die Versandadresse ist die vom Konto-/Depotinhaber für den Versand von Unterlagen der Bank gesondert mitgeteilte Adresse.

Ich wünsche, dass die PIN-/iTAN-Briefe an die Meldeadresse versandt werden.

## 6. Hinweis nach dem Telemediengesetz

Die im Rahmen des Online-Bankings und TBS anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und der von ihr beauftragten Rechenzentren LVM Landwirtschaftlicher Versicherungsverein Münster a.G., Münster und T-Systems RZ, Frankfurt a. Main, innerhalb Deutschlands bzw. der Europäischen Union erhoben, verarbeitet und genutzt. Einzelheiten zum Datenschutz kann der Teilnehmer unter [www.aab.de](http://www.aab.de) entnehmen.

## 7. Zugangsmedien

Sofern die Augsburger Aktienbank AG bei der Auftragserteilung über eines der genannten Kommunikationsmittel (z. B. Internet) nicht erreichbar ist, ist der Teilnehmer verpflichtet, auf ein anderes Kommunikationsmittel (z. B. Telefon, Telefax) auszuweichen.

## 8. Elektronisches Postfach/Verzichtserklärung des Konto-/Depotinhabers

Die Bank stellt dem Konto-/Depotinhaber im Rahmen des Online-Banking optional ein elektronisches Postfach zur Verfügung. Die Bank ist berechtigt, dem Konto-/Depotinhaber zur Erfüllung Ihrer Informations- und Rechnungslegungspflichten erforderliche Bankmitteilungen sowie sonstige geeignete Nachrichten gemäß Ziffer 1 der Online-Banking-Bedingungen durch Bereitstellung zum Abruf in dem kostenlos eingerichteten elektronischen Postfach nachzukommen.

Der Konto-/Depotinhaber verzichtet auf die papierhafte Bereitstellung der gemäß Ziffern 1 und 11 der Bedingungen für das Online-Banking zum Abruf bereitgestellten Bankmitteilungen. Der Konto-/Depotinhaber ist berechtigt den Versandweg jederzeit zu ändern. Der Konto-/Depotinhaber erhält dann die Bankmitteilungen gegen Ersatz der Portopauschale, deren Höhe sich nach dem jeweils gültigen Preis- und Leistungsverzeichnis der Bank bemisst, in Papierform auf dem Postweg.

Ich möchte das elektronische Postfach nicht nutzen und wünsche gegen Entrichtung der Portopauschale die Zusendung der Bankmitteilungen in Papierform auf dem Postweg. Entsprechend ermächtige ich hiermit die Bank die Portopauschale meinem bei der Augsburger Aktienbank AG geführten Konto zu belasten.

## 9. Reines Ausführungsgeschäft/Execution only/beratungsfreies Geschäft

Im Rahmen der Nutzung des Online-Bankings und des Telefon-Bank-Service kann der Teilnehmer in dem jeweils beschriebenen Leistungsumfang auch Wertpapieraufträge erteilen (Online-Brokerage). Beratungsleistungen und/oder Portfolioverwaltungsleistungen zu den vom Teilnehmer beabsichtigten Wertpapieraufträgen bietet die Bank im Rahmen des Online-Brokerage nicht an. Die Augsburger Aktienbank weist darauf hin, dass sie Kundenaufträge und Wertpapiergeschäfte im Interesse einer kostengünstigen Abwicklung lediglich ausführt (Execution only/reines Ausführungsgeschäft). Die Augsburger Aktienbank bietet keine Anlageberatung an. Sofern die Augsburger Aktienbank dem Konto-/Depotinhaber Prospekte, Marktcommentare und allgemeine Marktdaten, Charts, Nachrichten etc. zur Verfügung stellt, ist dies keine Anlageberatung, sondern dient der allgemeinen und nicht personenspezifischen Kundeninformation und soll dem Konto-/Depotinhaber lediglich die eigenständige und eigenverantwortliche Anlageentscheidung erleichtern. Sofern eine Kundenorder zu sogenannten komplexen Finanzinstrumenten (z. B. Zertifikate) erteilt wird, prüft die Augsburger Aktienbank AG lediglich die Angemessenheit der Dienstleistung und/oder des Finanzinstruments. Auf Buchstabe B der "Informationen für Wertpapierkunden und -interessenten der Augsburger Aktienbank AG" wird hingewiesen.

Ort, Datum \_\_\_\_\_

 Unterschrift Antragsteller

Hiermit bestätige ich, dass die Vertragserklärungen des Konto-/Depotinhabers in meiner Anwesenheit abgegeben wurden.

Ort, Datum \_\_\_\_\_

Stempel/Name in Druckbuchstaben \_\_\_\_\_

 Unterschrift des Vermittlers

Original für die Bank 

# Bedingungen für das Online-Banking

## 1. Leistungsangebot

(1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels Online-Banking in dem von der Bank angebotenen Umfang abwickeln. Die Bank behält sich das Recht vor, den Umfang der über das Online-Banking abwickelbaren Bankgeschäfte jederzeit zu erweitern, einzuschränken, von zusätzlichen Voraussetzungen abhängig zu machen oder das Online-Banking ohne nähere Angabe von Gründen ganz einzustellen. Gleichzeitig hat die Bank das Recht, die Art und Weise der Auftragserteilung unter Berücksichtigung der berechtigten Belange des Kunden jederzeit zu verändern oder von weiteren Aufträgen abhängig zu machen. Die Bank wird den Kunden über derartige Änderungen unterrichten. Zudem kann der Konto-/Depotinhaber Informationen der Bank mittels Online-Banking abrufen.

(2) Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.

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

(4) Die Bereitstellung der technischen Zugangswege (insbesondere der Internet-Zugang des Teilnehmers) gehört nicht zu den Leistungen der Bank, auch wenn über diese Zugangswege Leistungen der Bank genutzt werden können. Diese technischen Zugangswege werden aufgrund gesonderter Verträge bereit gestellt, die der Teilnehmer mit dem jeweiligen Anbieter abschließt. Die Bank ist für Störungen dieser technischen Zugangswege nicht verantwortlich; sie übernimmt hierfür keine Gewährleistung oder Haftung.

## 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 (siehe Nr. 3) und Aufträge zu autorisieren (siehe Nr. 4).

### 2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare indizierte Transaktionsnummern (iTAN)

### 2.2 Authentifizierungsinstrument

Die iTAN kann dem Teilnehmer auf folgendem Authentifizierungsinstrument zur Verfügung gestellt werden:

- auf einer Liste mit einmal verwendbaren iTANs.

## 3. Zugang zum Online-Banking

Der Teilnehmer erhält Zugang zum Online-Banking, wenn

- dieser 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 (siehe Nr. 8.1 und 9) vorliegt.

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

## 4. Online-Banking-Aufträge

### 4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Online-Banking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (iTAN) autorisieren und der Bank mittels Online-Banking übermitteln. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags.

### 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 Widerrufsmöglichkeit 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) im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauf folgenden 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 seinem Personalisierten Sicherheitsmerkmal legitimiert;
- die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) 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 Bedingungen 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, Bedingungen für das Wertpapiergeschäft) aus.

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

## 6. Information des Kontoinhabers über Online-Banking-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg,

- sofern es sich um einen Zahlungsdienstvertragsvertrag handelt und
- sofern Zahlungsvorgänge im Unterrichtszeitraum stattgefunden haben.

## 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 (siehe Nr. 2.1) geheim zu halten und nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument (siehe Nr. 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:

- Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (z. B. im Kundensystem).
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können; insbesondere darf das Personalisierte Sicherheitsmerkmal nicht an Mitarbeiter der Bank weitergegeben werden.
- Das Personalisierte Sicherheitsmerkmal 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 zur Autorisierung zum Beispiel eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung einer neuen iTAN-Liste nicht mehr als eine iTAN verwenden.

### 7.3 Sicherheit des Kundensystems

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

### 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, Wertpapier-Kennnummer) im Kundensystem 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 die gesondert mitgeteilten Kontaktdaten abgeben.

(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 Konto-/Depotinhaber 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 Nr. 8.1

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

### 9.2 Sperre auf Veranlassung der Bank

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

(2) Die Bank wird den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

### 9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber unverzüglich.

## 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, Bedingungen für das Wertpapiergeschäft).

### 10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

#### 10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 EUR, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigen 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 abhanden gekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 EUR, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der Personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 EUR nach Abs. 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

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

hatte und der Schaden dadurch eingetreten ist.

(5) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere 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 (siehe Nr. 8.1 Abs. 1),
- das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nr. 7.2 Abs. 2 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nr. 7.2 Abs. 1 2. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nr. 7.2 Abs. 2 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nr. 7.2 Abs. 2 4. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nr. 7.2 Abs. 2 5. Spiegelstrich),
- mehr als eine iTAN zur Autorisierung eines Auftrags verwendet hat (siehe Nr. 7.2 Abs. 2 6. Spiegelstrich),

(6) 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 des Depotinhabers bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften der Depotinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

#### 10.2.3 Haftung der Bank ab der Sperranzeige

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

#### 10.2.4 Haftungsausschluss

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

## 11. Vereinbarung über die Nutzung des elektronischen Postfachs

(1) Umfang und Übermittlung von Dokumenten

Die Bank stellt dem Teilnehmer in Erfüllung ihrer Informations- und Rechnungslegungspflichten nach Wahl der Bank einzelne und/oder sämtliche Dokumente, die im Rahmen der Konto-/Depotführung anfallen (nachfolgend Dokumente genannt), elektronisch, nach Maßgabe von Ziffer 6 zum Abruf bereit, d. h. der Teilnehmer kann sich die Dokumente online ansehen, herunterladen, ausdrucken und archivieren.

Die Bank behält sich das Recht vor, die Dateiform, die Auswahl und den Umfang der in das elektronische Postfach einzustellenden Dokumente nach Ihrem Ermessen (§ 315 BGB) zu ändern.

Die Inhalte des elektronischen Postfachs kann der Teilnehmer über den Menüpunkt „Postfach“ aus seiner Online-Banking-Anwendung abrufen.

(2) Verzicht auf papierhafte Dokumente

Der Teilnehmer verzichtet auf die papierhafte Bereitstellung von den in Abs. 1 genannten Dokumenten. Lediglich den „Zwangsauszug“ (vgl. Abs. 3) erhält der Teilnehmer per Post. Die Bank ist bereit, dem Teilnehmer auf dessen Wunsch innerhalb der gesetzlichen Aufbewahrungsfristen Dokumente (insbesondere Kontoauszüge/Rechnungsabschlüsse) in Papierform (Zweitschriften) auf seine Kosten zu erstellen und postalisch zu versenden. Das von der Bank hierfür festgesetzte jeweilige Entgelt ergibt sich aus dem jeweils gültigen Preis- und Leistungsverzeichnis der Bank. Nach Ablauf der gesetzlichen Aufbewahrungsfristen wird die Bank die Dokumente löschen.

(3) Zusendung von Dokumenten, Information des Teilnehmers per E-Mail

Die Bank behält sich das Recht vor, einzelne Dokumente dem Teilnehmer auf seine Kosten postalisch zuzusenden, wenn dies gesetzliche Vorgaben erforderlich machen oder sie dies auch unter Abwägung der Interessen des Teilnehmers für gerechtfertigt hält (z. B. bei vorübergehendem Ausfall des elektronischen Postfachs oder sonstigen technischen Problemen).

Sie kann dem Teilnehmer die Kontoauszüge/Rechnungsabschlüsse per Post zusenden, wenn sie feststellt, dass der elektronische Abruf der Kontoauszüge/Rechnungsabschlüsse nach Ablauf eines fest definierten Zeitraumes nicht erfolgt ist. Die Kosten

hierfür werden dem Teilnehmer in Rechnung gestellt.

Soweit nicht bereits an anderer Stelle vereinbart, legen Bank und Teilnehmer hiermit einen Zeitraum von 28 Tagen, nach dessen Ablauf eine Zusendung der Kontoauszüge/Rechnungsabschlüsse zwangsweise per Post erfolgt (Zwangsauszug), fest. Das Entgelt hierfür ergibt sich aus dem jeweils gültigen Preis- und Leistungsverzeichnis der Bank.

Der Teilnehmer kann sich optional beim Eingang neuer Dokumente in sein elektronisches Postfach per E-Mail benachrichtigen lassen. Die E-Mail-Adresse bzw. die Benachrichtigungsfunktion kann in der E-Mail-Konfiguration jederzeit geändert bzw. deaktiviert werden. Die E-Mail-Adresse wird durch die Bank vertraulich behandelt und nicht an Dritte weitergegeben. Die Benachrichtigungs-E-Mails enthalten keinerlei persönliche Informationen des Teilnehmers bzw. keine elektronischen Dokumente. Ebenso wenig wird der Teilnehmer mit der Benachrichtigungs-E-Mail aufgefordert, einen Link innerhalb der Nachricht anzuklicken bzw. seine Zugangsdaten zum Online-Banking, oder sonstigen persönlichen Dokumenten zu übermitteln. Auf die Benachrichtigungs-E-Mail kann nicht geantwortet werden. Die Benachrichtigungs-E-Mail dient lediglich der Information und entbindet den Teilnehmer nicht von seinen Kontroll-, Mitwirkungs- und Sorgfaltspflichten.

#### (4) Voraussetzungen für den Abruf der Dokumente, Mitwirkungspflichten des Teilnehmers

Der Teilnehmer verpflichtet sich zur Nutzung der Funktion „elektronisches Postfach“ eine Software z. B. Adobe Acrobat Reader einzusetzen, die folgende Anforderungen erfüllt:

- Der Name der Bank wird im elektronischen Kontoauszug/Rechnungsabschluss angegeben.
- Der Name des Kontoinhabers wird auf dem elektronischen Kontoauszug/Rechnungsabschluss angegeben.
- Der Hinweis auf den Rechnungsabschluss und die damit verbundenen Rechtsfolgen (Genehmigungsfiktion) sind auf dem elektronischen Kontoauszug angegeben.

Wird daher seitens des Teilnehmers festgestellt, dass die von ihm eingesetzte Software diesem Funktionsumfang nicht genügt (z. B. weil der Verwendungszweck nicht vollständig übermittelt wird), ist die eingesetzte Software für das Verfahren des elektronischen Postfachs nicht geeignet. In diesem Fall ist der Teilnehmer verpflichtet, die Übersendung der in Abs. 1 genannten Dokumente in Papierform zu beantragen. Die Bank wird daraufhin die Dokumente in Papierform zur Verfügung stellen, d. h. die Vereinbarung über die Nutzung des elektronischen Postfachs wird solange ausgesetzt, bis der Teilnehmer meldet, dass er über geeignete Software verfügt.

#### (5) Zugang

Soweit der Teilnehmer die Dokumente nicht bereits vorher abgerufen hat, gelten sie am Tag nach der Bereitstellung als zugegangen.

#### (6) Verfügbarkeit, Speicherung, Haftung

Der Teilnehmer nimmt zur Kenntnis, dass die Verfügbarkeit des elektronischen Postfachs aufgrund von Störungen von Netzwerk- oder Telekommunikationsverbindungen, höherer Gewalt, aufgrund von für den reibungslosen Betriebsablauf erforderlichen Wartungsarbeiten oder sonstigen Umständen eingeschränkt oder zeitweise ausgeschlossen sein kann.

Ausdrucke der in das elektronische Postfach eingestellten Dokumente stellen lediglich Zweitschriften dar und sind daher beweisrechtlich papierhaften Originaldokumenten nicht gleichgestellt.

Die Bank weist den Teilnehmer darauf hin, dass jedes Dokument grundsätzlich nur einmal übermittelt wird. Für die dauerhafte Speicherung und Aufbewahrung der Dokumente, ggfs. unter Beachtung steuerrechtlicher Vorgaben, ist der Teilnehmer selbst verantwortlich. Im elektronischen Postfach eingestellte Dokumente werden maximal zwei Jahre nach Einstellung des jeweiligen Dokumentes vorgehalten. Nach Ablauf dieser Frist wird die Bank die Dokumente automatisch und wird diese ohne zusätzliche Mitteilung an den Teilnehmer aus dem elektronischen Postfach entfernen. Im übrigen speichert die Bank die im elektronischen Postfach enthaltenen Dokumente auf ihren Systemen (z. B. im Kernbanksystem) entsprechend den gesetzlichen Aufbewahrungsfristen. Nach Ablauf dieser Fristen wird Sie die entsprechenden Dokumente löschen, ohne dass der Teilnehmer hierüber eine gesonderte Nachricht erhält.

Werden Dokumente verändert oder in veränderter Form in Umlauf gebracht, übernimmt die Bank hierfür keine Haftung. Die Bank übernimmt keine Gewähr, dass aufgrund der individuellen Systemumgebung des Teilnehmers ein Ausdruck der elektronischen Dokumente mit der Darstellung auf dem Bildschirm übereinstimmt.

Die Bank haftet nicht für dem Teilnehmer aus dem Verzicht auf papierhafte Dokumente entstehende Nachteile. Dies betrifft insbesondere die ggfs. notwendige Mitwirkungs- und Nachweispflicht über Buchungen gegenüber Dritten (z. B. Finanzbehörden). Es liegt in der Verantwortung des Teilnehmers, die Anerkennung der durch ihn erstellten Ausdrucke der elektronischen Dokumente, insbesondere des elektronischen Kontoauszuges/Rechnungsabschlusses, vor Abschluss dieser Vereinbarung mit den betroffenen Dritten zu vereinbaren/abzuklären.

#### (7) Kontroll- und Mitwirkungspflichten des Teilnehmers

Der Teilnehmer ist verpflichtet, das elektronische Postfach auf den Eingang neuer

Dokumente zu kontrollieren. Die Kontrolle ist regelmäßig – entsprechend den üblichen Gepflogenheiten bei einem normalen Briefkasten – insbesondere jedoch dann vorzunehmen, wenn aufgrund eines zuvor erteilten Auftrages mit der Einstellung neuer Dokumente zu rechnen ist. Der Teilnehmer verpflichtet sich im elektronischen Postfach neu hinterlegte Dokumente regelmäßig abzurufen und neu eingegangene Dokumente auf Richtigkeit und Vollständigkeit zu kontrollieren. Beanstandungen und Einwendungen sind der Bank unverzüglich nach Zugang des entsprechenden Dokuments und aus Beweisgründen schriftlich mitzuteilen. Soweit den Teilnehmern hinsichtlich der bislang papierhaft übersandten Dokumente Verpflichtungen treffen, bestehen diese in gleicher Weise für die durch das elektronische Postfach übermittelten Dokumente.

#### (8) Kündigung

Der Teilnehmer kann diese Vereinbarung über die Teilnahme am elektronischen Postfach jederzeit ohne Angabe von Gründen schriftlich kündigen. Ab dem Wirksamwerden der Kündigung werden die Dokumente papierhaft zur Verfügung gestellt. Das Entgelt hierfür ergibt sich aus dem jeweils gültigen Preis- und Leistungsverzeichnis der Bank. Die Bank ist nicht verpflichtet dem Teilnehmer die im Zeitpunkt der Wirksamkeit der Kündigung im elektronischen Postfach befindlichen Dokumente nachträglich postalisch unentgeltlich zuzusenden. Der Teilnehmer verpflichtet sich, die bis zum Wirksamwerden der Kündigung im elektronischen Postfach gespeicherten Dokumente zu kontrollieren und diese ggfs. auszudrucken und/oder abzuspeichern. Die Kündigung der Teilnahme am elektronischen Postfach lässt die Wirksamkeit der Vereinbarung über die Nutzung des Online-Bankings mit PIN und iTAN (Online-Banking) und Telefon-Bank-Service (TBS) nebst den Bedingungen für das Online-Banking und den Bedingungen für den Telefon-Bank-Service (TBS) im übrigen unberührt.

Stand: Oktober 2009

# Bedingungen für den Telefon-Bank-Service (TBS)

## 1. Leistungsangebot

(1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels Telefon-Bank-Service (Telefon-Banking) in dem von der Bank angebotenen Umfang abwickeln. Die Bank behält sich das Recht vor, den Umfang der über das Telefon-Banking abwickelbaren Bankgeschäfte jederzeit zu erweitern, einzuschränken, von zusätzlichen Voraussetzungen abhängig zu machen oder das Telefon-Banking ohne nähere Angabe von Gründen ganz einzustellen. Gleichzeitig hat die Bank das Recht, die Art und Weise der Auftragserteilung unter Berücksichtigung der berechtigten Belange des Kunden jederzeit zu verändern oder von weiteren Auflagen abhängig zu machen. Die Bank wird den Kunden über derartige Änderungen unterrichten. Zudem kann der Konto-/Depotinhaber Informationen der Bank mittels Telefon-Banking abrufen.

(2) Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.

(3) Zur Nutzung des Telefon-Banking gelten die mit der Bank unter Ziffer 5 Abs. 2 vereinbarten Verfügungsmitte.

(4) Die Bereitstellung der technischen Zugangswege gehört nicht zu den Leistungen der Bank, auch wenn über diese Zugangswege Leistungen der Bank genutzt werden können. Diese technischen Zugangswege werden aufgrund gesonderter Verträge bereitgestellt, die der Teilnehmer mit dem jeweiligen Anbieter abschließt. Die Bank ist für Störungen dieser technischen Zugangswege nicht verantwortlich; sie übernimmt hierfür keine Gewährleistung oder Haftung.

## 2. Voraussetzungen zur Nutzung des Telefon-Banking

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

### 2.1 Personalisierte Sicherheitsmerkmale

Personalisiertes Sicherheitsmerkmal, das auch alphanumerisch sein kann, ist:

- die persönliche Identifikationsnummer (Telefon-Bank-PIN).

### 2.2 Authentifizierungsinstrumente

Die Telefon-Bank-PIN kann dem Teilnehmer auf folgendem Authentifizierungsinstrument zur Verfügung gestellt werden:

- auf einem Dokument, das die Telefon-Bank-PIN beinhaltet.

## 3. Zugang zum Telefon-Banking

Der Teilnehmer erhält Zugang zum Telefon-Banking, wenn

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

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

## 4. Telefon-Banking-Aufträge

### 4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Telefon-Banking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (Telefon-Bank-PIN) autorisieren und der Bank mittels Telefon-Banking erteilen.

### 4.2 Widerruf von Aufträgen

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

## 5. Bearbeitung von Telefon-Banking-Aufträgen durch die Bank

(1) Die Bearbeitung der Telefon-Banking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauf folgenden 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 seinem Personalisierten Sicherheitsmerkmal legitimiert;
- die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor;

- das Telefon-Banking-Verfügungslimit in Höhe des Kontoguthabens bzw. in Höhe des durch gesonderte Vereinbarung eingeräumten Überziehungskredits, höchstens jedoch 10.000 EUR pro Tag ist nicht überschritten;
- die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

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

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

## 6. Information des Kontoinhabers über Telefon-Banking-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Telefon-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg,

- sofern es sich um einen Zahlungsdienstleistungsvertrag handelt und
- sofern Zahlungsvorgänge im Unterrichtszeitraum stattgefunden haben.

## 7. Sorgfaltspflichten des Teilnehmers

### 7.1 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer hat

- seine Personalisierten Sicherheitsmerkmale (siehe Nr. 2.1) geheim zu halten und nur über das Telefon-Banking an die Bank zu übermitteln sowie
- sein Authentifizierungsinstrument (siehe Nr. 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals ist, kann das Telefon-Banking-Verfahren missbräuchlich nutzen.

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

- Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden.
- Bei Mitteilung des Personalisierten Sicherheitsmerkmals mittels Telefon-Banking ist sicherzustellen, dass andere Personen dieses nicht ausspähen können; insbesondere darf das Personalisierte Sicherheitsmerkmal nur an Mitarbeiter der Bank zum Zwecke der Autorisierung weitergegeben werden.
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des Telefon-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.

### 7.2 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem Telefon-Banking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapier-Kennnummer) zur Bestätigung telefonisch wiedergibt, ist der Teilnehmer verpflichtet, vor der mittels Telefon-Banking zu erteilenden Bestätigung die Übereinstimmung der von der Bank telefonisch wiedergegebenen 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 die gesondert mitgeteilten Kontaktdaten abgeben.

(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 Konto-/Depotinhaber 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 Nr. 8.1

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

### 9.2 Sperre auf Veranlassung der Bank

- (1) Die Bank darf den Telefon-Banking-Zugang für einen Teilnehmer sperren, wenn
  - sie berechtigt ist, den Telefon-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 den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

### 9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber unverzüglich.

## 10. Haftung

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

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

### 10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

#### 10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

- (1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 EUR, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigen 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 abhanden gekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 EUR, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der Personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.
- (3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 EUR nach Abs. 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- (4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nr. 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.
- (5) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere 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 (siehe Nr. 8.1 Abs. 1),
  - das Personalisierte Sicherheitsmerkmal elektronisch gespeichert hat (siehe Nr. 7.1 Abs. 2 1. Spiegelstrich),
  - das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nr. 7.1 Abs. 1 2. Spiegelstrich),
  - das Personalisierte Sicherheitsmerkmal außerhalb des Telefon-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nr. 7.1 Abs. 2 3. Spiegelstrich).
- (6) 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 des Depotinhabers bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstruments oder

auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften der Depotinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

### 10.2.3 Haftung der Bank ab der Sperranzeige

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

### 10.2.4 Haftungsausschluss

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

Stand: Oktober 2009