



# PSD GiroDirekt

Umstellung auf ein Gehaltskonto



Hier ist günstig sicher.

Kontonummer

Hinweis: Bitte deutlich und in Druckschrift schreiben. Gerasterte Felder bitte freilassen.

## Antwort

PSD Bank München eG  
Sitz Augsburg  
86135 Augsburg

### 1. Kontoinhaber

Frau  Herr

Name, Vorname

Straße, Nummer

PLZ, Ort

Geburtsdatum

Familienstand

Telefon privat

Telefon geschäftlich

E-Mail

Bitte senden Sie mir den PSD Newsletter per E-Mail zu.

### Gehaltskonto – Umstellung

Ich/Wir möchten das o. g. PSD GiroDirekt künftig als Gehaltskonto nutzen.

Der erste Gehaltseingang erfolgt voraussichtlich am   
Tag/Monat/Jahr

### Kartenbestellung PSD BankCard

Ich beantrage die Ausstellung einer PSD BankCard und die Ausgabe einer persönlichen Geheimzahl für den von der Bank bestimmten Gültigkeitszeitraum.

Karteninhaber

Auf dem Chip meiner BankCard soll das Geburtsdatum verschlüsselt – also für Dritte nicht lesbar – angebracht werden. Dadurch ist es mir möglich, mich beispielsweise an Automaten die eine Alterserkennung prüfen, zu legitimieren, um die angebotene Ware zu erwerben.

Ich bin einverstanden  Ich möchte diese Funktion nicht nutzen

### Sonstige Bedingungen

Für das Vertragsverhältnis gelten ergänzend die Allgemeinen Geschäftsbedingungen (AGB-Banken) der Bank und deren Sonderbedingungen für den Überweisungsverkehr, den Lastschriftverkehr, die PSD BankCard, das PSD OnlineBanking, die PSD PostBox und für das TelefonBanking (PSD ServiceDirekt). Die AGB und die Sonderbedingungen erkenne ich an. Die Bedingungen können jederzeit in den Geschäftsräumen der Bank oder unter [www.psd-muenchen.de](http://www.psd-muenchen.de) eingesehen werden; auf Wunsch werden diese zugesandt.

### Schufa-Klausel – freiwillig –

Ich willige ein, dass die PSD Bank München eG, Sitz Augsburg (nachfolgend „PSD Bank“ genannt) der SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden, Daten über die Beantragung, die Durchführung und Beendigung dieser Kontoverbindung übermittelt.

Unabhängig davon wird die PSD Bank der SCHUFA auch Daten über ihre gegen mich bestehenden fälligen Forderungen übermitteln. Dies ist nach dem Bundesdatenschutzgesetz (§ 28a Absatz 1 Satz 1) zulässig, wenn ich die geschuldete Leistung trotz Fälligkeit nicht erbracht habe, die Übermittlung zur Wahrung berechtigter Interessen der PSD Bank oder Dritter erforderlich ist und

– Die Forderung vollstreckbar ist oder ich die Forderung ausdrücklich anerkannt habe oder

– Ich nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden bin, die PSD Bank mich rechtzeitig, jedoch frühestens bei der ersten Mahnung, über die bevorstehende Übermittlung nach mindestens vier Wochen unterrichtet hat und ich die Forderung nicht bestritten habe oder

– Das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen von der PSD Bank fristlos gekündigt werden kann und die PSD Bank mich über die bevorstehende Übermittlung unterrichtet hat

Darüber hinaus wird die PSD Bank der SCHUFA auch Daten über sonstiges nichtvertragsgemäßes Verhalten (Konten- oder Kreditkartenmissbrauch oder sonstiges betrügerisches Verhalten) übermitteln. Diese Meldungen dürfen nach dem Bundesdatenschutzgesetz (§ 28 Absatz 2) nur erfolgen, soweit dies zur Wahrung berechtigter Interessen des Kreditinstitutes oder Dritter erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung überwiegt.

Insofern befreie ich die PSD Bank zugleich vom Bankgeheimnis.

Die SCHUFA speichert und nutzt die erhaltenen Daten. Die Nutzung umfasst auch die Errechnung eines Wahrscheinlichkeitswertes auf Grundlage des SCHUFA-Datenbestandes zur Beurteilung des Kreditrisikos (Score). Die erhaltenen Daten übermitteln sie an Ihre Vertragspartner im Europäischen Wirtschaftsraum und der Schweiz, um diesen Informationen zur Beurteilung der Kreditwürdigkeit von natürlichen Personen zu geben. Vertragspartner der SCHUFA sind Unternehmen, die aufgrund von Leistungen oder Lieferung finanzielle Ausfallrisiken tragen (insbesondere Kreditinstitute sowie Kreditkarten- und Leasinggesellschaften, aber auch etwa Vermietungs-, Handels-, Telekommunikations-, Energieversorgungs-, Versicherungs- und Inkassounternehmen). Die SCHUFA stellt personenbezogene Daten nur zur Verfügung, wenn ein berechtigtes Interesse hieran im Einzelfall glaubhaft dargelegt wurde und die Übermittlung nach Abwägen aller Interessen zulässig ist. Daher kann der Umfang der jeweils zur Verfügung gestellten Daten nach der Art der Vertragspartner unterschiedlich sein. Darüber hinaus nutzt die SCHUFA die Daten zur Prüfung der Identität und des Alters von Personen auf Anfrage ihrer Vertragspartner, die beispielsweise Dienstleistungen im Internet anbieten.

Ich kann Auskunft bei der SCHUFA über die mich betreffenden gespeicherten Daten erhalten. Weiter Informationen über das SCHUFA-Auskunfts- und Score-Verfahren sind unter [www.meineschufa.de](http://www.meineschufa.de) abrufbar. Die postalische Adresse der SCHUFA lautet: SCHUFA Holding AG, Verbraucherservice, Postfach 5640, 30056 Hannover.

Ort, Datum  Unterschrift des Kontoinhabers (bei Minderjährigen auch Unterschrift beider gesetzl. Vertreter)  
– gilt als Unterschriftsprobe – bitte auf allen Formularen und Karten so unterschreiben



[www.psd-muenchen.de](http://www.psd-muenchen.de)

Kundennummer

**Hinweis:** Bitte deutlich und in Druckschrift schreiben. Gerasterte Felder bitte freilassen.

Antwort

PSD Bank München eG  
Sitz Augsburg  
86135 Augsburg

Kontoinhaber	
<input type="checkbox"/> Frau	<input type="checkbox"/> Herr
<input type="text"/>	
Name, Vorname	
<input type="text"/>	
Straße, Nummer	
<input type="text"/>	
PLZ, Ort	
<input type="text"/>	<input type="text"/>
Telefon privat	Telefon geschäftlich
<input type="text"/>	
E-Mail	
<input type="checkbox"/> Bitte senden Sie mir den PSD Newsletter per E-Mail zu.	

### Vereinbarung über PSD OnlineBanking

- Ich möchte am PSD OnlineBanking teilnehmen. Die Zugangsdaten sowie den PSD Key erhalte ich mit separater Post. Verfügungen über PSD OnlineBanking sind begrenzt auf 10.000 Euro täglich.
- Meine Teilnahme erfolgt über das kostenlose mobileTAN-Verfahren
- Meine deutsche Handynummer lautet:
- Meine Teilnahme erfolgt über das Sm@rt-TAN-plus-Verfahren (Voraussetzung PSD GiroDirekt und PSD BankCard). Den nötigen TAN-Generator Version 1.4 besitze ich bereits bzw. werde ich über die Internetseite [www.psd-bank.de/shop](http://www.psd-bank.de/shop) bestellen. Nach Erhalt des PSD Key und der PIN werde ich mich für das Verfahren im PSD OnlineBanking aktivieren.
- Ich möchte zusätzlich zum PSD OnlineBanking die PSD PostBox nutzen. Die PSD Bank wird Dokumente und Informationen (z.B. Kontoauszüge und Wertpapierordermitteilungen) für den Kontoinhaber elektronisch innerhalb der PSD PostBox bereitstellen. Mit der Bereitstellung der Dokumente und Informationen in der PSD PostBox gelten diese als zugegangen. Eine zusätzliche papierhafte Versendung erfolgt grundsätzlich nicht.

Für den Zugang zu einem Depot ist zusätzlich der Rahmenvertrag über die Nutzung des PSD OnlineBrokerage bzw. der PSD PostBox für Wertpapierordermitteilungen erforderlich.

### Vereinbarung über TelefonBanking (PSD ServiceDirekt)

- Ich möchte am PSD ServiceDirekt teilnehmen. Die PIN für die telefonische Auftragserteilung erhalte ich mit separater Post. Der Nutzer ist mit der Weitergabe seiner persönlichen Daten an die Service GmbH der PSD Banken einverstanden, damit eine Nutzung des PSD ServiceDirekt möglich ist.
- Der persönliche Verfügungsrahmen bei Aufträgen vom PSD GiroDirekt auf das unten genannte Referenzkonto beträgt 25.000 Euro, auf eine andere Bankverbindung beträgt der Rahmen 5.000 Euro.

### Allgemeines

Beide Vereinbarungen gelten zu allen unter der o.a. Kundennummer gegenwärtig und zukünftig geführten Konten und Depots, inklusive aller Konten und Depots, für die eine Mitkontoinhaberschaft besteht. Dieser Zugang kann auch für alle Konten und Depots für die eine Vollmacht besteht und zukünftig eingerichtet wird genutzt werden.

### Sonstige Bedingungen

Für das Vertragsverhältnis gelten die Allgemeinen Geschäftsbedingungen (AGB-Banken) sowie die Sonderbedingungen für PSD OnlineBanking, die PSD PostBox und das TelefonBanking (PSD ServiceDirekt). Die AGB und die Sonderbedingungen erkenne ich an. Der Wortlaut der o.g. Bedingungen, können im Internet unter [www.psd-muenchen.de](http://www.psd-muenchen.de) und in den Geschäftsräumen der PSD Bank eingesehen werden. Auf Wunsch werden diese zugesandt.

### Externe Bankverbindung (Referenzkonto)

Meine verbindliche Girokontonummer (Referenzbankverbindung) lautet:

\_\_\_\_\_

Kontonummer/IBAN                      Bankleitzahl/BIC                      Bank

\_\_\_\_\_

Kontoinhaber (ggf. vom Kunden abweichender Kontoinhaber,                                            Unterschrift Kontoinhaber (falls nicht identisch mit PSD Bank-Kunde)

Bis auf Widerruf bevollmächtigt der Kunde die PSD Bank, über PSD OnlineBanking oder PSD ServiceDirekt erteilte Aufträge vom Referenzkonto mit Einziehungsauftrag abzubuchen oder diesem gutzuschreiben. Falls das Referenzkonto keine Deckung aufweist, besteht keine Einlöschungspflicht. Die ggf. durch Rückbelastung entstehenden Kosten sind vom Kunden zu tragen.

Die Referenzbankverbindung bezieht sich auf die o.g. Kundennummer, nicht jedoch auf Kundennummern, für die lediglich eine Vollmacht besteht.

**Überweisungen aus Sparkonten sind bei allen Zugängen nur auf das angegebene Referenzkonto möglich.**

Eine Änderung der Referenzbankverbindung ist schriftlich durch den Kontoinhaber bzw. bei Oder-Konten durch einen der beiden Kontoinhaber möglich.

\_\_\_\_\_

Ort, Datum                                            Unterschrift des Antragstellers/ der/des gesetzlichen Vertreter(s)

## Sonderbedingungen für das PSD OnlineBanking

Stand: 10/2009

### 1. Leistungsangebot

- (1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels OnlineBanking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels OnlineBanking 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 OnlineBanking gelten die mit der Bank gesondert vereinbarten Verfügungsmitel. Eine Änderung dieser Mitel kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

### 2. Voraussetzungen zur Nutzung des OnlineBanking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels OnlineBanking 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).

#### 2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind:

- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN),
- der Nutzungscode für die elektronische Signatur.

#### 2.2 Authentifizierungsinstrumente

Die TAN bzw. die elektronische Signatur können dem Teilnehmer auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:

- auf einer Liste mit einmal verwendbaren TAN,
- mittels eines TAN-Generators, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist,
- mittels eines mobilen Endgerätes (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
- auf einer Chipkarte mit Signaturfunktion oder
- auf einem sonstigen Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden.

Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

### 3. Zugang zum OnlineBanking

Der Teilnehmer erhält Zugang zum OnlineBanking, wenn

- der Teilnehmer die Kontonummer oder seine individuelle Kundenkennung (PSD-Key oder Alias) und seine PIN oder elektronische Signatur übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (vgl. Nummer 7.1 und 8) vorliegt.

Nach Gewährung des Zugangs zum OnlineBanking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

### 4. OnlineBanking-Aufträge

#### 4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss OnlineBanking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (TAN oder elektronische Signatur) autorisieren und der Bank mittels OnlineBanking übermitteln. Die Bank bestätigt mittels OnlineBanking den Eingang des Auftrags.

#### 4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines OnlineBanking-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 OnlineBanking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im OnlineBanking ausdrücklich vor.

### 5. Bearbeitung von OnlineBanking-Aufträgen durch die Bank

- (1) Die Bearbeitung der OnlineBanking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der OnlineBanking-Seite der Bank oder im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der OnlineBanking-Seite der Bank angegebenen oder 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 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 (z. B. Wertpapierorder) liegt vor.
  - Das OnlineBanking-Datenformat ist eingehalten.

- Das gesondert vereinbarte OnlineBanking-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 OnlineBanking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.
- (3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den OnlineBanking-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 OnlineBanking zur Verfügung stellen.

### 6. Sorgfaltspflichten des Teilnehmers

#### 6.1 Technische Verbindung zum OnlineBanking

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

#### 6.2 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 OnlineBanking-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 OnlineBanking-Verfahren missbräuchlich nutzen.

- (2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:
  - Die Personalisierten Sicherheitsmerkmale dürfen nicht elektronisch gespeichert werden (z. B. im Kundensystem).
  - Bei Eingabe der Personalisierten Sicherheitsmerkmale ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
  - Die Personalisierten Sicherheitsmerkmale dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf Online-Händlerseiten).
  - Die Personalisierten Sicherheitsmerkmale dürfen nicht außerhalb des OnlineBanking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
  - Die PIN und der Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
  - Der Teilnehmer darf zur Autorisierung z. B. eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung einer neuen TAN-Liste nicht mehr als eine TAN verwenden.
  - Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht für das OnlineBanking genutzt werden.

#### 6.3 Sicherheit des Kundensystems

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

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

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

### 7. Anzeige- und Unterrichtungspflichten

#### 7.1 Sperranzeige

- (1) Stellt der Teilnehmer den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seiner persönlichen Sicherheitsmerkmale fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über eine gesondert mitgeteilte Telefonnummer 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 seiner Personalisierten Sicherheitsmerkmale erlangt hat oder
  - das Authentifizierungsinstrument oder die Personalisierten Sicherheitsmerkmale verwendet, muss er ebenfalls eine Sperranzeige abgeben.

## 7.2 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.

## 8. Nutzungssperre

### 8.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 7.1,

- den OnlineBanking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument.

### 8.2 Sperre auf Veranlassung der Bank

- (1) Die Bank darf den OnlineBanking-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, den OnlineBanking-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.

### 8.3 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 Konto-/Depotinhaber.

### 8.4 Automatische Sperre eines chip-basierten Authentifizierungsinstruments

- (1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn der Nutzungscodes für die elektronische Signatur dreimal in Folge falsch eingegeben wird.
- (2) Ein TAN-Generator, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.
- (3) Die in den Absätzen 1 und 2 genannten Authentifizierungsinstrumente können dann nicht mehr für das OnlineBanking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des OnlineBanking wiederherzustellen.

## 9. Haftung

### 9.1 Haftung der Bank bei nicht autorisierten und nicht oder fehlerhaft ausgeführten OnlineBanking-Verfügungen

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

### 9.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

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

- (1) Beruhen ein nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen oder sonst abhanden gekommenen 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 oder Diebstahl des Authentifizierungsinstruments ein Verschulden trifft.
- (2) Kommt es vor der Sperranzeige zu einem nicht autorisierten Zahlungsvorgang aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen oder gestohlen worden ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Teilneh-

mer 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 Zahlungen über die Haftungsgrenze von 150 Euro nach Absatz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen gehandelt hat.
- (4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 7.1 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 dann vorliegen, wenn er
- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmale der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (vgl. Nummer 7.1 Absatz 1),
  - die Personalisierten Sicherheitsmerkmale im Kundensystem gespeichert hat (vgl. Nummer 6.2 Absatz 2, 1. Spiegelstrich),
  - die Personalisierten Sicherheitsmerkmale einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde (vgl. Nummer 6.2 Absatz 1, 2. Spiegelstrich),
  - die Personalisierten Sicherheitsmerkmale erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (vgl. Nummer 6.2 Absatz 2, 3. Spiegelstrich),
  - die Personalisierten Sicherheitsmerkmale außerhalb des OnlineBanking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (vgl. Nummer 6.2 Absatz 2, 4. Spiegelstrich),
  - die Personalisierten Sicherheitsmerkmale auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (vgl. Nummer 6.2 Absatz 2, 5. Spiegelstrich),
  - mehr als eine TAN zur Autorisierung eines Auftrags verwendet (vgl. Nummer 6.2 Absatz 2, 6. Spiegelstrich),
  - beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das OnlineBanking nutzt (vgl. Nummer 6.2 Absatz 2, 7. Spiegelstrich).
- (6) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

### 9.2.2 Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhend 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 Kontoinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

### 9.2.3 Haftung der Bank ab der Sperranzeige

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

### 9.2.4 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.

**10. 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- oder Beschwerdestellen wenden.

### 11. Hinweis nach § 13 Abs. 1 TMG (Telemediengesetz)

Alle im Rahmen des OnlineBanking anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und gegebenenfalls dem von ihr beauftragten Rechenzentrum innerhalb Deutschlands bzw. der Europäischen Union verarbeitet.

## Sonderbedingungen für die Nutzung der PSD PostBox

Stand: 10/2009

### 1. Die PSD PostBox

Die Bank bietet dem Kunden die Möglichkeit eines Zugangs zu seinen bei der Bank geführten Konten und Depots über das Internet. Im Rahmen der Geschäftsbeziehung zwischen der Bank und dem Kunden, der für die Nutzung der PSD PostBox freigeschaltet ist, gilt die PSD PostBox als Kommunikationsweg, über den die Bank dem Kunden Dokumente und Mitteilungen (nachfolgend Informationen genannt), wie z. B. Kontoauszüge und Wertpapierabrechnungen in elektronischer Form bereitstellt. Die Bank ist berechtigt, den Leistungsumfang der PSD PostBox zu erweitern oder einzuschränken. Mit der Anmeldung zur PSD PostBox werden dem Kunden die Informationen in die PSD PostBox eingestellt.

### 2. Übermittlung der Kontodaten

Die Bank stellt dem Kunden darüber hinaus auch termingebundene Informationen, die den Geschäftsverkehr mit der Bank betreffen, elektronisch als Datei zur Verfügung; dies gilt auch für den Rechnungsabschluss sowie die Anlagen zu Kontoauszügen. Soweit den Kunden hinsichtlich der bislang papierhaft übersandten Informationen Verpflichtungen treffen, bestehen diese in gleicher Weise für die in den Posteingang übermittelten Informationen.

Der Kunde ist verpflichtet, regelmäßig und zeitnah die Informationen im Posteingang abzurufen und die Inhalte zu prüfen. Er hat der Bank eventuelle Unstimmigkeiten unverzüglich anzuzeigen. Es gelten insbesondere die Nr. 7.2 sowie Nr. 11.4 und Nr. 11.5 der Allgemeinen Geschäftsbedingungen (AGB-Banken) und 2.4 der Sonderbedingungen für Zahlungen mittels Lastschrift im Einzugsermächtigungsverfahren.

### 3. Verzicht auf papierhafte Kontoauszüge

Die Bank kann ihre Informationsverpflichtungen aus der Geschäftsbeziehung dadurch erfüllen, dass sie Informationen elektronisch in den Posteingang übermittelt. Sie wird die Informationen, die sie im Posteingang bereitstellt, grundsätzlich nicht zusätzlich papierhaft versenden. Der Kunde verzichtet ausdrücklich auf den postalischen Versand dieser Informationen, wenn die entsprechenden Konten auf die PSD PostBox umgestellt sind. Die Bank ist berechtigt, Informationen aus der PSD PostBox, nach Ablauf von 15 Monaten, zu entfernen, ohne den Kunden hierüber gesondert zu informieren.

### 4. Zusendung von Kontoauszügen

Auf Verlangen des Kunden wird die Bank dem Kunden Informationen kostenpflichtig zusenden. Unabhängig davon ist die Bank gleichwohl berechtigt, Informationen auf dem Postweg oder in sonstiger Weise an den Kunden zu senden, wenn sie dieses unter Berücksichtigung des Kundeninteresses für zweckmäßig hält. Die Entgelte für die Zusendung auf dem postalischem Weg ergeben sich aus dem „Preis- und Leistungsverzeichnis“.

### 5. Zugang

Soweit der Kunde die Informationen nicht bereits vorher abgerufen hat, gelten diese am Tag nach der Bereitstellung als zugegangen.

### 6. Kündigung

Der Kunde kann die Nutzung der PSD PostBox jederzeit schriftlich ohne Einhaltung einer Frist kündigen. Die Bank kann die Nutzung der PSD PostBox jederzeit mit einer Frist von 2 Monaten kündigen, es sei denn, es liegt ein wichtiger Grund vor, der sie zu einer außerordentlichen Kündigung berechtigen würde. Ein wichtiger Grund liegt insbesondere dann vor, wenn es der Bank auch unter angemessener Berücksichtigung der Belange des Kunden unzumutbar erscheint, den elektronischen PSD PostBox-Dienst fortzusetzen.

Die Bank wird nach dem Wirksamwerden einer Kündigung alle Informationen im Rahmen der Geschäftsbeziehung per Post an die vom Kunden angegebene Anschrift versenden. Im Falle einer fristlosen Kündigung durch den Kunden kann dieses jedoch erst nach einer angemessenen Bearbeitungszeit erfolgen. Die Bank ist nicht verpflichtet, dem Kunden die im Zeitpunkt des Wirksamwerdens der Kündigung im Posteingang befindlichen Informationen nachträglich postalisch zuzusenden. Die Entgelte ergeben sich aus dem „Preis- und Leistungsverzeichnis“.

### 7. Anerkennung durch Finanzbehörden

Der elektronische Kontoauszug bzw. Rechnungsabschluss erfüllt nach Auffassung der Finanzverwaltung weder die Anforderungen der steuerlichen Aufbewahrungspflicht nach § 147 AO noch die einer Rechnung im Sinne des Umsatzsteuergesetzes. Er wird daher nur im Privatkundenbereich und damit für den Kontoinhaber anerkannt, der nicht buchführungs- und aufzeichnungspflichtig im Sinne der §§ 145 ff. AO ist.

Die Bank gewährleistet nicht, dass die Steuer- oder Finanzbehörden die im Posteingang gespeicherten Informationen anerkennen. Der Kunde hat sich darüber vorher bei dem für ihn zuständigen Finanzamt zu informieren. Die Informationen können nach ihrer Übermittlung in den Posteingang nicht verändert werden. Die Bank garantiert die Unveränderbarkeit der in der PSD PostBox bereit gestellten Daten. Diese Garantie gilt jedoch nicht, sofern die Daten außerhalb der PSD PostBox gespeichert oder aufbewahrt werden. Dabei ist zu beachten, dass ein Ausdruck eines Dokuments aufgrund der individuellen Hard- oder Softwareeinstellung von der Darstellung am Bildschirm abweichen kann. Soweit die Dokumente verändert werden oder in veränderter Form in Umlauf gebracht werden, haftet die Bank hierfür nicht.

## Sonderbedingungen für das TelefonBanking (PSD ServiceDirekt)

Stand: 10/2009

### 1. Leistungsangebot

(1) Der Konto-/Depotinhaber kann Bankgeschäfte im Rahmen des TelefonBanking mittels Telefon in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels TelefonBanking abrufen. Die Abwicklung mittels Telefon umfasst insbesondere Geschäftsvorfälle in den Bereichen

- Kontoführung
- Zahlungsverkehr
- Karten und Kartensperre
- Einlagen
- Information über Kontostände und Umsätze
- Produktanlagen (Neu- und Wiederanlagen)
- Unterstützung bei Fragen zum OnlineBanking (z. B. Trojaner-Meldungen, externe BankingSoftware)
- Entgegennahme neuer Vereinbarungen bzw. Änderungen für den telefonischen und elektronischen Vertriebsweg
- allgemeine Informationen und Serviceangebote
- aktive Kundenansprache zu Produkten und Serviceangeboten

Weiterhin kann der Kunde folgende, an deutschen Börsen handelbare Wertpapiere kaufen und verkaufen:

- Aktien
- Renten
- Investmentfonds
- Zeichnung von Neuemissionen

Die im TelefonBanking erteilten Wertpapieraufträge werden ohne Beratung durchgeführt. Die Bank setzt voraus, dass der Kunde genaue Vorstellungen über Art und Umfang der von ihm gewünschten Wertpapiergeschäfte hat und deren Risiken einschätzen kann.

Der Kunde ist verpflichtet, die Wertpapierkennnummer und Wertpapierbezeichnung anzugeben. Bei einer Abweichung von Wertpapierkennnummer und Wertpapierbezeichnung wird das Geschäft nicht ausgeführt.

Die Berechtigung zur Erteilung von Wertpapieraufträgen in TelefonBanking bedarf in der Regel einer separaten Vereinbarung inkl. Informationen über die Kenntnisse im Wertpapiergeschäft.

- (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 TelefonBanking gelten die mit der Bank gesondert vereinbarten Verfügungsmitte. Eine Änderung dieser Mitte kann der Teilnehmer mit seiner Bank gesondert vereinbaren.
- (4) Die Bank ist berechtigt, den Leistungsumfang von TelefonBanking zu erweitern oder einzuschränken. Weiterhin ist sie berechtigt, TelefonBanking unter Einhaltung einer angemessenen Frist einzustellen.

### 2. Voraussetzungen zur Nutzung des TelefonBanking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels TelefonBanking das mit der Bank vereinbarte Personalisierte Sicherheitsmerkmal, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen und Aufträge zu autorisieren (vgl. Nummern 3 und 4.1).

Als Personalisiertes Sicherheitsmerkmal im Rahmen von TelefonBanking dient entweder eine persönliche Identifikationsnummer (PIN) oder ein persönliches Codewort. Die Bank legt fest, welches Personalisierte Sicherheitsmerkmal für TelefonBanking eingesetzt wird.

### 3. Zugang zum TelefonBanking

Der Teilnehmer erhält Zugang zum TelefonBanking mittels Telefon, wenn

- der Teilnehmer die Kunden-/Kontonummer oder seine individuelle Kundenkennung (PSD Key oder Alias) nennt und seine PIN über die Tastatur des Telefons eingegeben hat bzw. sich mit seinem persönlichen Codewort legitimiert hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (vgl. Nummer 8) vorliegt.

Nach Gewährung des Zugangs zum TelefonBanking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

Die Bank darf sich zur Durchführung von TelefonBanking-Geschäften eines Erfüllungsgehilfen bedienen, der die technische Abwicklung für die Bank durch eine zentrale Auftragsannahme vornimmt. Dieser Erfüllungsgehilfe ist berechtigt, im Rahmen der Abwicklung der Aufträge Einsicht in Kundenkonten und Kundendepots zu nehmen.

### 4. TelefonBanking-Aufträge

#### 4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss TelefonBanking-Aufträge (z.B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (PIN bzw. Codewort) autorisieren. Der Auftrag wird am Telefon bestätigt.

#### 4.2 Widerruf von TelefonBanking-Aufträgen

Die Widerrufbarkeit eines TelefonBanking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr).

#### 5. Bearbeitung von TelefonBanking-Aufträgen durch die Bank

(1) Die Bearbeitung der TelefonBanking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf den 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 darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

(2) Der Auftrag wird ausgeführt, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat sich mit dem Personalisierten Sicherheitsmerkmal autorisiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z.B. Wertpapierorder) liegt vor.
- Das gesondert vereinbarte TelefonBanking-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 Absatz 2 Satz 1 vor, führt die Bank die TelefonBanking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den TelefonBanking-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, fernmündlich oder schriftlich zur Verfügung stellen.

### 6. Sorgfaltspflichten des Teilnehmers

#### 6.1 Geheimhaltung des Personalisierten Sicherheitsmerkmals

(1) Der Teilnehmer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN / dem persönlichen Codewort erlangt. Denn jede andere Person, die im Besitz der PIN / des persönlichen Codewortes ist, hat die Möglichkeit, das TelefonBanking zu nutzen. Sie kann z. B. Aufträge zu Lasten des Kontos erteilen.

(2) Insbesondere ist Folgendes zum Schutz der PIN / des persönlichen Codewortes zu beachten:

- Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (z. B. im Kundensystem).
- Bei Eingabe bzw. Übermittlung des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen bzw. mithören können.
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des TelefonBanking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.

Verwendet der Teilnehmer ein Telefon mit Nummernspeicher und Wahlwiederholungsfunktion, ist er verpflichtet, nach Beendigung des Telefonats mit der Bank den Speicherinhalt zu überspielen (z. B. durch Eingabe einer beliebigen Nummer über die Tastatur). Dadurch wird verhindert, dass ein Dritter durch Nutzung der Wahlwiederholungsfunktion Kenntnis von der zuvor eingegebenen PIN erhält und hierdurch ein missbräuchlicher Zugang zum TelefonBanking ermöglicht wird.

#### 6.2 Änderung des Personalisierten Sicherheitsmerkmals

Der Teilnehmer ist verpflichtet, bei erstmaliger Nutzung seine PIN zu ändern. Darüber hinaus ist der Teilnehmer jederzeit berechtigt, seine PIN zu ändern. Das persönliche Codewort kann durch den Teilnehmer jederzeit geändert werden. Die Änderung hat grundsätzlich schriftlich gegenüber der Bank zu erfolgen und gilt ab dem Datum des Zugangs bei der Bank.

#### 6.3 Kontrolle der Auftragsdaten mit von der Bank mitgeteilten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem TelefonBanking-Auftrag (z.B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) telefonisch wiederholt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der mitgeteilten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

## 7. Anzeige- und Unterrichtungspflichten

### 7.1 Sperranzeige

(1) Stellt der Teilnehmer fest oder hat er den Verdacht, dass eine andere Person von seiner PIN Kenntnis erhalten hat, ist der Teilnehmer verpflichtet, unverzüglich seine PIN zu ändern. Sofern ihm dies nicht möglich ist, hat er die Bank unverzüglich zu unterrichten. In diesem Fall wird die Bank den Telefonzugang zum TelefonBanking sperren.

Stellt der Teilnehmer fest oder hat er den Verdacht, dass eine andere Person von seinem persönlichen Codewort Kenntnis erhalten hat, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Zudem ist der Teilnehmer verpflichtet, schriftlich die Änderung seines persönlichen Codewortes über die Bank zu beantragen (Änderung gilt ab dem Datum des Zugangs bei der Bank).

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

### 7.2 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.

## 8. Nutzungssperre

### 8.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 7.1, den TelefonBanking-Zugang für ihn oder alle Teilnehmer.

### 8.2 Sperre auf Veranlassung der Bank

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

- sie berechtigt ist, den TelefonBanking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der PIN / des persönlichen Codewortes dies rechtfertigen, oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung der PIN / des persönlichen Codewortes besteht.

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

### 8.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder dem Teilnehmer eine neue PIN zusenden / den Teilnehmer auffordern, ihr schriftlich ein neues persönliches Codewort mitzuteilen, wenn die Gründe für die Sperre nicht mehr gegeben sind.

### 8.4 Automatische Sperre der PIN

Das System sperrt die PIN automatisch, wenn der Teilnehmer dreimal hintereinander eine falsche PIN eingibt. Auf Anforderung erhält der Teilnehmer eine neue PIN zugesandt.

## 9. Haftung

### 9.1 Haftung der Bank bei nicht autorisierten und nicht oder fehlerhaft ausgeführten TelefonBanking-Verfügungen

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

### 9.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seiner PIN/ seines persönlichen Codewortes

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

(1) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung der PIN / des persönlichen Codewortes, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der PIN bzw. des Codewortes schuldhaft verletzt hat.

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

(3) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 6.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(4) Kommt es 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 dann vorliegen, wenn er

- den Verlust oder Diebstahl der PIN / des persönlichen Codewortes oder die missbräuchliche Nutzung der PIN / des persönlichen Codewortes (insbesondere durch Verletzung seiner Sorgfaltspflichten) der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (vgl. Nummer 7.1),
- die PIN im Telefon mit Nummernspeicher und Wahlwiederholungsfunktion oder anderweitig gespeichert hat (vgl. Nummer 6.1 Absatz 2, 1. Spiegelstrich und Satz 2),
- das Personalisierte Sicherheitsmerkmal (PIN bzw. das persönliche Codewort) einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde (vgl. Nummer 6.1 Absatz 1 und Absatz 2, 2. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal außerhalb des ServiceDirekt-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (vgl. Nummer 6.1 Absatz 2, 3. Spiegelstrich).

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

#### 9.2.2 Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhend nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung einer verlorengegangenen oder gestohlenen PIN / eines verlorengegangenen oder gestohlenen persönlichen Codewortes oder sonstigen missbräuchlichen Nutzung der PIN / des persönlichen Codewortes und ist der Bank hierdurch ein Schaden entstanden, haften der Kontoinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

#### 9.2.3 Haftung der Bank ab der Sperranzeige

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

#### 9.2.4 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.

## 10. Telefonaufzeichnung

Der Teilnehmer ist damit einverstanden, dass die Bank die im Rahmen des TelefonBanking geführten Telefonate sowie die von ihm über die Tastatur des Telefons eingegebenen Ziffern (ausgenommen PIN) aufzeichnet und aufbewahrt. Dies ist zur ordnungsgemäßen Auftragsbearbeitung und aus Beweisgründen erforderlich.

## 11. 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- oder Beschwerdestellen wenden.