

PSD Bank Kiel eG

Kundennummer \_\_\_\_\_

MH: \_\_\_\_\_ B: \_\_\_\_\_ I: \_\_\_\_\_ A: \_\_\_\_\_ IQ: \_\_\_\_\_ VK: \_\_\_\_\_  
wird von der PSD Bank ausgefüllt

Antwort

PSD Bank Kiel eG  
Kehdenstr. 12 - 16  
24103 Kiel

**Kontoinhaber**  Frau  Herr  Eheleute

\_\_\_\_\_  
Vorname(n), Name

\_\_\_\_\_  
Straße, Nr.

\_\_\_\_\_  
PLZ, Ort

\_\_\_\_\_  
Telefon tagsüber für Rückfragen

\_\_\_\_\_  
E-Mail

## PSD OnlineBanking / PSD ServiceDirekt (TelefonBanking)

Zwischen dem nachfolgenden Bevollmächtigten, im Folgenden als „Teilnehmer“ bezeichnet, sowie der PSD Bank wird Folgendes vereinbart:

Bevollmächtigter <sup>1</sup> \_\_\_\_\_  
Name, Vorname, Geburtsdatum, Kundennummer

**PSD OnlineBanking** inkl. elektronischem Postfach <sup>2</sup>

**PSD ServiceDirekt (TelefonBanking)**

mit Sm@rt-TAN-plus-Verfahren <sup>3</sup>

mit SecureGo-Verfahren <sup>4</sup>

Der Teilnehmer erhält Zugang zu allen unter der im Kopf angegebenen Kundennummer gegenwärtig und zukünftig geführten Konten in dem von der PSD Bank angebotenen Umfang. Das Verfügungslimit im PSD OnlineBanking beträgt zurzeit 15.000 EUR pro Tag, im PSD ServiceDirekt (TelefonBanking) 15.000 EUR pro Tag. Eine Änderung des Verfügungslimits ist nur in Textform durch den Kontoinhaber, bei Gemeinschaftskonten mit Einzelverfügungsbefugnis durch einen der Kontoinhaber, möglich.

<sup>1</sup> Für den Bevollmächtigten muss eine Vollmacht zu Lebzeiten und über den Tod hinaus vorliegen oder auf besonderem Formular erteilt werden.

<sup>2</sup> Die Nutzung des elektronischen Postfachs ist dem Bevollmächtigten gestattet, wenn die Nutzung auch dem/den Kontoinhaber(n) selbst möglich ist.

<sup>3</sup> Der erforderliche TAN-Generator kann über die Internetseite [www.psd-bank.de/Online-Shop](http://www.psd-bank.de/Online-Shop) bestellt werden. Die Nutzung setzt eine girocard (Debitkarte) voraus.

<sup>4</sup> Die erforderliche Smartphone-App für Android bzw. iOS ist im App-Store erhältlich.

## Telefonaufzeichnung

Der Teilnehmer willigt ein, dass die Bank die mit ihm im Rahmen des PSD ServiceDirekt geführten Telefonate sowie die von ihm über die Tastatur des Telefons eingegebenen Ziffern (ausgenommen PIN) aufzeichnet und solange aufbewahrt, wie dies zur ordnungsgemäßen Auftragsverarbeitung und aus Beweisgründen erforderlich ist.

## Bedingungen

Es gelten die Allgemeinen Geschäftsbedingungen der Bank sowie die Sonderbedingungen für das PSD OnlineBanking, für PSD ServiceDirekt (TelefonBanking) und die Nutzung des elektronischen Postfachs. Die Bedingungen können in den Geschäftsräumen der Bank oder unter [www.psd-kiel.de](http://www.psd-kiel.de) eingesehen werden. Auf Verlangen werden sie ausgehändigt.

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

 \_\_\_\_\_  
Unterschrift Teilnehmer

**(wird von der PSD Bank ausgefüllt)**

Die Unterschrift des Bevollmächtigten

wurde vor mir geleistet

wurde von mir geprüft

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

\_\_\_\_\_  
Mitarbeiter der Bank



## 1. Leistungsangebot

(1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels Online Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online Banking abrufen. Des Weiteren sind sie gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absätze 33 und 34 Zahlungsdienstenaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.

(2) Kunde und Bevollmächtigte werden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden einheitlich als „Konto“ bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

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

## 2. Voraussetzungen zur Nutzung des Online Banking

(1) Der Teilnehmer kann das Online Banking nutzen, wenn die Bank ihn authentifiziert hat.

(2) Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des Personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).

(3) Authentifizierungselemente sind

- Wissensselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer (PIN) oder der Nutzungscode für die elektronische Signatur) und
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern (TAN), die den Besitz des Teilnehmers nachweisen, wie die girocard mit TAN-Generator oder das mobile Endgerät), sowie
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

(4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissensselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.

## 3. Zugang zum Online Banking

(1) Der Teilnehmer erhält Zugang zum Online Banking der Bank, wenn

- er seine individuelle Teilnehmerkennung (z. B. Kontonummer, Anmeldename) angibt und
- er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9 dieser Bedingungen) vorliegt.

Nach Gewährung des Zugangs zum Online Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge erteilt werden.

(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z. B. zum Zweck der Änderung der Anschrift des Kunden) fordert die Bank den Teilnehmer auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Online Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kontoinhabers und die Kontonummer sind für den vom Teilnehmer genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Zahlungsdaten (§ 1 Absatz 26 Satz 2 ZAG).

## 4. Aufträge

### 4.1 Auftragserteilung

Der Teilnehmer muss einem Auftrag (z. B. Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z. B. Eingabe einer TAN oder elektronische Signatur als Nachweis des Besitzelements) zu verwenden, sofern mit der Bank nichts anderes vereinbart wurde. Die Bank bestätigt mittels Online Banking den Eingang des Auftrags.

### 4.2 Widerruf von Aufträgen

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

## 5. Bearbeitung von Aufträgen durch die Bank

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

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

- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1 dieser Bedingungen).
- 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 (vgl. Nummer 1 Absatz 3 dieser Bedingungen).
- Die weiteren Ausführungsbedingungen 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 Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr, Sonderbedingungen für Wertpapiergeschäfte) aus.

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

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

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

## 7. Sorgfaltspflichten des Teilnehmers

### 7.1 Schutz der Authentifizierungselemente

(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vgl. Nummern 3 und 4 dieser Bedingungen).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

- (a) Wissensselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere
  - nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden,
  - nicht außerhalb des Online Banking in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden,
  - nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
  - nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Online Banking und Fingerabdrucksensor) dient.
- (b) Besitzelemente, wie z. B. die girocard mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
  - sind die girocard mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,

- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können,
  - ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für das Online Banking (z. B. Online Banking-App, Authentifizierungs-App) nicht nutzen können,
  - ist die Anwendung für das Online Banking (z. B. Online Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons),
  - dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und
  - muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das Online Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online Banking des Teilnehmers aktivieren.
- (c) Seinelemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinelemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online Banking genutzt wird, Seinelemente anderer Personen gespeichert, ist für das Online Banking das von der Bank ausgegebene Wissensselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinelement.

(3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (z. B. Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.

(4) Die für das mobileTAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Online Banking nicht mehr nutzt.

(5) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 4 darf der Teilnehmer seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden (siehe Nummer 1 Absatz 1 Sätze 3 und 4 dieser Bedingungen). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

## 7.2 Sicherheitshinweise der Bank

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

## 7.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (z. B. mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen. Bei Feststellung von Abweichungen ist die Transaktion abzubrechen.

## 8. Anzeige- und Unterrichtungspflichten

### 8.1 Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.

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

(3) Hat der Teilnehmer den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

### 8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

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

## 9. Nutzungssperre

### 9.1 Sperre auf Veranlassung des Teilnehmers

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

- den Online Banking-Zugang für ihn oder alle Teilnehmer oder
- seine Authentifizierungselemente zur Nutzung des Online Banking.

### 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 der Authentifizierungselemente des Teilnehmers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

### 9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

### 9.4 Automatische Sperre eines Chip-basierten Besitzelements

(1) Eine Chipkarte mit Signaturfunktion sperrt sich selbst, wenn der Nutzungscodes für die elektronische Signatur dreimal in Folge falsch eingegeben wird.

(2) Ein TAN-Generator als Bestandteil einer Chipkarte, 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 Besitzelemente können dann nicht mehr für das Online Banking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Online Banking wiederherzustellen.

### 9.5 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Kunden verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Bank wird den Kunden über eine solche Zugangsverweigerung auf dem vereinbarten Weg unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Bank die Zugangssperre auf. Hierüber unterrichtet sie den Kunden unverzüglich.

## 10. Haftung

### 10.1 Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Bank bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr, Sonderbedingungen für Wertpapiergeschäfte).

### 10.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

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

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn

- es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach

- Nummer 7.1 Absatz 2,
- Nummer 7.1 Absatz 4,
- Nummer 7.3 oder
- Nummer 8.1 Absatz 1

dieser Bedingungen verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Sein (siehe Nummer 2 Absatz 3 dieser Bedingungen).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

(6) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 dieser Bedingungen nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(8) Ist der Kunde kein Verbraucher, gilt ergänzend Folgendes:

- Der Kunde haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach Absätzen 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen verstoßen hat.
- Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

#### **10.2.2 Haftung des Kunden bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige**

Beruhend nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

#### **10.2.3 Haftung 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. 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 Streit-schlichtungs- oder Beschwerdestellen wenden.

## **Sonderbedingungen für die Nutzung des elektronischen Postfachs**

Stand: Juli 2017

### **1. Das elektronische Postfach**

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 des elektronischen Postfachs freigeschaltet ist, gilt das elektronische Postfach als Kommunikationsweg. Der Kunde kann das elektronische Postfach im bereitgestellten Funktionsumfang nutzen. Wenn der Bevollmächtigte Zugang zum Online Banking hat, ist ihm die Nutzung des elektronischen Postfachs in gleicher Weise wie dem Kontoinhaber bzw. den Kontoinhabern gestattet.

### **2. Übermittlung von Konto- und Kundendokumenten**

Bei Nutzung des elektronischen Postfachs werden dem Kunden sämtliche Konto- und Kundendokumente dort eingestellt. Dies umfasst beispielsweise Konto- und Depotauszüge, Rechnungsabschlüsse, Kreditkartenabrechnungen sowie Angebote zur Änderung der Allgemeinen Geschäftsbedingungen, Sonderbedingungen oder Entgelte.

### **3. Verzicht auf papierhafte Konto- und Kundendokumente**

Die Bank kann ihre Informationsverpflichtungen aus der Geschäftsbeziehung dadurch erfüllen, dass sie Informationen elektronisch in den Posteingang übersendet. Die Übersendung der Mitteilung erfolgt insbesondere durch Einstellung von Dateien im PDF-Format in das elektronische Postfach. Die Bank 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 das elektronische Postfach umgestellt sind. Die Bank bleibt dazu berechtigt, dem Kunden Dokumente per Post zuzusenden, wenn sie dies unter Berücksichtigung der Kundeninteressen für zweckmäßig hält oder es aus rechtlichen Gründen erforderlich ist.

### **4. Mitwirkungspflichten des Kunden**

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.

### **5. Kündigung**

Der Kunde kann die Nutzung des elektronischen Postfachs jederzeit in Textform ohne Einhaltung einer Frist kündigen. Die Bank kann die Nutzung des elektronischen Postfachs 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 Postfach-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“.

### **6. Anerkennung durch Finanzbehörden**

Kunden, die handels- und steuerrechtlichen Aufbewahrungspflichten unterliegen, sollten sich bei einem Angehörigen der steuerberatenden Berufe informieren, was im Fall des Bezugs von elektronischen Dokumenten (z. B. Kontoauszügen) zur Erfüllung dieser Pflichten zu beachten ist. Die Informationen können nach ihrer Übermittlung in den Posteingang nicht verändert werden. Die Bank garantiert die Unveränderbarkeit der in das elektronische Postfach bereit gestellten Daten. Diese Garantie gilt jedoch nicht, sofern die Daten außerhalb des elektronischen Postfachs 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.

## 1. Leistungsangebot

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

(2) Der Teilnehmer kann Bankgeschäfte im Rahmen von PSD ServiceDirekt mittels Telefon in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels PSD ServiceDirekt abrufen. Die im PSD ServiceDirekt erteilten Wertpapieraufträge werden ohne Beratung durchgeführt. Die Berechtigung zur Erteilung von Wertpapieraufträgen mittels PSD ServiceDirekt bedarf einer separaten Rahmenvereinbarung.

(3) Zur Nutzung von PSD ServiceDirekt gelten die mit der Bank gesondert vereinbarten Verfügungsmitel. Eine Änderung dieser Mitel kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

## 2. Voraussetzungen zur Nutzung von PSD ServiceDirekt

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels PSD ServiceDirekt die mit der Bank vereinbarte persönliche Identifikationsnummer (PIN), um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen und Aufträge zu autorisieren (vgl. Nummer 4.1).

## 3. Zugang zum PSD ServiceDirekt

Der Teilnehmer erhält Zugang zum PSD ServiceDirekt 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,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (vgl. Nummer 7) vorliegt.

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

Die Bank darf sich zur Durchführung von PSD ServiceDirekt-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 zu nehmen.

## 4. PSD ServiceDirekt-Aufträge

### 4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss PSD ServiceDirekt-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit der vereinbarten PIN autorisieren und der Bank mittels Telefon übermitteln. Der Auftrag wird am Telefon bestätigt.

### 4.2 Widerruf von PSD ServiceDirekt-Aufträgen

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

## 5. Bearbeitung von PSD ServiceDirekt-Aufträgen durch die Bank

(1) Die Bearbeitung der PSD ServiceDirekt-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 darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

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

- Der Teilnehmer hat sich mit seiner PIN legitimiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das gesondert vereinbarte PSD ServiceDirekt-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 PSD ServiceDirekt-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr, Sonderbedingungen für Wertpapiergeschäfte) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den PSD ServiceDirekt-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, eine Information zur Verfügung stellen.

## 6. Sorgfaltspflichten des Teilnehmers

### 6.1 Technische Verbindung zum PSD ServiceDirekt

Der Teilnehmer ist verpflichtet, die Verbindung zum PSD ServiceDirekt nur über die von der Bank gesondert mitgeteilten TelefonBanking-Telefonnummern herzustellen.

### 6.2 Geheimhaltung des Personalisierten Sicherheitsmerkmals

(1) Der Teilnehmer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN erlangt. Denn jede andere Person, die im Besitz der

PIN ist, hat die Möglichkeit, den PSD ServiceDirekt missbräuchlich zu nutzen.

(2) Insbesondere ist Folgendes zum Schutz der PIN zu beachten:

- Die Weitergabe der PIN an andere Personen ist nicht zulässig.
- Die im Telefonspeicher gespeicherte PIN ist zu löschen oder zu überschreiben, damit nachfolgende Nutzer des Geräts nicht diese ausspähen können.
- Die PIN darf nicht elektronisch gespeichert werden (z. B. im Kundensystem).
- Bei Eingabe bzw. Übermittlung der PIN ist sicherzustellen, dass andere Personen diese nicht ausspähen bzw. mithören können.
- Die PIN darf nicht außerhalb des PSD ServiceDirekt-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.

## 6.3 Änderung der PIN

Der Teilnehmer ist verpflichtet, bei erstmaliger Nutzung seine PIN zu ändern. Darüber hinaus ist der Teilnehmer jederzeit berechtigt, seine PIN zu ändern.

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

Soweit die Bank dem Teilnehmer Daten aus seinem PSD ServiceDirekt-Auftrag (z. B. Betrag, IBAN 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

- den Verlust oder Diebstahl der PIN,
- die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seiner PIN

fest oder hat er den Verdacht, dass eine andere Person von seiner PIN Kenntnis erhalten hat, ist der Teilnehmer verpflichtet, die Bank hierüber unverzüglich zu 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.

### 7.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Teilnehmer 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

8.1 Sperre auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 7.1, den PSD ServiceDirekt-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 PSD ServiceDirekt-Vertrag aus wichtigem Grund zu kündigen,
  - sachliche Gründe im Zusammenhang mit der Sicherheit der PIN dies rechtfertigen, oder
  - der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung der PIN besteht.

(2) Die Bank wird den Teilnehmer 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, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Teilnehmer unverzüglich.

### 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 PSD ServiceDirekt-Verfügungen

Die Haftung der Bank bei nicht autorisierten und nicht oder fehlerhaft ausgeführten PSD ServiceDirekt-Verfügungen richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr, Sonderbedingungen für Wertpapiergeschäfte).



