

# PSD OnlineBanking mit PSD PostBox

Hier ist günstig sicher

Kundennummer Antwort

PSD Bank Koblenz eG  
Casinostraße 51  
56068 Koblenz

**Kontoinhaber**
 Frau  Herr  Eheleute

Name, Vorname

Straße, Nummer

PLZ, Ort

Telefon privat

Telefon geschäftlich

E-Mail

**Ich möchte im OnlineBanking folgendes Verfahren nutzen:** MobileTAN-Verfahren (TAN per SMS) Sm@rt-TAN-plus-Verfahrenmeine Mobilfunknummer/Änderung der Mobilfunknummer: **Teilnehmer/Bevollmächtigter**

Folgende Kontoinhaber bzw. Verfügungsberechtigte (Bevollmächtigte, gesetzliche Vertreter) sollen zu allen gegenwärtig und zukünftig geführten Konten und Depots unter der o. a. Kundennummer per PSD ServiceDirekt (Telefon-Banking) bzw. PSD OnlineBanking in dem von der Bank angebotenen Umfang (Bedingungen siehe Folgeblätter) Zugang erhalten:

Name, Vorname Teilnehmer, Kundennummer

Datum, Unterschrift

Name, Vorname Teilnehmer

Datum, Unterschrift

**Referenzbankverbindung**

Die verbindliche Referenzbankverbindung für die oben angegebene Kundennummer für den unbaren Zahlungsverkehr lautet

Girokontonummer

Bankleitzahl

IBAN/BIC

Bank

Kontoinhaber/Zahler

Unterschrift des Kontoinhabers/Zahlers

Umbuchungen aus Sparkonten sind nur auf das Referenzkonto möglich.

Ich möchte am PSD OnlineBanking teilnehmen und damit die PSD PostBox nutzen. Eine PIN erhalte ich mit separater Post. Ich erhalte Zugang mittels OnlineBanking zu allen unter der o. a. Kundennummer gegenwärtig und zukünftig geführten Konten und Depots. Dieser Zugang gilt auch für alle Konten und Depots, für die eine Vollmacht besteht.

Der Höchstbetrag pro Buchungstag beträgt 5.000,00 EUR. Verfügungen über mehr als 5.000,00 EUR pro Buchungstag sind aus Sicherheitsgründen nicht möglich. Wünsche ich eine Änderung der Höchstbeträge, muss ich dies der Bank schriftlich mitteilen.

Es ist mir bekannt, dass ich aus Gründen der Sicherheit die mir mit dem PIN-Brief mitgeteilte PIN unmittelbar bei Erstnutzung des OnlineBanking-Services abändern muss.

**Die umseitigen Sonderbedingungen für PSD OnlineBanking erkenne/n ich/wir an.** Ergänzend gelten die Allgemeinen Geschäftsbedingungen der PSD Bank Koblenz eG. Der Wortlaut dieser Bedingungen kann in den Geschäftsräumen der PSD Bank Koblenz eG eingesehen werden; auf Verlangen werden sie ausgehändigt.

**Hinweis nach § 13 Abs. 1 Telemediengesetz**

Alle im Rahmen des OnlineBanking anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank bearbeitet und genutzt.

Ort, Datum

Unterschrift des Kontoinhabers

**Zusatzklärung bei Minderjährigenkonten**

Wir genehmigen alle Rechtsgeschäfte, die alle gegenwärtigen oder künftigen Konten unter der o. a. Kundennummer betreffen, und erteilen die in den Bedingungen aufgeführten Vollmachten. Gleichzeitig bevollmächtigen wir und gegenseitig, den Minderjährigen gegenüber der PSD Bank Koblenz eG allein zu vertreten.

Ort, Datum

Unterschrift des Vertretungsberechtigten

## Sonderbedingungen für das PSD OnlineBanking

### 1. Leistungsangebot

- (1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels Online-Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er 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. Eine Änderung dieser Limite kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

### 2. Voraussetzungen zur Nutzung des Online-Banking

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

#### 2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind:

- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN),
- der Nutzungscodes 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 Online-Banking

Der Teilnehmer erhält Zugang zum Online-Banking, wenn

- der Teilnehmer die Kontonummer oder seine individuelle Kundenkennung 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 8) 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 (TAN oder elektronische Signatur) 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) auf der Online-Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank angegebenen oder im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „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 Online-Banking-Datenformat ist eingehalten.
  - Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.
  - Die Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Überweisungsbedingungen) 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 Absatz 2 Satz 1 nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen und dem Teilnehmer eine Information über die Nichtausführung und – soweit möglich – über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Online-Banking zur Verfügung stellen.

#### 6. Sorgfaltspflichten des Teilnehmers

##### 6.1 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.

##### 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 Online-Banking-Zugangskanäle an diese zu übermitteln sowie
  - sein Authentifizierungsinstrument (vgl. Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen Personalisierten Sicherheitsmerkmal das Online-Banking-Verfahren missbräuchlich nutzen.
- (2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:
  - Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (z. B. im Kundensystem).
  - Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht auspähen können.
  - 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 und der Nutzungscodes 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 Online-Banking genutzt werden.

##### 6.3 Sicherheit des Kundensystems

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

##### 6.4 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, 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 seines Persönlichen Sicherheitsmerkmals 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 seines Personalisierten Sicherheitsmerkmals erlangt hat oder
- das Authentifizierungsinstrument oder das Personalisierte Sicherheitsmerkmal 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 8.1,

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

##### 8.2 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.

#### 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 Kunden.

#### 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 Online-Banking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

### 9. Haftung

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

Die Haftung der Bank bei nicht autorisierten und nicht oder fehlerhaft ausgeführten Online-Banking-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) Beruht ein nicht autorisierter Zahlungsvorgang vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen 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 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 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 handelt hat.

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

(5) Kommt es vor der Sperranzeige zu einer nicht autorisierten Verfügung 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 Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (vgl. Nummer 8.1 Absatz 1),
  - das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (vgl. Nummer 6.2 Absatz 2, 1. Spiegelstrich),
  - das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde (vgl. Nummer 6.2 Absatz 1, 2. Spiegelstrich),
  - das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (vgl. Nummer 6.2 Absatz 2, 3. Spiegelstrich),
  - das Personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (vgl. Nummer 6.2 Absatz 2, 4. Spiegelstrich),
  - das Personalisierte Sicherheitsmerkmal 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 Online-Banking 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

Beruhet eine nicht autorisierte Wertpapiertransaktion 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 Online-Banking-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 vorhersehbaren 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 hätte vermieden werden können.

### 10. Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit

Für die Beilegung von Streitigkeiten mit der Bank kann sich der Teilnehmer an die in 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

### 1. Die PSD PostBox

Im Rahmen der Geschäftsbeziehung zwischen der Bank und dem Kunden, der für die Nutzung der PSD PostBox freigeschaltet ist, gilt die PSD PostBox als Kanal, über den die Bank dem Kunden Dokumente in elektronischer Form bereitstellt. Ausgenommen sind Dokumente, bei denen die Schriftform vorgeschrieben ist. Mit der Anmeldung werden dem Kunden sämtliche Dokumente – Kontoauszüge und Mitteilungen – zu gegenwärtigen und künftigen Konten in die PSD PostBox eingestellt.

### 2. Übermittlung der Kontodaten

Die Bank stellt dem Kunden Auszüge und Mitteilungen, die den Geschäftsverkehr mit der Bank betreffen, elektronisch als Datei zur Verfügung; dies gilt auch für Anlagen zu Kontoauszügen. Der Rechnungsabschluss wird dem Kunden ebenfalls elektronisch als Datei zur Verfügung gestellt. Der Kunde ist verpflichtet, seine Dokumente aus der PSD PostBox regelmäßig abzurufen.

### 3. Verzicht auf papierhafte Kontoauszüge

Der Kunde verzichtet auf die papierhafte Bereitstellung von Dokumenten, wenn die entsprechenden Konten auf die PSD PostBox umgestellt sind. Lediglich den „Zwangsauszug“ (vgl. Nr. 4) erhält der Kunde per Post. Die Bank ist bereit, dem Kunden für einen Zeitraum von zehn Jahren papierhafte Kontoauszüge auf seine Kosten zu erstellen.

### 4. Zusendung von Kontoauszügen

Die Bank kann dem Kunden einzelne Mitteilungen sowie den Rechnungsabschluss kostenpflichtig zusenden, wenn sie dies auch unter Abwägung der Interessen des Kunden für gerechtfertigt hält. Sie kann dem Kunden die Kontoauszüge per Post zusenden, wenn sie feststellt, dass der elektronische Abruf der Kontoauszüge nach Ablauf eines fest definierten Zeitraumes nicht erfolgt ist. Die Kosten hierfür werden dem Kunden in Rechnung gestellt.

### 5. Voraussetzungen für den Abruf des elektronischen Kontoauszugs

Der Kunde verpflichtet sich zur Nutzung der Funktion „PSD PostBox“ eine Software (z. B. Adobe Acrobat Reader) einzusetzen, die folgende Anforderungen erfüllt:

- Der Name der Bank wird im elektronischen Kontoauszug angegeben
- Der Name des Kontoinhabers wird auf dem elektronischen Kontoauszug angegeben.
- Die maximale Anzahl von 14 Verwendungszweckzeilen je Umsatz muss im Kontoauszug darstellbar sein.

### 6. Zugang

Soweit der Kunde den Kontoauszug nicht bereits vorher abgerufen hat, gilt er am Tag nach der Bereitstellung als zugegangen.

### 7. Kündigung

Der Kunde kann die Nutzung der PSD PostBox jederzeit kündigen. Hat der Kunde mittels seiner PSD BankCard Zugang zum Kontoauszugdrucker, werden ihm ab Wirksamwerden der Kündigung die Kontoauszüge über den Kontoauszugdrucker zur Verfügung gestellt. Anderenfalls werden dem Kunden die Kontoauszüge papierhaft per Postversand zur Verfügung gestellt. Das Entgelt hierfür ergibt sich aus dem Preis- und Leistungsverzeichnis.

### 8. 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 Privatkontobereich und damit für den Kontoinhaber anerkannt, der nicht buchführungs- und aufzeichnungspflichtig im Sinne der §§ 145 ff. AO ist.