PSA DIREKTBANK
ONLINE GELDANLAGEN

Sonderbedingungen Online-Banking (Stand 12 / 2016)

1. Leistungsangebot und Begriffsbestimmungen

- PSA Direktbank ist ein Geschäftsbereich der PSA Bank Deutschland GmbH und wird im Folgenden einheitlich als "Bank" bezeichnet.
- Der Kontoinhaber kann in dem von der Bank angebotenen Umfang Bankgeschäfte mittels Online-Banking abwickeln. Des Weiteren kann er Informationen der Bank mittels Online-Banking abrufen.
- Kontoinhaber sowie vom Kontoinhaber Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer" bezeichnet.

2. Voraussetzungen der Nutzung des Online-Bankings

Um sich im Online-Banking gegenüber der Bank als berechtigte Teilnehmer auszuweisen (siehe Nummer 3) und im Online-Banking Aufträge an die Bank zu autorisieren (siehe Nummer 4) benötigt der Teilnehmer die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungs-instrumente.

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (mTAN, s. Nummer 2.2).

2.2 Authentifizierungsinstrumente

Als Authentifizierungsinstrument kommen lediglich mobile Endgeräte (zum Beispiel Mobiltelefon) in Betracht, die zum Empfang von SMS geeignet sind. Mittels eines solchen Authentifizierungsinstruments können dem Teilnehmer mTAN per SMS zur Verfügung gestellt werden.

3. Zugang zum Online-Banking

Teilnehmer erhalten Zugang zum Online-Banking, wenn

- sie ihre individuelle Kundenkennung und ihre PIN übermittelt haben,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.

Teilnehmer können nach Gewährung des Zugangs zum Online-Banking Informationen abrufen oder Aufträge erteilen.

4. Online-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

Die Wirksamkeit eines Online-Banking-Auftrags setzt voraus, dass der Teilnehmer den Online-Banking-Auftrag mit dem vereinbarten Personalisierten Sicherheitsmerkmal (mTAN) autorisiert und der Bank mittels Online-Banking übermittelt. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Möglichkeit des Widerrufs eines Online-Banking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann, wenn die Bank eine Widerrufsmöglichkeit im Online-Banking nicht ausdrücklich vorsieht, nur außerhalb des Online-Banking erfolgen.

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 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 darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

(2) Die Bank führt den Auftrag erst dann aus, wenn die folgenden Ausführungsbedingungen erfüllt sind:

- der Teilnehmer hat sich mit seinem Personalisierten Sicherheitsmerkmal legitimiert;
- die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor;
- das Online-Banking-Datenformat ist eingehalten;
- die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 vor, führt die Bank die Online-Banking-Aufträge nach Maßgabe der Sonderbedingungen, die für die jeweilige Auftragsart gelten (zum Beispiel Bedingungen für den Überweisungsverkehr), aus.

(4) Liegen die Ausführungsbedingungen nach Absatz 2 nicht vor, führt die Bank den Online-Banking-Auftrag nicht aus und informiert den Teilnehmer mittels Online-Banking über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6. Information des Kontoinhabers über Online-Banking-Verfügungen

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

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum Online-Banking

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

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Um eine missbräuchliche des Online-Banking durch Nutzung der Persönlichen Sicherheitsmerkmale und des Authentifizierungsinstruments durch Dritte zu verhindern, hat der Teilnehmer

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

(2) Zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments ist insbesondere Folgendes zu beachten:

- Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (zum Beispiel im Kundensystem).
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (zum Beispiel nicht auf Online-Händlerseiten).
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden (zum Beispiel nicht per E-Mail).
- Die PIN darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung zum Beispiel eines Auftrags oder der Aufhebung einer Sperre nicht mehr als eine mTAN verwenden.
- Das Gerät, mit dem die mTAN empfangen werden (zum Beispiel Mobiltelefon), darf nicht gleichzeitig für das Online-Banking genutzt werden.

7.3 Sicherheitshinweise

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

7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

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

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl des Authentifizierungsinstruments,
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines Persönlichen Sicherheitsmerkmals

fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Eine solche Sperranzeige kann auch jederzeit über die gesondert mitgeteilten Kontaktdaten erfolgen.

(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 Personalisierte Sicherheitsmerkmal verwendet,

muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Nimmt der Teilnehmer einen nicht autorisierten oder fehlerhaft ausgeführten Auftrag wahr, hat er die Bank hierüber zu unterrichten.

PSA Bank Deutschland GmbH, Geschäftsbereich PSA Direktbank, Siemensstraße 10, 63263 Neu-Isenburg
Telefon: +49 6102 / 833 999 0; info@psa-direktbank.de; www.psa-direktbank.de
Geschäftsführer: Jean-Baptiste Charles, Michelle Giblin; Aufsichtsratsvorsitzender: Thomas Hanswillemenke
Sitz: Neu-Isenburg; AG Offenbach am Main, HRB 48096; USt-IdNr.: DE298051057; BIC BPNDDE52XXX
IHK Offenbach – Vers.-Vermittler: D-9D1T-2B2X4-71

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

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

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

9.2 Sperre auf Veranlassung der Bank

(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 Teilnehmer von der Sperre möglichst vor, spätestens nach der Sperre unverzüglich unter Angabe der Gründe, die zu der Sperre geführt haben, unterrichten.

9.3 Aufhebung der Sperre

Liegen die Gründe für eine Sperre nicht mehr vor, hebt die Bank die Sperre auf oder tauscht das Personalisierte Sicherheitsmerkmal aus, und teilt dies dem Teilnehmer unverzüglich mit.

10. Haftung

10.1 Haftung der Bank bei nicht autorisierter Online-Banking-Verfügung und nicht oder fehlerhaft ausgeführter Online-Banking-Verfügung

Die Haftung der Bank bei nicht autorisierter Online-Banking-Verfügung und nicht oder fehlerhaft ausgeführter Online-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr).

10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

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

(2) Beruht der nicht autorisierte, vor der Sperranzeige erfolgte Zahlungsvorgang auf einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,– Euro nur, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der Personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden 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 verstoßen hat.

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach 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 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. Von einer grob fahrlässigen Verletzung der Sorgfaltspflichten kann insbesondere ausgegangen werden, wenn der Teilnehmer

- nach entsprechender Kenntniserlangung den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt (siehe Nummer 8.1 Absatz 1),
- das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2 Absatz 2 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1 2. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2 4. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 5. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2 6. Spiegelstrich),
- beim mTAN-Verfahren das Gerät, mit dem die mTAN empfangen werden (z. B. Mobiltelefon), auch für das Online-Banking nutzt (siehe Nummer 7.2 Absatz 2 7. Spiegelstrich).

(6) Für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, ist die maximale Haftung des Kontoinhabers auf den vereinbarten Verfügungsrahmen beschränkt.

10.2.2 Haftung der Bank ab der Sperranzeige

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

10.2.3 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, oder vom Zahlungsdienstleister auf Grund einer gesetzlichen Verpflichtung herbeigeführt wurden.

11. Elektronischer Kommunikationsweg: Zurverfügungstellung von Nachrichten an den Kontoinhaber im Online-Banking

11.1 Inhalt

Im Rahmen der Geschäftsbeziehung zwischen der Bank und dem Kontoinhaber gilt für die Zurverfügungstellung von Nachrichten an den Kunden der elektronische Kommunikationsweg als vereinbart, d.h. Nachrichten der Bank werden dem Kontoinhaber im Online-Banking zur Verfügung gestellt. So zur Verfügung gestellte persönliche Dokumente können sich Teilnehmer online ansehen, herunterladen und ausdrucken. Die Dokumentenauswahl kann von der Bank jederzeit erweitert oder verringert werden. Die Bank wird den Kontoinhaber hierüber informieren. Nachrichten oder Anfragen des Kontoinhabers an die Bank sind über das Online-Banking nicht möglich; der Kunde kann sich hierzu per E-Mail, per Telefon oder schriftlich an die Bank wenden.

11.2 Verzicht auf papierhafte Postzustellung

Der Kommunikationsweg über das Online-Banking wird mit dem Abschluss des Vertrags zum Internetbanking eingerichtet. Mit der Einrichtung des persönlichen Online-Banking Zugangs verzichtet der Kontoinhaber auf den postalischen Versand der eingestellten Dokumente. Auch bei Nutzung des Online-Banking ist die Bank berechtigt, die hinterlegten Dokumente postalisch oder auf andere Weise dem Kontoinhaber zuzusenden, wenn dies gesetzliche Vorgaben erforderlich machen oder es aufgrund anderer Umstände (z.B. vorübergehender Ausfall des Online-Banking) zweckmäßig oder erforderlich ist.

11.3 Mitwirkungspflichten des Kontoinhabers

Der Kontoinhaber verpflichtet sich, die Nachrichten, die ihm im Rahmen seines persönlichen Online-Banking-Zugangs zur Verfügung gestellt werden, regelmäßig auf hinterlegte Dokumente zu prüfen. Er kontrolliert die hinterlegten Dokumente auf Richtigkeit und Vollständigkeit. Beanstandungen sind der Bank unverzüglich, jedoch spätestens 6 Wochen nach Zugang mitzuteilen.

11.4 Speicherungsdauer von Nachrichten

Die Bank speichert die wie zuvor beschrieben zur Verfügung gestellten Dokumente im Rahmen der gesetzlichen Aufbewahrungsfristen. Nach Ablauf der Frist kann die Bank die entsprechenden Dokumente und Nachrichten aus dem Postfach entfernen, ohne dass der Kontoinhaber hierüber eine gesonderte Nachricht erhält.

PSA Bank Deutschland GmbH, Geschäftsbereich PSA Direktbank, Siemensstraße 10, 63263 Neu-Isenburg
Telefon: +49 6102 / 833 999 0; info@psa-direktbank.de; www.psa-direktbank.de
Geschäftsführer: Jean-Baptiste Charles, Michelle Giblin; Aufsichtsratsvorsitzender: Thomas Hanswillemenke
Sitz: Neu-Isenburg; AG Offenbach am Main, HRB 48096; USt-IdNr.: DE298051057; BIC BPNDDE52XXX
IHK Offenbach – Vers.-Vermittler: D-9D1T-2B2X4-71