

Postbank Online-Banking

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. Die Bank ist berechtigt, dem Konto-/Depotinhaber Änderungen der Allgemeinen Geschäftsbedingungen der Bank und der besonderen Bedingungen für einzelne Geschäftsbeziehungen sowie sonstige, neben den Kontoauszugsinformationen erstellte Mitteilungen durch Einstellen in die Online-Banking-Nachrichten-Box zu übermitteln.

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

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

2 Voraussetzungen zur Nutzung des Online-Banking

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

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- die persönliche Identifikationsnummer (PIN)
- einmal verwendbare Transaktionsnummern (TAN)
- der Nutzungscode für die elektronische Signatur¹⁾

2.2 Authentifizierungsinstrumente

Die TAN beziehungsweise die elektronische Signatur¹⁾ kann dem Nutzer auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:

- mittels eines TAN-Generators, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist²⁾
- mittels eines mobilen Endgerätes (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobile TAN)
- auf einer Chipkarte mit Signaturfunktion³⁾
- 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 Nutzer erhält Zugang zum Online-Banking, wenn

- dieser Nutzer die Kontonummer oder seine individuelle Kundenkennung und seine PIN oder elektronische Signatur übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Nutzers ergeben hat und
- keine Sperre des Zugangs (vgl. Nr. 8.1 und 9) vorliegt.

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

4 Online-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Nutzer muss Online-Banking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten personalisierten Sicherheitsmerkmal (TAN oder elektronische Signatur¹⁾) autorisieren und dem Kreditinstitut mittels Online-Banking übermitteln. Das Kreditinstitut bestätigt mittels Online-Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

(1) Die Widerrufbarkeit eines Online-Banking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden besonderen Bedingungen (z. B. „Besondere Bedingungen – Überweisungen“).

(2) 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 Aufträgen durch das Kreditinstitut

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

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

- Der Nutzer hat sich mit einem personalisierten Sicherheitsmerkmal legitimiert.
- Die Berechtigung des Nutzers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen besonderen Bedingungen (z. B. ausreichende Kontodeckung gemäß den „Besonderen Bedingungen – Überweisungen“) liegen vor.

Liegen die Ausführungsvoraussetzungen nach Satz 1 vor, führt die Bank die Online-Banking-Aufträge nach Maßgabe der für die jeweilige Auftragsart geltenden Besonderen Bedingungen (z. B. „Besonderen Bedingungen – Überweisungen“) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen und dem Nutzer über die Nichtausführung und, soweit möglich, über deren Gründe und die

Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtet werden können, mittels Online-Banking eine Information zur Verfügung stellen.

6 Information des Nutzers über Online-Banking-Verfügungen

Die Bank unterrichtet den Nutzer mindestens einmal monatlich über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg. Mit Nutzern, die nicht Verbraucher sind, wird die Art und Weise sowie die zeitliche Folge der Unterrichtung gesondert vereinbart.

7 Sorgfaltspflichten des Nutzers

7.1 Technische Verbindung zum Online-Banking

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

7.2 Geheimhaltung des personalisierten Sicherheitsmerkmals und sichere Aufbewahrung des Authentifizierungsinstruments

(1) Der Nutzer hat

- sein personalisiertes Sicherheitsmerkmal (vgl. Nr. 2.1) geheim zu halten und nur über die vom Kreditinstitut gesondert mitgeteilten Online-Banking-Zugangskanäle an sein Kreditinstitut zu übermitteln sowie
- sein Authentifizierungsinstrument (vgl. Nr. 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen personalisierten Sicherheitsmerkmal das Online-Banking-Verfahren missbräuchlich nutzen.

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

- Das personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (z. B. im Kundensystem).
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- 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 Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Nutzer darf zur Autorisierung z. B. eines Auftrags oder der Aufhebung einer Sperre nicht mehr als eine TAN verwenden.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.

7.3 Sicherheit des Kundensystems

Der Nutzer hat die Sicherheitshinweise auf

¹⁾ Dieses persönliche Sicherheitsmerkmal bietet die Bank derzeit nicht an.

²⁾ Letzteres bietet die Bank als Authentifizierungsinstrument derzeit nicht an.

³⁾ Dieses Authentifizierungsinstrument bietet die Bank derzeit nicht an.

der Internetseite der Bank zum Online-Banking, insbesondere die empfohlenen Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), zu beachten.

7.4 Kontrolle der Auftragsdaten mit vom Kreditinstitut angezeigten Daten

Soweit die Bank dem Nutzer Daten aus seinem Online-Banking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Nutzers (z. B. Mobiltelefon) zur Bestätigung anzeigt, ist der Nutzer 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 Nutzer

– den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder

– die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines persönlichen Sicherheitsmerkmals oder

– keine Übereinstimmung der von der Bank dem Nutzer angezeigten Transaktionsdaten mit den von ihm für die Transaktion vorgesehenen Daten (vgl. Nr. 7.4) fest,

muss der Nutzer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Nutzer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten übermitteln.

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

(3) Hat der Nutzer den Verdacht, dass eine andere Person unberechtigt

– den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines personalisierten Sicherheitsmerkmals erlangt hat oder

– das Authentifizierungsinstrument oder das personalisierte Sicherheitsmerkmal verwendet,

muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhafte Aufträge

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

9 Nutzungssperre

9.1 Sperre auf Veranlassung des Nutzers

Die Bank sperrt auf Veranlassung des Nutzers, insbesondere im Fall der Sperranzeige nach Nr. 8.1,

– den Online-Banking-Zugang für ihn oder alle Teilnehmer oder

– sein Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Online-Banking-Zugang für einen Nutzer 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 seines Zahlungsauffähigungsinstruments besteht, insbesondere dreimal in Folge eine falsche PIN übermittelt wurde.

(2) Die Bank wird dem Nutzer unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das personalisierte Sicherheitsmerkmal bzw. das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind.

Auch hierüber unterrichtet sie den Nutzer in der vereinbarten Weise.

9.4 Automatische Sperre eines chipbasierten Authentifizierungsinstruments

(1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur 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 Nutzer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeit wiederherzustellen.

10 Haftung

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

Die Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Bedingungen (z. B. „Besondere Bedingungen – Überweisungen“).

10.2 Haftung des Nutzers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

10.2.1 Haftung des Nutzers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

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

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verloren gegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Nutzer für den der Bank dadurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Nutzer seiner Pflicht zur sicheren Aufbewahrung der personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

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

(4) Der Nutzer ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Nutzer 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 Nutzer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Nutzer den hierdurch entstandenen Schaden in vollem Umfang. Grobe

Fahrlässigkeit des Nutzers kann insbesondere vorliegen, wenn er

– den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals der Bank oder die fehlende Übereinstimmung der von der Bank dem Nutzer angezeigten Transaktionsdaten mit den von ihm für die Transaktion vorgesehenen Daten nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (vgl. Nr. 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 2 2. Spiegelstrich),

– das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 1 2. 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 mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Online-Banking nutzt (siehe Nummer 7.2 Absatz 2 7. Spiegelstrich).

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

10.2.2 Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige
Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verloren gegangenen oder gestohlenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des personalisierten Sicherheitsinstruments oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften Bank und Nutzer nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung der Bank ab der Sperranzeige
Sobald die Bank eine Sperranzeige eines Nutzers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-Banking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Nutzer 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.

Fassung: 21. November 2011