

Besondere Bedingungen Postbank

Postbank Online-Banking

1 Leistungsangebot

(1) Der Konto-/Depotinhaber 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. Sie sind zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrages einen Zahlungsauslösedienst gemäß § 1 Absatz 33 Zahlungsdiensteaufsichtsgesetz und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienst gemäß § 1 Absatz 34 Zahlungsdiensteaufsichtsgesetz zu nutzen.

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 einheitlich als „Teilnehmer“, Konto und Depot werden im Folgenden 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 Verfügungsmittele.

2 Voraussetzungen zur Nutzung des Online-Banking

Der Teilnehmer benötigt für die Nutzung des Online-Banking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nr. 3) und Aufträge zu autorisieren (siehe Nr. 4). Statt eines Personalisierten Sicherheitsmerkmals kann auch ein biometrisches Merkmal des Teilnehmers zum Zwecke der Authentifizierung bzw. Autorisierung vereinbart werden.

2.1 Personalisierte Sicherheitsmerkmale
Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die die Bank dem Teilnehmer zum Zwecke der Authentifizierung bereitstellt. Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind beispielsweise

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

2.2 Authentifizierungsinstrumente
Authentifizierungsinstrumente sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurde und die vom Teilnehmer zur Erteilung eines Online-Banking-Auftrags verwendet werden. Insbesondere mittels folgender Authentifizierungsinstrumente kann das Personalisierte Sicherheitsmerkmal (z. B. TAN) dem Teilnehmer zur Verfügung gestellt werden:

- PIN-Brief,
- TAN-Generator, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist²⁾
- Online-Banking-App auf einem mobilen Endgerät (z. B. Mobiltelefon) zum Empfang oder zur Erzeugung von TAN,
- mobiles Endgerät (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
- Chipkarte mit Signaturfunktion³⁾ oder
- ein sonstiges Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden.

3 Zugang zum Online-Banking

Der Nutzer erhält Zugang zum Online-Banking, wenn

- er die Kontonummer oder seine individuelle Teilnehmererkennung sowie seine PIN oder elektronische Signatur übermittelt oder sein biometrisches Merkmal eingesetzt 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.

Die Sätze 1 und 2 gelten auch, wenn der Teilnehmer Zahlungsaufträge über einen Zahlungsauslösedienst auslöst und Zahlungskontoinformationen über einen Kontoinformationsdienst anfordert (siehe Nr. 1 Absatz 1 Satz 3).

Soweit ein Konto-/Depotinhaber einem Bevollmächtigten einen Online-Banking-Zugang für sein Konto/Depot einräumt, trägt der Konto-/Depotinhaber dafür Sorge, dass der Bevollmächtigte die dem Nutzer des Online-Banking nach diesen besonderen Bedingungen obliegenden Pflichten einhält; der Konto-/Depotinhaber haftet für ein Verschulden des Bevollmächtigten wie für eigenes Verschulden.

4 Online-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung
Der Teilnehmer muss Online-Banking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem von der Bank bereitgestellten Personalisierten Sicherheitsmerkmal (z. B. TAN) oder mit dem vereinbarten biometrischen Sicherheitsmerkmal autorisieren und der Bank mittels Online-Banking übermitteln. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags. Die Sätze 1 und 2 gelten auch, wenn der Teilnehmer einen Zahlungsauftrag über einen Zahlungsauslösedienst (siehe Nr. 1 Absatz 1 Satz 3) auslöst und übermittelt.

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 Widerrufmöglichkeit 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 Postbank“ 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 Postbank“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis Postbank“ 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 Teilnehmer hat den Auftrag 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 weiteren 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. Sie wird dem Teilnehmer hierüber mittels Online-Banking eine Information zur Verfügung stellen und soweit möglich dabei Gründe und Möglichkeiten nennen, 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 monatlich über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg. Mit Kontoinhaber, die nicht Verbraucher sind, wird die Art und Weise sowie die zeitliche Folge der Unterrichtung gesondert vereinbart.

7 Sorgfaltspflichten des Teilnehmers

7.1 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. Zur Erteilung eines Zahlungsauftrags und zum Abrufen von Informationen über

1) Dieses personalisierte 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.

ein Zahlungskonto kann der Teilnehmer die technische Verbindung zum Online-Banking auch über einen Zahlungsauslösedienst beziehungsweise einen Kontoinformationsdienst (siehe Nr. 1 Absatz 1 Satz 3) herstellen.

7.2 Geheimhaltung des Personalisierten Sicherheitsmerkmals und sichere Aufbewahrung des Authentifizierungsinstrumentes

- (1) Der Kontoinhaber hat
- das Personalisierte Sicherheitsmerkmal (vgl. Nr. 2.1) geheim zu halten sowie
 - das Authentifizierungsinstrument (vgl. Nr. 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstrumentes ist, kann in Verbindung mit der Kenntnis des dazugehörigen personalisierten Sicherheitsmerkmal das Online-Banking-Verfahren missbräuchlich nutzen. Die Geheimhaltungspflicht bezüglich der Personalisierten Sicherheitsmerkmale nach Satz 1 wird nicht verletzt, wenn der Teilnehmer diese zur Erteilung eines Zahlungsauftrags oder zum Abruf von Informationen über ein Zahlungskonto an den von ihm ausgewählten Zahlungsauslösedienst beziehungsweise Kontoinformationsdienst übermittelt (siehe Nr. 1 Absatz 1 Satz 3).

- (2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstrumentes zu beachten:
- Das Personalisierte Sicherheitsmerkmal darf nicht ungesichert elektronisch gespeichert werden.
 - Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
 - Das Personalisierte Sicherheitsmerkmal darf nicht per E-Mail weitergegeben.
 - Das Personalisierte Sicherheitsmerkmal (z. B. PIN) darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
 - Der Teilnehmer 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 Sicherheitshinweise der Bank
Der Teilnehmer hat die Sicherheitshinweise auf 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 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) 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 Authentifizierungsinstrumentes, die missbräuchliche Verwendung oder
 - die sonstige nicht autorisierte Nutzung des Authentifizierungsinstrumentes oder eines seiner Personalisierten Sicherheitsmerkmale
 - keine Übereinstimmung der von der Bank dem Teilnehmer angezeigten Transaktionsdaten mit den von ihm für die Transaktion vorgesehenen Daten (vgl. Nr. 7.4) fest,
- muss der Teilnehmer die Bank hierüber unverzüglich 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.

- (3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt
- den Besitz an dem 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 Teilnehmer 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 Nr. 8.1,
- den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
 - das 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 Authentifizierungsinstrumentes oder des personalisierten Sicherheitsmerkmals dies rechtfertigen oder
 - der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung seines Zahlungsauslösedienstinstrumentes besteht, insbesondere dreimal in Folge eine falsche PIN übermittelt wurde.

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

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber unverzüglich.

9.4 Automatische Sperre eines chipbasierten Authentifizierungsinstrumentes

- (1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscod für die elektronische Signatur 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 Authentifizierungsinstrumente können dann nicht mehr für das Online-Banking genutzt werden. Der Teilnehmer 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, fehlerhaft oder verspätet ausgeführten Online-Banking-Verfügung
Die Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Online-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung eines Personalisierten Sicherheitsmerkmals oder seines Authentifizierungsinstrumentes

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 verloren gegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstrumentes oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungsinstrumentes, haftet der Kontoinhaber 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 Kontoinhaber 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 Authentifizierungsinstrumentes vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder

– der Verlust des Authentifizierungsinstruments 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 Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von Absatz 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere 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 (siehe Nr. 8.1 Absatz 1),
- das Personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe Nr. 7.2 Absatz 2 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nr. 7.2 Absatz 1),
- das Personalisierte Sicherheitsmerkmal per E-Mail weitergegeben hat (siehe Nr. 7.2 Absatz 2 3 Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nr. 7.2 Absatz 2 4 Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nr. 7.2 Absatz 2 5 Spiegelstrich),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Online-Banking nutzt (siehe Nr. 7.2 Absatz 2 6 Spiegelstrich).

(4) Abweichend von Absatz 1 und 3 ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt hat, obwohl die Bank zur starken Kundenauthentifizierung nach § 68 Absatz 4 Zahlungsdiensteaufsichtsgesetz verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, das der Teilnehmer weiß, z. B. PIN), Besitz (etwas, das der Teilnehmer besitzt, z. B. TAN-Generator) oder Inhärenz (etwas, das der Teilnehmer ist, z. B. Fingerabdruck).

(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 Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 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.

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

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

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

10.2.2 Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige
Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen 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: 25. Mai 2018