Postbank – eine Niederlassung
der Deutsche Bank AG

Antrag für den Zugang zur Bank über elektronische Medien

Ihr Vertragspartner:
Postbank – eine Niederlassung der Deutsche Bank AG
(nachfolgend „Bank“ genannt)

Filialnr. | Kundennummer

Kontoinhaber

Vorname/n

Nachname/Firmenname

Anmeldung zum Postbank Online-Banking für folgende Person:

Vorname/n

Nachname

Voraussetzung für die Anmeldung zum Online- und/oder Telefon-Banking ist, dass die Person, Kontoinhaber, Vertretungsberechtigter oder Bevollmächtigter ist, z. B. auf Grund einer Bankvollmacht.

Anmeldung zum Postbank Online-Banking

Bitte ankreuzen.

☐ Hiermit beantrage/n ich/wir die Freischaltung aller unter der oben genannten Kundennummer geführten bestehenden und künftigen Konten und ggf. Depots für das Postbank Online-Banking.

Sofern ich bereits einen Verfügungsrahmen für oben genannte Kundennummer vereinbart habe, gilt dieser auch weiterhin. Falls nicht, gilt ein Verfügungsrahmen von 2.500 Euro (pro Tag und Kundennummer).

Abweichend davon wird folgender Verfügungsrahmen vereinbart:

Euro

Ausstattung mit Zugangsdaten

Sofern die oben genannte Person bereits über persönliche Zugangsdaten für das Postbank Online-Banking verfügt, gelten diese auch für oben genannte Kundennummer. Andernfalls werden diese an die Adresse der oben genannten Person gesandt.

BestSign

Für das Online-Banking der Postbank wird neben den Zugangsdaten (Postbank ID und Passwort) das Sicherheitsverfahren BestSign benötigt. BestSign kann sowohl für die Anmeldung zum Postbank Online-Banking, als auch für die Freigabe von Aufträgen und Transaktionen, z. B. Überweisungen genutzt werden.

Falls BestSign bereits in einem bestehenden Online-Zugang genutzt wird, kann dies ebenfalls für die oben angegebene Kundennummer verwendet werden.

Falls nicht, benötigt o. g. Person die Postbank BestSign App auf einem Smartphone oder ein separates BestSign-Gerät.

Die „Postbank BestSign“ App wird kostenfrei im Google PlayStore (für Android) und im Apple Store (für iOS) angeboten.

Das BestSign-Gerät von SealOne® wird im Online-Shop unter www.postbank.de/bestsign angeboten.

Alle Informationen und Anleitungen zu BestSign stehen unter www.postbank.de/bestsign bereit.

Sofern ein neues BestSign-Verfahren eingerichtet wird, senden wir Ihnen auf Wunsch einen Code per SMS an ihre Mobilfunknummer. Geben Sie hier ihre Mobilfunknummer an:

Aktivierungsverfahren

☐ Ich möchte die Mobilfunknummer nutzen, um das Sicherheitsverfahren Postbank BestSign zu aktivieren.

Bitte geben Sie eine Mobilfunknummer an. Wenn der Mobilfunkanbieter nicht in Deutschland ansässig ist, stellen Sie die entsprechende Ländervorwahl voran. Beispiel für Frankreich +33 oder 0033 gefolgt von ihrer Mobilfunknummer.

Mobilfunknummer

Vorwahl | Rufnummer

Alternativ können Sie einen Aktivierungsbrief bei der Einrichtung in der BestSign-App oder nach dem Login im Postbank Online-Banking anfordern.

Der Nutzer soll für folgende Dienstleistungen berechtigt sein:

Bitte ankreuzen.

☐ Ich möchte bzw. die oben genannte Person, z. B. Bevollmächtigte/r soll die Standardfunktionen nutzen.

Hiervon sollen folgende **Funktionen ausgenommen** sein:

☐ Kontoumsätze einsehen

☐ In- und Auslandsüberweisungen tätigen[1]

☐ Depotumsätze einsehen

☐ Wertpapieraufträge erteilen[1]

Lastschriften

Bitte ankreuzen.

Darüber hinaus soll die Einreichung von

☐ SEPA-Basis-Lastschriften

☐ SEPA-Firmen-Lastschriften

für o. g. Person freigeschaltet werden.

Voraussetzung ist eine bestehende Vereinbarung mit der Bank zur Einreichung von Lastschriften.

Nutzung des eSafe (digitales Postfach und Schließfach)

Bitte ankreuzen.

☐ Bitte aktivieren Sie für mein Konto und/oder Depot den eSafe (digitales Postfach) für den Empfang von Bankmitteilungen. „Digitales Schließfach“ und „eSafe-Client“ bietet die Bank erst zu einem späteren Zeitpunkt an. Die diesbezüglichen Regelungen dieser Bedingungen werden schon jetzt mit Ihnen vereinbart und treten in Kraft, wenn die Bank diese Funktionen anbietet und Sie diese auch nutzen.

Mit der Aktivierung des Postfachs im eSafe erhalte ich zukünftig wichtige Bankdokumente direkt in mein Online-Banking und kann diese über PC, Tablet oder Smartphone abrufen.

Die Nutzungsbedingungen habe ich gelesen und akzeptiere sie.

Ich erkläre mich damit einverstanden, dass mir Bankmitteilungen, u. a. vertraglich und aufsichtsrechtlich geschuldete Informationen insbesondere Allgemeine Geschäftsbedingungen sowie ggfs. deren Änderungen, Preisverzeichnis, Kontoabrechnungen, Zinsänderungen, Mitteilungen zu eingeräumten Kontoüberziehungen (z. B. DispoKredit, Kreditlinien etc.) und zu geduldeten Kontoüberziehungen (z. B. Sollzinsen, Inanspruchnahmen, Beratungsangebote, Änderungen zur Höhe eines Dispokredite etc.) sowie Wertpapierabrechnungen, regelmäßige Berichte über Finanzinstrumente oder Wertpapierdienstleistungen (z. B. Berichte nach Art. 59 f. Delegierte Verordnung (EU) 2017/565 etc.) auf einem anderen dauerhaften Datenträger als Papier (eSafe, Internet oder E-Mail) übermittelt werden, soweit diese nach den gesetzlichen Vorgaben zulässig ist.

[1] **Hinweis für Minderjährige:** Minderjährige ohne Verfügungsberechtigung können lediglich Konto- und Depotinformationen abfragen.

Antrag für den Zugang zur Bank über elektronische Medien

Nutzung des eSafe (digitales Postfach und Schließfach) Fortsetzung

Es gelten die Bedingungen zur Nutzung des Postbank eSafe (digitales Postfach und Schließfach).

E-Mail-Adresse (Pflichtfeld)

Anmeldung der Kundennummer für das Postbank Telefon-Banking

Bitte ankreuzen.

☐ Ich, als Kontoinhaber oder Vertretungsberechtigter beantrage die Freischaltung aller Konten und ggf. Depots unter meiner oben genannten Kundennummer für das Postbank Telefon-Banking.

Der Zugang zu den Konten und Depots erfolgt über Telefon-Banking-ID und PIN.

Sofern die oben genannte Person, z. B. Bevollmächtigte/r bereits über persönliche Zugangsdaten verfügt, gelten sie auch für diese Kundennummer. Andernfalls werden dies an die Adresse der oben genannten Person zugesandt.

Damit kann ich den Standardfunktionsumfang des Postbank Telefon-Banking nutzen (z. B. Kontoumsätze einsehen, In- und Auslandsüberweisungen tätigen, Depotumsätze einsehen und Wertpapieraufträge erteilen).

Voraussetzung für die Teilnahme am Telefon-Banking und Wertpapiergeschäft ist die Aufzeichnung der Telefonate. Die Aufzeichnung erfolgt zu Nachweiszwecken sowie aufgrund gesetzlicher Vorgaben. Nach Ablauf entsprechender Aufbewahrungsfristen werden diese Daten gelöscht.

Hinweise

— Es gelten die allgemeinen Geschäftsbedingungen und Sonderbedingungen der Bank
insbesondere die Bedingungen für den Zugang zur Bank über elektronische Medien, die Bedingungen für den Electronic Broking Service sowie die Bedingungen zur Nutzung des Postbank eSafe (digitales Postfach und Schließfach).

Sie können den Wortlaut dieser Bedingungen in den Filialen der Deutschen Post AG, die Postbank Dienstleistungen anbieten oder in den Postbank Filialen einsehen.

Unterschriften

Datum

Ort

Unterschrift

1. Kontoinhaber/in bzw. Vertretungsberechtigte/r

X

2.Kontoinhaber/in bzw. Vertretungsberechtigte/r oder Bevollmächtigte/r

X

Postbank – eine Niederlassung
der Deutsche Bank AG

Bedingungen für den Zugang zur Bank über elektronische Medien

Stand: Oktober 2022

1. Leistungsangebot

(1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels elektronischer Zugangsmedien, im Einzelnen Online-Banking und Telefon-Banking (jeweils einzeln „Online-Banking“ bzw. „Telefon-Banking“ sowie gemeinsam „Zugangsmedien“ bzw. „elektronische Medien“), in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online- und Telefon-Banking abrufen. Im Rahmen des Online-Bankings sind sie gemäß § 675f Absatz 3 BGB zusätzlich berechtigt, Zahlungsauslösedienste gemäß § 1 Absätze 33 und 34 Zahlungsdiensteaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen sorgfältig ausgewählte sonstige Drittdienste nutzen.

(2) Kunde und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.

(3) Für die Nutzung der Zugangsmedien gelten die mit der Bank gesondert vereinbarten Verfügungslimite.

2. Voraussetzungen zur Nutzung der elektronischen Medien

(1) Der Teilnehmer kann Bankgeschäfte über elektronische Medien abwickeln, 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 bestimmten 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[1] erteilen (siehe Nummer 4 dieser Bedingungen).

(3) Authentifizierungselemente sind
– Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. die persönliche Identifikationsnummer [PIN] oder das persönliche Passwort),
– Besitzelemente, also etwas, was nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder Empfang von einmal verwendbaren Transaktionsnummern [TAN], die girocard mit TAN-Generator oder das mobile Endgerät), oder
– 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 das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.

(5) Je nach Authentifizierungsverfahren und -instrument benötigt der Teilnehmer hierfür gegebenenfalls geeignete Hard- und Software. Über das Angebot der bankeigenen Anwendungen hinaus bleibt der Teilnehmer selbst für die Beschaffung, Installation und Pflege dieser Hard- und Software verantwortlich.

(6) Bei einer Nutzung einer Hard- bzw. Software von Drittanbietern durch den Teilnehmer übernimmt die Bank keine eigene Gewährleistung oder sonstige Verantwortung für eine andauernde Eignung oder Verfügbarkeit im Zusammenhang mit einem Authentifizierungsverfahren.

3. Zugang über elektronische Medien

(1) Der Teilnehmer erhält Zugang zu Online- und Telefon-Banking der Bank, wenn
– dieser die Kontonummer oder seinen individuellen Benutzernamen angibt und
– er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
– keine Sperre des Zugangs (siehe Nummer 8.1 und 9 dieser Bedingungen) vorliegt. Nach Gewährung des Zugangs zum Online- und Telefon-Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge[1] 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 Authentifizierungselementes 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 Daten (§ 1 Absatz 26 Satz 2 ZAG).

4. Aufträge[1]

4.1. Auftragserteilung

(1) 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 Übertragung einer elektronischen Signatur als Nachweis des Besitzelements) zu verwenden. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags.

(2) Der Teilnehmer kann Telefon-Banking-Aufträge nur nach erfolgreicher Autorisierung mit von der Bank bereitgestelltem Personalisiertem Sicherheitsmerkmal erteilen. Die Bank bestätigt den Eingang des Auftrags auf dem vom Teilnehmer für den Auftrag gewählten Zugangsweg. Die zwischen der Bank und dem Kontoinhaber übermittelte Telefonkommunikation wird zu Beweiszwecken automatisch aufgezeichnet und gespeichert.

4.2. Widerruf von Aufträgen

Die Widerrufbarkeit eines 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- und Telefon-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Online- und Telefon-Banking ausdrücklich vor.

923 933 010 Oktober 2022

[1] Zum Beispiel Überweisung, Dauerauftrag und Lastschrift

5. Bearbeitung von Aufträgen[1] durch die Bank

(1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Online- und Telefon- Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufs. 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 dem „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 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.
– Im Telefon-Banking wird die Bank Verfügungen über das Konto, die eine Zahlung[1] an einen Dritten (abweichende Kontonummer) enthalten, bis zu einem Betrag von insgesamt unter 50.000 EUR pro Tag ausführen, sofern nicht ein anderer Verfügungshöchstbetrag mit dem Teilnehmer vereinbart ist. Für Überträge (Überweisungen) innerhalb der gleichen Kundennummer oder An- und Verkäufe von Wertpapieren gilt diese Betragsgrenze nicht.
– Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen 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. Bedingungen für den Überweisungsverkehr, Bedingungen für Wertpapiergeschäfte) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen und den Teilnehmer 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- bzw. Telefon-Banking oder postalisch informieren.

6. Information des Kunden über Online- und Telefon-Bankingverfügungen[1]

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

7. Sorgfaltspflichten des Teilnehmers

7.1. Schutz der Authentifizierungsinstrumente

(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- und Telefon-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummer 3 und 4 dieser Bedingungen).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:
a) Wissenselemente, wie z. B. die PIN, sind geheim zu halten. Sie dürfen insbesondere
– nicht außerhalb des Online-Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden.
– nicht ungesichert außerhalb des zugelassenen Authentifizierungsverfahrens elektronisch gespeichert werden (z. B. PIN im Klartext im Computer oder im mobilen Endgerät) und
– nicht auf einem Gerät notiert sein oder als Abschrift zusammen mit einem Gerät, das als Besitzelement (z. B. mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Online-Banking und Fingerabdrucksensor) dient, aufbewahrt werden.
b) Besitzelemente, wie z. B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
– ist 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 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 ein Gerät als Besitzelement für das Online- Banking des Teilnehmers aktivieren.
c) Seinselemente, 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 Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online-Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Online-Banking das von der Bank ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Beim mobileTAN-Verfahren darf das mobile Gerät, mit dem die TAN empfangen werden (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 (siehe Nummer 1 Absatz 1 Satz 3 dieser Bedingungen) verwenden. Möchte der Teilnehmer einen sonstigen Drittdienst nutzen (siehe Nummer 1 Absatz 1 Satz 4 dieser Bedingungen), hat er diesen mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

[1] Zum Beispiel Überweisung, Dauerauftrag und Lastschrift

(6) Der Aufforderung per elektronischer Nachricht (z. B. E-Mail), eine damit übersandte Verknüpfung zum (vermeintlichen) Online-Banking der Bank anzuwählen und darüber persönliche Zugangsdaten einzugeben, darf nicht gefolgt werden.

(7) Anfragen außerhalb der bankseitig zur Verfügung gestellten originären Zugangswege, in denen nach vertraulichen Daten wie PIN, Geheimzahl oder Passwort/TAN gefragt wird, dürfen nicht beantwortet werden. Die Nutzung von Zahlungsauslösediensten bzw. Kontoinformationsdiensten bleibt hiervon unberührt.

(8) Der Teilnehmer hat vor seinem jeweiligen Zugang zum Online-Banking sicherzustellen, dass auf dem verwendeten System handelsübliche Sicherheitsvorkehrungen (wie Anti-Viren-Programm und Firewall) installiert sind und diese ebenso wie die verwendete System- und Anwendungssoftware regelmäßig aktualisiert werden. Beispiele handelsüblicher Sicherheitsvorkehrungen kann der Teilnehmer den Internetseiten der Bank entnehmen.

(9) Die Softwareanwendungen der Bank sind ausschließlich direkt von der Bank oder von einem von der Bank benannten Anbieter zu beziehen.

7.2. Sicherheitshinweise der Bank

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. Darüber hinaus hat der Kunde in eigener Verantwortung etwaige Sicherheitshinweise der Anbieter der eingesetzten Kundensysteme zu beachten (z. B. Sicherheitsupdates von Systemsoftware mobiler Endgeräte).

7.3. Prüfung durch Abgleich der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Daten (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (z. B. mittels mobilem Endgerät oder Lesegerät). Der Teilnehmer ist verpflichtet, vor der Autorisierung (z. B. Eingabe der TAN) die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen. Stimmen die angezeigten Daten nicht überein, ist der Vorgang abzubrechen und die Bank unverzüglich zu informieren.

8. Anzeige- und Unterrichtungspflichten

8.1. Sperranzeige

(1) Stellt der Teilnehmer
– den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. mobiles Endgerät, Signaturkarte) oder
– die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine 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 vom Teilnehmer bezeichneten 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- und Telefon-Banking-Zugang für einen Teilnehmer sperren oder ein Authentifizierungsinstrument nicht mehr zulassen, wenn
– sie berechtigt ist, den Online- und Telefon-Banking-Vertrag aus wichtigem Grund zu kündigen,
– sachliche Gründe im Zusammenhang mit der Sicherheit seiner Authentifizierungselemente dies rechtfertigen,
– der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht oder
– ein genutzter Zugangsweg bzw. ein im Zusammenhang mit einem Authentifizierungsverfahren zugelassenes Gerät von der Bank als unsicher eingestuft wird. Als Zugangsweg gelten auch Softwareanwendungen der Bank in allen zur Verfügung stehenden Versionen.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre postalisch, telefonisch oder online 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. Der Teilnehmer kann eine von ihm veranlasste Sperrung nur postalisch oder mit telefonisch legitimiertem Auftrag aufheben lassen.

9.4. Automatische Sperre eines chipbasierten Besitzelements

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

(2) Wird die Geheimzahl zur WebSign-Chipkarte bzw. zur personalisierten Electronic-Banking-Karte dreimal hintereinander (Karten ab Bestelldatum 09/2012) bzw. achtmal hintereinander (Karten vor Bestelldatum 09/2012) falsch eingegeben, wird die Karte automatisch gesperrt.

923 933 010 Oktober 2022

(3) Ein TAN-Generator als Bestandteil einer Chipkarte, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn der Code dreimal in Folge falsch eingegeben wird.

(4) Die in den Absätzen 1, 2 und 3 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. Vereinbarung eines elektronischen Kommunikationswegs

(1) Der Kunde und die Bank vereinbaren, dass die Bank mit dem Nutzer elektronisch kommunizieren kann, d. h. per E-Mail über die durch den Nutzer angegebene E-Mail-Adresse.

(2) Der Kunde ist damit einverstanden, entsprechende Mitteilungen unverschlüsselt per E-Mail zu erhalten. Insbesondere ist die Bank berechtigt, dem Kunden Änderungen ihrer Allgemeinen Geschäftsbedingungen und der besonderen Bedingungen für einzelne Geschäftsbeziehungen auf diesem Weg zu übermitteln. Personenbezogene Daten werden auf diesem Weg nicht übertragen.

11. Haftung

11.1. Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags[1] und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Bank bei einer nicht autorisierten Online- und Telefon-Banking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Online-/Telefon-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für Wertpapiergeschäfte).

11.2. Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

11.2.1. Haftung des Kunden für nicht autorisierte Zahlungsvorgänge[1] 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 EUR, 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 Zahlungsvorgangzu 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 Anzeige- und Sorgfaltspflichten 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 3
– 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 nach § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Inhärenz (siehe Nr. 2 Absatz 3 dieser Bedingungen).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

(6) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 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 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. Punkt findet keine Anwendung.

[1] Zum Beispiel Überweisung, Dauerauftrag und Lastschrift

11.2.2. Haftung bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige

Beruhen 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.

11.2.3. Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-/Telefon-Banking-Verfügungen[1] entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

11.2.4. 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.

923 933 010 Oktober 2022

[1] Zum Beispiel Überweisung, Dauerauftrag und Lastschrift

Bedingungen für den Electronic Broking Service (EBS)

Für die Teilnahme am Electronic Broking Service (EBS) gelten ergänzend zu den „Bedingungen für den Zugang zur Bank über elektronische Medien“ die folgenden Bedingungen.

1. Leistungsumfang
Der Depotinhaber kann in Abhängigkeit von der konkreten Ausgestaltung der jeweiligen EBS Online-Anwendung (z. B. Internet-Broking) den Electronic Broking Service auf seinem Personal Computer nutzen, um

– Informationen und Analysen über seine in den Electronic Broking Service einbezogenen Konten und Depots zu erhalten,
– Aufträge zum Kauf von Wertpapieren aus der EBS-Wertpapierpalette zu Lasten seiner in den Electronic Broking Service einbezogenen Konten nach Maßgabe der Ziffer 2 dieser Bedingungen zu erteilen,
– Aufträge zum Verkauf von Wertpapieren aus der EBS-Wertpapierpalette zu Lasten seiner im Electronic Broking Service geführten Depots zu tätigen,
– Informationen, Stammdaten, Kennzahlen und Einschätzungen, soweit vorhanden, zu den in der Wertpapierpalette des EBS geführten Wertpapiergattungen zu erhalten,
– Kursinformationen zu den in der Wertpapierpalette des EBS geführten Wertpapieren zu beziehen und Devisenkurse zu den wichtigsten Währungen abzufragen.

Die Bank erbringt im Rahmen des Electronic Broking Service keine Anlageberatung. Auch die vorgenannten Informationen, Stammdaten, Kennzahlen und Einschätzungen stellen keine Anlageberatung dar. Sie dienen ausschließlich dem Zweck, den Kunden in die Lage zu versetzen, eine selbstständige Anlageentscheidung zu treffen.

Alle Einzelheiten über den Umfang des Dienstleistungsangebotes der Bank im Rahmen der jeweiligen EBS Online-Anwendung sind in einer Benutzeranleitung enthalten, die mit der jeweiligen Software zur Verfügung gestellt wird.

2. Risikoklassenprüfung bei Kaufaufträgen
Die Bank ordnet jedem Verfügungsberechtigten auf der Grundlage seiner Angaben im KapitalAnlageCheck/Kundenangaben zum Wertpapiergeschäft eine persönliche Erfahrungs-Risikoklasse zu. Abhängig von der Depotform vergibt die Bank außerdem für bestimmte Unterdepots eine Depot-Risikoklasse auf der Grundlage der Angaben des Depotinhabers und teilt diese dem Depotinhaber mit. Über den Electronic Broking Service erteilte Kaufaufträge des Depotinhabers führt die Bank ungeachtet der vorgenannten Risikoklassen aus. Soweit eine andere verfügungsberechtigte Person als der Depotinhaber einen Kaufauftrag erteilt, wird dieser nur bis zur Grenze der Depot-Risikoklasse ausgeführt.

3. Zugang zum Electronic Broking Service
EBS Online-Anwendungen können so ausgestaltet sein, dass der Kunde Zugang zu der Online-Nutzung durch Eingabe eines frei wählbaren persönlichen Kennworts erhält. Die Eingabe des persönlichen Kennworts ergänzt in diesen Fällen das Zugangsverfahren durch Eingabe von PIN und, falls im Einzelfall vorgesehen, TAN (Ziff. 4.1 der „Bedingungen für den Zugang zur Bank über elektronische Medien“). Einzelheiten werden dem Kunden jeweils in der Benutzerführung angezeigt.

4. Auftragserteilung zum Kauf und Verkauf von Wertpapieren
Aufträge zum Kauf bzw. Verkauf von Wertpapieren sind vom Kunden erst dann erteilt, wenn er die bei aufgebauter Online-Verbindung von der Bank zurückgesandte Rückmeldung im Bildschirmdialog bestätigt und die Order damit freigibt. Der in der Rückmeldung enthaltene voraussichtliche Kurswert beruht auf dem zuletzt verfügbaren Kurs aus den Systemen der Bank. Dieser Betrag dient lediglich als Richtgröße für den Kunden und entspricht weder dem genauen Preis des Ausführungsgeschäfts noch entspricht er dem endgültigen Abrechnungsbetrag der Wertpapiertransaktion. Der Preis des Ausführungsgeschäfts wird erst mit der Orderausführung an der Börse bestimmt; der endgültige Abrechnungsbetrag enthält zusätzlich das Entgelt der Bank und die von ihr in Rechnung gestellten Auslagen einschließlich fremder Kosten.

5. Orderänderung und Orderlöschung
Soweit einzelne EBS Online-Anwendungen die Möglichkeit vorsehen, erteilte Aufträge zum Kauf bzw. Verkauf von Wertpapieren nachträglich zu ändern oder zu löschen, bestehen diese Änderungs- und Widerrufsmöglichkeiten nur, sofern der ursprüngliche Wertpapierauftrag zwischenzeitlich noch nicht ausgeführt wurde. Maßgeblich ist dabei nicht der im „Orderbuch“ des Kunden ausgewiesene Orderstatus; dieser stellt keine Echtzeit-Information dar, sondern unterliegt aus technischen Gründen einer Zeitverzögerung. Entscheidend für die Möglichkeit der Orderänderung und Orderlöschung (Widerruf) ist vielmehr ausschließlich, ob diese Nachricht so rechtzeitig eingeht, dass die Bank die Ausführung des ursprünglichen Wertpapierauftrags tatsächlich noch verhindern kann.

6. Ausführungsplatz/Ausführungsart
Bei über EBS Online-Anwendungen erteilten Aufträgen zum Kauf oder Verkauf von Wertpapieren können Ausführungsplatz und Ausführungsart festgelegt werden. Wird kein Ausführungsplatz und keine Ausführungsart festgelegt, erfolgt die Ausführung gemäß den „Grundsätzen für die Ausführung von Aufträgen in Finanzinstrumenten“ der Bank. Aus technischen Gründen können für einzelne Wertpapiere nicht alle in Betracht kommenden Börsenplätze systemseitig vorgegeben werden. In diesem Fall beschränkt sich das Weisungsrecht des Kunden im Rahmen des EBS auf die systemseitig vorgesehenen Ausführungsorte. Die Möglichkeit der anderweitigen Auftragserteilung, z. B. unmittelbar über den Kundenberater, besteht in jedem Fall.

7. Informationen, Meinungsaussagen, Einschätzungen
Die über den Electronic Broking Service abrufbaren Informationen, Stammdaten, Kennzahlen und Marktkurse bezieht die Bank aus öffentlich zugänglichen Quellen und von Dritten, die sie für zuverlässig hält. Eine Garantie für die Richtigkeit oder Vollständigkeit der Angaben kann die Bank nicht übernehmen, und keine Aussage ist als solche Garantie zu verstehen. Alle Meinungsaussagen geben die aktuelle Einschätzung eines der Researchteams der Bank wieder. Die zum Ausdruck gebrachten Meinungen können sich ohne vorherige Ankündigung ändern. Weder die Bank noch deren übrige assoziierte Unternehmen haften für die Verwendung der über den Electronic Broking Service abgerufenen Informationen, Stammdaten, Kennzahlen, Marktdaten und Einschätzungen und deren Inhalt.

8. Geheimhaltung der Berechtigungsmerkmale
EBS Online-Anwendungen stehen als persönliche Instrumente ausschließlich dem Depotinhaber zur Verfügung. Sieht die jeweilige EBS Online-Anwendung ein persönliches Kennwort des Kunden vor, gelten für dieses die Regelungen über die Geheimhaltung der PIN und der TAN in Ziff. 7 der „Bedingungen für den Zugang zur Bank über elektronische Medien“ entsprechend. Mit dem Bezug seiner Konto- und Depotdaten und deren Abspeicherung auf dem Personal Computer ist der Kunde für die Geheimhaltung dieser Daten selbst verantwortlich.

Ergänzend gelten die Allgemeinen Geschäftsbedingungen und die „Sonderbedingungen für Wertpapiergeschäfte“, die in jeder Geschäftsstelle eingesehen werden können und die auf Wunsch dem Kunden zugesandt werden.