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 / Firma

Bei Unterzeichnung durch mehrere Kontoinhaber gilt jeweils statt der verwendeten Einzahl die Mehrzahl.

Anmeldung der Kundennummer für das Online-Banking

Bitte ankreuzen.

☐ Hiermit melde ich mein(e) Konto/Konten und Depot(s)* unter der o. g. Kundennummer für das Online-Banking an.

Für Online-Überweisungen wird ein Verfügungsrahmen von 2.500 Euro pro Tag beantragt, wenn nachstehend kein abweichender Rahmen beantragt wird.

Abweichend beantragter Verfügungsrahmen:

Euro

Anmeldung des Nutzers für das Online-Banking

Der Zugang soll für

Bitte ankreuzen.

☐ den o. g. Kontoinhaber

oder, falls hiervon abweichend,

☐ folgenden Nutzer

Vorname/n

Nachname

Geburtsdatum

Eine wirksame Anmeldung setzt voraus, dass der Nutzer verfügungsberechtigt ist, z. B. auf Grund einer Bankvollmacht.

Damit kann ich bzw. der oben genannte Nutzer in dem von der Bank angebotenem Umfang das Online-Banking nutzen (z. B. Kontoumsätze einsehen, In- und Auslandsüberweisungen tätigen, Depotumsätze einsehen und Wertpapieraufträge erteilen).*

Sofern der Nutzer nur in eingeschränktem Umfang Zugriff auf das Online-Banking haben soll, so ist bei einem vom Kontoinhaber abweichenden Nutzer das angehängte Formular „Antrag für den Zugang zur Bank über elektronische Medien für einen weiteren Nutzer“ zu verwenden.

Einschränkungen für den Kontoinhaber sind separat zu beauftragen.

Darüber hinaus soll die Einreichung von

☐ SEPA-Basis-Lastschriften

☐ SEPA-Firmen-Lastschriften

freigeschaltet werden.

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

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.

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.

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.

Rufnummer

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.

Einverständniserklärung zu Bankmitteilungen

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.

Die Bank wird mich über die Einstellung einer Mitteilung in den eSafe gesondert per E-Mail benachrichtigen.

E-Mail-Adresse (Pflichtfeld)

Geltungshinweis / Bedingungen

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

„Digitales Schließfach“ und „eSafe-Client“ bietet die Bank erst zu einem späteren Zeitpunkt an. Die diesbezüglichen Regelungen der oben erwähnten Bedingungen werden schon jetzt mit Ihnen vereinbart und treten in Kraft, wenn die Bank diese Funktionen anbietet und Sie diese auch nutzen.

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

Postbank – eine Niederlassung
der Deutsche Bank AG

Antrag für den Zugang zur Bank über elektronische Medien

Telefon-Banking

Bitte ankreuzen.

☐ Hiermit melde ich mein/e bestehenden und zukünftigen Konto/Konten, Depot/s unter der genannten Kundennummer für die genannte Person zum Telefon-Banking an.

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 in dem von der Bank angebotenen Umfang das Postbank Telefon-Banking nutzen (z. B. Kontoumsätze einsehen, In- und Auslandsüberweisungen tätigen, Depotumsätze einsehen und Wertpapieraufträge erteilen).

Aufzeichnung der Telefonkommunikation

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.

Einbeziehung der Geschäftsbedingungen

Maßgebend für die Geschäftsverbindung sind die Allgemeinen Geschäftsbedingungen der Bank. Es gelten die Bedingungen für den Zugang zur Bank über elektronische Medien und die Bedingungen zur Nutzung des eSafe (digitales Postfach und Schließfach).

Der Wortlaut der einzelnen Regelungen kann in den Geschäftsräumen der Bank oder unter www.postbank.de eingesehen werden. Sie werden auf Wunsch ausgehändigt oder zugesandt.

Unterschriften

Datum

Ort

Unterschrift Kontoinhaber

X

Unterschrift der Person, für die ein Zugang beantragt wird

X

Postbank – eine Niederlassung
der Deutsche Bank AG

Antrag für den Zugang zur Bank über elektronische Medien für einen weiteren Nutzer

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

Filialnr. | Kundennummer

Kontoinhaber

Vorname/n

Nachname

Bei Unterzeichnung durch mehrere Kontoinhaber gilt jeweils statt der verwendeten Einzahl die Mehrzahl.

Nutzer

Neben dem Kontoinhaber können weitere Nutzer zum Online-Banking und/oder Telefon-Banking angemeldet werden. Eine wirksame Anmeldung setzt voraus, dass der Nutzer verfügungsberechtigt ist, z. B. auf Grund einer Bankvollmacht.

Der Verfügungsberechtigte soll den jeweiligen elektronischen Zugang zu meinem/unserem Konto/Depot nutzen:

Vorname/n

Nachname

Geburtsdatum

Anmeldung des Nutzers für das Online-Banking

Der Nutzer soll folgende Bankdienstleistungen nutzen

Bitte ankreuzen.

- ☐ Kontoumsätze einsehen
- ☐ Digitales Postfach (eSafe) einsehen
- ☐ In- und Auslandsüberweisungen tätigen*
- ☐ Depotumsätze einsehen
- ☐ Wertpapieraufträge erteilen*
- ☐ SEPA-Basis-Lastschriften einreichen**
- ☐ SEPA-Firmen-Lastschriften einreichen**
- ☐ Sonstige Aufträge erteilen (z. B. Mitteilungen an die Bank senden)

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.

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.

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.

Rufnummer

Telefon-Banking

Bitte ankreuzen.

☐ Hiermit melde ich mein/e bestehenden und zukünftigen Konto/Konten, Depot/s unter der genanten Kundennummer für die genannte Person zum Telefon-Banking an.

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 in dem von der Bank angebotenen Umfang des Postbank Telefon-Banking nutzen (z. B. Kontoumsätze einsehen, In- und Auslandsüberweisungen tätigen, Depotumsätze einsehen und Wertpapieraufträge erteilen).

Aufzeichnung der Telefonkommunikation

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.

Einbeziehung der Geschäftsbedingungen

Maßgebend für die Geschäftsverbindung sind die Allgemeinen Geschäftsbedingungen der Bank. Es gelten die Bedingungen für den Zugang zur Bank über elektronische Medien und die Bedingungen zur Nutzung des eSafe (digitales Postfach und Schließfach).

Der Wortlaut der einzelnen Regelungen kann in den Geschäftsräumen der Bank oder unter www.postbank.de eingesehen werden. Sie werden auf Wunsch ausgehändigt oder zugesandt.

Datum

Ort

Unterschriften

Unterschrift Kontoinhaber

X

Unterschrift der Person, für die ein Zugang beantragt wird

X

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

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

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 zur Nutzung des Postbank eSafe (digitales Postfach und Schließfach[1])

Stand: 10/2022

Präambel

Kunden der Postbank (im Folgenden Bank) haben die Möglichkeit, im Online-Banking den eSafe zu nutzen. Der eSafe besteht aus zwei Bausteinen, zum einen dem digitalen Postfach und zum anderen dem digitalen Schließfach[1]. Das digitale Postfach nutzt die Bank, um dem Kunden Bankdokumente zu kommen zu lassen, die der Kunde dann in digitaler Fassung abrufen und speichern kann. Das Postfach dient der Kommunikation zwischen Bank und Kunden. Im digitalen Schließfach[1] hat der Kunde die Möglichkeit eigene Dokumente hochzuladen und zu verwahren, ohne dass ein Dritter auf diese zugreifen kann, vergleichbar einem Bankschließfach, nur digital.

I Allgemeine Rahmenbedingungen

1. Der eSafe

(1.1) Die Nutzung des eSafe beinhaltet die Nutzung des digitalen Postfachs (siehe Kapitel II) wie auch des digitalen Schließfachs[1] (siehe Kapitel III).

(1.2) Das digitale Postfach (im Folgenden Postfach) ist ein elektronischer Briefkasten, in dem für den Kunden bestimmte persönliche Mitteilungen der Bank (im Folgenden Bankmitteilungen) in elektronischer Form verschlüsselt und dauerhaft abrufbar eingestellt werden.

(1.3) In dem persönlichen digitalen Schließfach[1] (im Folgenden Schließfach) kann der Kunde sowohl Dokumente als auch Passwörter verschlüsselt speichern.

(1.4) Der Kunde kann den eSafe-Client[1] nutzen, um seine Dokumente und Passwörter zu synchronisieren.

(1.5) Darüber hinaus behält sich die Bank das Recht vor, den eSafe und zugehörige Funktionalitäten teilweise oder insgesamt weiterzuentwickeln, zu ändern oder zu ergänzen.

2. Aktivierung des eSafe

(2.1) Die Aktivierung des eSafe setzt einen hierauf gerichteten Antrag des zum Online-Banking angemeldeten Kunden voraus. Der Antrag kann auch im Zusammenhang mit der Beantragung des Online-Banking Zugangs, der Eröffnung einer Kundenverbindung oder einer Produkteröffnung gestellt werden.

(2.2) Die Annahme seitens der Bank erfolgt durch die Freischaltung des eSafe.

3. Voraussetzung und Zugangswege

(3.1) Der Kunde benötigt zur Nutzung des eSafe einen Internetzugang, eine gültige und üblicherweise für die Kommunikation mit Dritten verwendete E-Mail-Adresse, einen aktuellen, marktüblichen Internetbrowser, einen Zugang zum jeweiligen Online-Banking sowie ein aktives TAN-Verfahren bei der Bank.

(3.2) Als Zugangsweg steht dem Kunden insbesondere das Online-Banking über einen marktüblichen Internetbrowser zur Verfügung.

4. Zugang zum eSafe und Nutzungsrecht

(4.1) Der Zugang zum Safe setzt die Anmeldung im Online-Banking voraus.

(4.2) Der Kunde hat nach erfolgter Anmeldung das Recht, den eSafe für eigene Zwecke und im Einklang mit diesen Nutzungsbedingungen für die hierin vorgesehene Dauer zu nutzen.

5. Gewährleistung und Haftung

(5.1) Soweit dies nicht in diesen Nutzungsbedingungen ausdrücklich erklärt wird, erfolgen keine spezifischen Zusicherungen in Bezug auf die Dienste oder irgendwelche Garantien durch die Bank. Insbesondere erfolgt keine Zusage bezüglich der Inhalte, spezifischer Funktionalitäten oder deren Zuverlässigkeit, Verfügbarkeit oder Eignung der Dienste für Kundenzwecke.

(5.2) Für Störungen, insbesondere für vorübergehende, technisch bedingte Zugangsbeschränkungen zum eSafe, haftet die Bank nur bei Vorsatz und grober Fahrlässigkeit und stellt die eSafe Funktionalität lediglich in der jeweils aktuellen Form bereit.

(5.3) Der eSafe ist üblicherweise entsprechend der Online-Banking Funktionalität und vorbehaltlich üblicher Wartungsfenster ständig verfügbar, es besteht jedoch kein Anspruch hierauf. Soweit aus technischen Gründen ausnahmsweise Wartungsarbeiten mit Auswirkungen auf die eSafe Funktionalität erforderlich werden, wird die Bank nach Möglichkeit rechtzeitig im Online-Banking darüber informieren.

(5.4) Für die Anbindung an das Internet und zugehöriger Netzverbindung auf Kundenseite trägt der Kunde selbst Sorge. Im Falle länger anhaltender Störungen kann die Bank für Bankmitteilungen andere Kommunikationswege (z. B. postalischer Versand) nutzen.

6. Kündigung durch den Kunden

(6.1) Der Kunde kann den eSafe jederzeit ohne Angabe von Gründen kündigen. Eine Kündigung kann auch im Online-Banking erfolgen.

(6.2) Die Folgen der Kündigung sind in den Kapiteln II 4 für das Postfach und in III 5 für das Schließfach[1] näher erläutert.

7. Datenschutz

Die Bank verarbeitet die personenbezogenen Daten des Kunden im Rahmen der geltenden Datenschutzgesetze ausschließlich zu den oben unter Ziffer 1 genannten Zwecken.

8. Ergänzende Geltung der Allgemeinen Geschäftsbedingungen

Ergänzend gelten die Allgemeinen Geschäftsbedingungen und Sonderbedingungen der Bank, die in den Geschäftsräumen der Bank oder unter https://www.postbank.de/agb eingesehen werden können und dem Kunden auf Wunsch zur Verfügung gestellt werden.

1) Die eSafe-Funktionen „digitales Schließfach“ und „eSafe-Client“ bietet die Bank derzeit noch nicht an. Die diesbezüglichen Regelungen dieser Bedingungen treten in Kraft, wenn die Bank diese Funktionen anbietet und der Kunde sie nutzt.

II Digitales Postfach

1. Leistungsangebot und -umfang

(1.1) Im Postfach werden dem Kunden Bankmitteilungen (z. B. Kontoauszüge, Rechnungsabschlüsse, Wertpapierdokumente, Kreditkartenabrechnungen etc.) in elektronischer Form eingestellt.

(1.2) Der Kunde kann sich die Bankmitteilungen dauerhaft online ansehen, diese herunterladen oder löschen. Das Löschen einer Mitteilung erfolgt durch den Kunden und ist endgültig.

(1.3) Die Nutzung des Postfachs ist ausschließlich dem Kunden selbst und den von ihm hierzu berechtigten Personen vorbehalten.

(1.4) Bei dem Eingang von Bankmitteilungen wird der Kunde mindestens einmal täglich hierüber an die von ihm mitgeteilte E-Mail-Adresse benachrichtigt.

2. Einstellung von Bankmitteilungen

(2.1) Die Bank kommt ihrer Verpflichtung zur Übermittlung, Unterrichtung oder Zurverfügungstellung von Bankmitteilungen auf einem dauerhaften Datenträger durch deren Einstellung in das Postfach nach.

(2.2) Mit der Einrichtung des Postfachs ist der Kunde nach Maßgabe dieser Bedingungen ausdrücklich damit einverstanden, dass kein postalischer Versand der in das Postfach einzustellenden Bankmitteilungen stattfindet. Hiervon umfasst sind Bankmitteilungen sowohl für aktuelle als auch für zukünftig vom Kunden gewählte Bankleistungen, insbesondere auch diejenigen, die der Textform unterliegen. Die Bestimmung unter Nr. I.5 bleibt unberührt.

(2.3) Die Bankmitteilungen gehen dem Kunden spätestens einen Tag nach dem Zeitpunkt zu, in dem die Bank die Mitteilungen in das Postfach eingestellt hat und den Kunden über den Eingang für ihn wichtiger Bankmitteilungen per E-Mail informiert hat.

(2.4) Kann die E-Mail-Benachrichtigung nicht zugestellt werden (z. B. E-Mail-Adresse nicht mehr gültig), wird die Bank den Kunden kontaktieren. Die Bankmitteilungen können papierhaft zur Verfügung gestellt werden. Ein hierfür ggf. anfallendes Entgelt ergibt sich aus dem Preis- und Leistungsverzeichnis der Bank.

3. Speicherung der Bankmitteilungen

(3.1) Die Bank speichert die eingestellten Bankmitteilungen während der Gesamtdauer der Nutzung des Online-Bankings durch den Kunden im Rahmen einer bestehenden Konto- oder Depotverbindung.

(3.2) Die Bank stellt die Unveränderbarkeit der in das Postfach eingestellten und dort gespeicherten Bankmitteilungen im Rahmen einer bestehenden Konto- oder Depotverbindung sicher.

(3.3) Die Bank ist innerhalb der gesetzlichen Aufbewahrungsfristen jederzeit in der Lage, dem Kunden auf dessen Anforderung eine papierhafte Ausfertigung dieser Bankmitteilungen zur Verfügung zu stellen. Ein hierfür ggf. anfallendes Entgelt ergibt sich aus dem Preis- und Leistungsverzeichnis der Bank.

4. Folgen der Kündigung

(4.1) Die Bank wird dem Kunden die für das Postfach vorgesehenen Bankmitteilungen nach Kündigung des eSafe auf einem vereinbarten oder neu zu vereinbarenden Weg zukommen lassen. Ein hierfür ggf. anfallendes Entgelt ergibt sich aus dem Preis- und Leistungsverzeichnis der Bank.

(4.2) Die bis zu diesem Zeitpunkt in das Postfach eingestellten Bankmitteilungen bleiben für den Kunden weiterhin abrufbar. Hierfür benötigt der Kunde weiterhin eine gültige E-Mail-Adresse, einen aktuellen, marktüblichen Internetbrowser, einen Zugang zum jeweiligen Online-Banking sowie ein aktives TAN-Verfahren bei der Bank.

5. Folgen der Beendigung der Geschäftsbeziehung

(5.1) Bei Beendigung der Geschäftsbeziehung bzw. Schließung des Online-Banking Zugangs werden die zu diesem Zeitpunkt im Postfach eingestellten Bankmitteilungen – sofern noch nicht vom Kunden gelöscht – für einen Zeitraum von vier Jahren weiterhin über einen Download-Link zur Verfügung gestellt. Die Frist beginnt mit Schluss des Jahres, in der die Geschäftsbeziehung beendet bzw. das Online-Banking geschlossen wurde.

(5.2) Der Link wird dem Kunden per E-Mail zugesendet. Ein entsprechendes Passwort, welches den Zugriff des Kunden auf den Link legitimiert, wird dem Kunden auf postalischem Weg zur Verfügung gestellt.

6. Anerkennung durch Finanzbehörden

(6.1) Die im Postfach bereitgestellten Bankmitteilungen, wie z. B. der elektronische Kontoauszug oder Rechnungsabschluss, erfüllen nach Auffassung der Finanzverwaltung weder die Anforderungen der steuerlichen Aufbewahrungspflicht nach § 147 AO noch die einer Rechnung im Sinne des Umsatzsteuergesetzes.

(6.2) Diese Bankmitteilungen werden daher nur im Privatkundenbereich und damit nur für den Kontoinhaber anerkannt, der nicht buchführungs- und aufzeichnungspflichtig i. S. d. §§ 145 ff. AO ist.

(6.3) Die Bank gewährleistet nicht, dass die Finanzbehörden die im Posteingang gespeicherten Informationen anerkennen. Der Kunde sollte sich darüber vorher bei dem für ihn zuständigen Finanzamt informieren.

III Digitales Schließfach[1]

1. Leistungsangebot und -umfang

(1.1) Im Schließfach[1] kann der Kunde sowohl Dokumente grundsätzlich jedes gängigen Dateityps als auch Passwörter elektronisch speichern.

(1.2) Der Kunde erhält mit der Aktivierung des eSafe einen kostenfreien digitalen Online-Speicher als virtuelle Schließfachvariante.

(1.3) Darüber hinaus kann der Kunde zwischen verschiedenen kostenpflichtigen Schließfachvarianten wählen, die sich im Leistungsumfang (bspw. der Speicherkapazität) unterscheiden. Einzelheiten ergeben sich aus dem Preis- und Leistungsverzeichnis der Bank. Im Rahmen der zugewiesenen Speicherkapazität kann der Kunde seine elektronischen Daten hochladen und abspeichern. Die Obergrenze für das einzelne hochgeladene Dokument beträgt 2 Gigabyte (GB).

(1.4) Der Kunde kann die Schließfachvariante zu jeder Zeit ändern, sofern die Voraussetzung für die neu gewählte Schließfachvariante vorliegt.

2. Verfügungen über den Inhalt des Schließfachs[1]

(2.1) Das Schließfach[1] ist für die ausschließliche und persönliche Nutzung des Kunden als eine Einzelperson bestimmt. Eine Bevollmächtigung Dritter ist ausgeschlossen.

(2.2) Der Kunde kann die von ihm im Schließfach[1] gespeicherten Daten jederzeit herunterladen.

(2.3) Der Kunde kann seine Dokumente und Passwörter jederzeit löschen. Dokumente werden beim Löschen in den Papierkorb verschoben. Wenn der Kunde diese Dokumente endgültig löschen möchte, muss er diese im Papierkorb löschen. Die im Papierkorb abgelegten Dokumente werden bis zum endgültigen Löschen auf die Speicherkapazität angerechnet. Passwörter werden direkt endgültig gelöscht.

3. Verantwortlichkeit für die im Schließfach[1] gespeicherten Daten

(3.1) Die Bank hat keinen Zugang zum Schließfach[1] und somit keinen Zugriff auf die Daten des Kunden. Die Bank erhält keine Kenntnis vom Inhalt des Schließfachs[1]. Der Kunde hat sicherzustellen, dass im Schließfach[1] keine elektronischen Zahlungsmittel (bspw. Bitcoins) abgelegt sind und die in seinem Schließfach[1] gespeicherten Daten nicht gegen Rechte Dritter (insbesondere das allgemeine Persönlichkeitsrecht, Veröffentlichungsrechte, Rechte am geistigen Eigentum und Urheberrechte) verstoßen.

(3.2) Sämtliche Rechte an den gespeicherten Daten verbleiben beim Kunden.

(3.3) Macht ein Dritter gegenüber der Bank eine Rechtsverletzung durch Inhalte des Schließfachs[1] geltend oder liegt ein hinreichend begründeter Verdacht einer Straftat vor, ist die Bank berechtigt, die entsprechenden Inhalte des Schließfachs[1] bis zur Klärung dieses Vorfalls vorläufig zu sperren. Die Bank behält sich in diesem Fall weitere Rechte einschließlich eines sofortigen Kündigungsrechts des Schließfachs[1] vor und wird im Falle eines berechtigten Herausgabeanspruchs oder einer verbindlichen Anordnung durch Behörden oder Gerichte entsprechende Inhalte des Schließfachs[1] übermitteln.

4. Entgelt und Abrechnungszeitraum

(4.1) Das vom Kunden ggf. zu entrichtende Entgelt bestimmt sich nach der jeweils vom Kunden gewählten kostenpflichtigen Produktvariante. Die einzelnen Konditionen werden dem Kunden vor Auswahl einer kostenpflichtigen Produktvariante angezeigt und ergeben sich aus dem Preis- und Leistungsverzeichnis der Bank.

(4.2) Die Abrechnung erfolgt monatlich (Abrechnungszeitraum). Der Abrechnungszeitraum beginnt an dem Tag des ersten Vertragsabschlusses.

5. Folgen der Kündigung

(5.1) Der Kunde hat mit der Kündigung der kostenpflichtigen Schließfachvariante weiterhin Zugriff auf sein Schließfach[1] und die darin gespeicherten Daten. Hierfür benötigt der Kunde weiterhin einen aktuellen, marktüblichen Internetbrowser, einen Zugang zum jeweiligen Online-Banking sowie ein aktives TAN-Verfahren bei der Bank.

(5.2) Neue, geänderte Dokumente und Passwörter können nur eingestellt werden, wenn der tatsächlich genutzte Speicherbereich unter den Vorgaben der kostenfreien Produktvariante liegt.

(5.3) Bereits getätigte Zahlungen für eine kostenpflichtige Produktvariante werden ab dem Zeitpunkt der Kündigung anteilig zurückerstattet.

6. Folgen der Beendigung der Geschäftsbeziehung

Bei Beendigung der Geschäftsbeziehung bzw. Schließung des Online-Banking Zugangs ist der Kunde dafür verantwortlich, dass die im Schließfach[1] gespeicherten Daten rechtzeitig vor Schließung des Online-Banking Zugangs heruntergeladen werden. Hierfür benötigt der Kunde weiterhin einen aktuellen, marktüblichen Internetbrowser, einen Zugang zum jeweiligen Online-Banking sowie ein aktives TAN-Verfahren bei der Bank.

1) Die eSafe-Funktionen „digitales Schließfach“ und „eSafe-Client“ bietet die Bank derzeit noch nicht an. Die diesbezüglichen Regelungen dieser Bedingungen treten in Kraft, wenn die Bank diese Funktionen anbietet und der Kunde sie nutzt.