COMMERZBANK

Vertretungsberechtigungen, Bankvollmachten und Unterschriftsproben

mit Digital Banking Vereinbarung für den/die Bevollmächtigte/n

IBAN
(Pflichtfeld)*: _____

(22-stellig, bitte ohne Leerzeichen eingeben)

Hinweis: Diese Vollmacht gilt für alle bestehenden und künftigen Konten und Depots Ihrer mit der obigen IBAN verknüpften Kundennummer (entspricht Ziff. 14 – 20 der IBAN)

An

Commerzbank AG
Kaiserstraße 16
60282 Frankfurt

Diese Vollmacht gilt für rechtsfähige Stiftungen

Hinweis: Sofern **gesetzliche Vertreter** Ihres Unternehmens eine Vertretungsberechtigung erhalten, muss für jede Kundennummer ein eigenes Formular „Vertretungsberechtigungen, Bankvollmacht und Unterschriftsproben“ ausgefüllt werden!

Kundenbezeichnung

_____

_____

I. Vertretungsberechtigung und Vollmacht

Personendaten des/der Bevollmächtigten (gemäß Legitimationsdokument – Kopie beifügen):

Hinweis: Die mit * gekennzeichneten Felder sind Pflichtfelder

Anrede* ☐ Frau ☐ Herr ☐ An

Titel _____

Vorname(n)* _____

Nachname* _____

Geburtsname (falls abweichend)* _____

Geburtsdatum* _____ Geburtsort* _____

Geburtsland* _____ Staatsangehörigkeit*[2] _____

Steuer-Identifikationsnummer (deutsch)[1] _____

1) **Die Angabe der Steuer-Identifikationsnummer (Steuer-ID) in diesem Dokument ist freiwillig und kann zu einem späteren Zeitpunkt auch direkt durch den/die Bevollmächtigte/n erfolgen.**
2) **Sofern die/der Bevollmächtigte nicht Bürger/in eines EU-Landes ist und diese/r in Deutschland wohnt, muss zusammen mit der Vollmachtunterlage eine Kopie des Aufenthaltstitels eingereicht werden.**

1523/12/31 – HD0724-01

Vertretungsberechtigungen, Bankvollmachten und Unterschriftsproben

mit Digital Banking Vereinbarung für den/die Bevollmächtigte/n

IBAN
(Pflichtfeld)*: _____

(22-stellig, bitte ohne Leerzeichen eingeben)

Meldeadresse des/der Bevollmächtigten (gemäß Legitimationsdokument)

Hinweis: Die mit * gekennzeichneten Felder sind Pflichtfelder

Straße* _____ Hausnummer _____

PLZ* _____ Ort* _____

Land* _____

E-Mail-Adresse und Mobilfunknummer für das Legitimationsverfahren per videoIDENT

Mobilfunknummer[3] _____

E-Mail-Adresse[3] _____

3) Wenn sich der/die Bevollmächtigte später per videoIDENT-Verfahren legitimieren will, sind E-Mail-Adresse und Mobilnummer Pflichtangaben; diese Informationen werden allerdings nicht zu werblichen Zwecken genutzt. Ohne diese elektronischen Kontaktdaten wird die Legitimation per PostIdent-Verfahren durchgeführt.

Rolle/Funktion/Dienststellung des/der Bevollmächtigten (zutreffendes bitte ankreuzen)

☐ 1. Im Stiftungsregister eingetragene/r gesetzliche/r Vertreter/in (Vorstandsmitglied)
(bitte beglaubigte Kopie (Stiftungs-)Register bzw. Vertretungsbescheinigung Genehmigungsbehörde/Bestellungsausschuss beifügen, sofern zur Hand)

Hinweis: Alle Abweichungen vom Sitftungsregister müssen von dem/r gesetzlichen Vertreter/in genehmigt werden, der/die in dem Fall das Formular gemäß seiner/ihrer Eintragung im Stiftungsegister unterschreibt.

☐ 2. Sonstige, vertretungsberechtigte Person (z. B. Beiratsmitglied o. ä.)

Umfang der Vertretungsberechtigung

Die nachstehend genannte Person ist berechtigt, uns gegenüber der Bank gemäß den in den Wahlmöglichkeiten gesetzten Kreuzen wie folgt zu vertreten:

☐ **E** = Einzeln

☐ **A** = Allgemein, d. h. gemeinschaftlich vertretungsberechtigt mit einem Vertretungsberechtigten der Klasse „E“ oder „A“

Vertretungsberechtigungen, Bankvollmachten und Unterschriftsproben

mit Digital Banking Vereinbarung für den/die Bevollmächtigte/n

IBAN
(Pflichtfeld)*: _____

(22-stellig, bitte ohne Leerzeichen eingeben)

II. Anmeldung zur Teilnahme am Digital Banking

Für den/die Bevollmächtigte/n werden alle bestehenden und zukünftigen Konten und Depots unter meiner Kundennummer für das Digital Banking freigeschaltet.

Authentifizierung und Autorisierung

Zur Authentifizierung des Teilnehmers und zur Autorisierung seiner Willenserklärungen werden folgende Verfahren vereinbart:

– Für das Telefon Banking: PIN und mündliche Zustimmung
– Für das Online Banking: PIN und photoTAN mit photoTAN-App oder photoTAN-Lesegerät

☐ Bitte stellen Sie der/dem Bevollmächtigten ein photoTAN-Lesegerät zur Verfügung. Die Kosten für das Lesegerät in Höhe von 29,90 Euro inkl. MwSt. und Versand werden meinem in der Kopfzeile dieses Formulars aufgeführten Girokonto belastet. Als Rechnung dient die Umsatzanzeige auf dem Kontoauszug. Bis zur vollständigen Bezahlung des Kaufpreises bleibt die Ware Eigentum der Bank. Versand und Reklamationsvereinbarung erfolgen durch die Bank-Verlag GmbH, Wendelinstraße 1, 50933 Köln.

Den Aktivierungsbrief für das photoTAN-Verfahren und die Teilnehmernummer sendet die Commerzbank dem/der Bevollmächtigten zu. Sofern der/die Bevollmächtigte das photoTAN-Verfahren nicht innerhalb von 180 Tagen aktiviert, wird dieses wieder deaktiviert. Eine spätere Anmeldung ist jederzeit möglich.

Sofern keine anders lautenden Limite zur Kundennummer vereinbart sind, gelten für das Online Banking die folgenden Standardlimite: 10.000 Euro pro Auftrag im Inlandszahlungsverkehr, 5.000 Euro im Auslandszahlungsverkehr, 10.000 Euro pro Auftrag im Wertpapiergeschäft (max. 50.000 Euro pro Tag). Ein anderer Nutzungsumfang kann separat pro Kundennummer festgelegt werden. Zukünftige Konten und Depots werden automatisch im Online Banking mit den vereinbarten Limiten pro Kundennummer freigeschaltet.

Aufzeichnung von Telefongesprächen und elektronischer Kommunikation

Die Commerzbank ist berechtigt, telefonisch erteilte Aufträge und Anfragen zum Zwecke der Beweissicherung aufzuzeichnen. Die Aufzeichnungen werden längstens für drei Monate aufbewahrt und dann gelöscht. Abweichend hierzu ist die Commerzbank bei telefonisch veranlassten Aufträgen und Anträgen mit Bezug zum Wertpapiergeschäft gesetzlich verpflichtet, alle diesbezüglichen Telefonate bzw. die elektronische Kommunikation aufzuzeichnen und diese Aufzeichnungen fünf, auf Veranlassung der zuständigen Behörde auch sieben Jahre, aufzubewahren. Erst nach Ablauf dieser gesetzlichen Aufbewahrungsfristen werden diese Aufzeichnungen gelöscht.

☐ Der/die Vollmachtgeber/in nutzt eine Finanzsoftware und benötigt das **Online Banking nach HBCI/FinTS-Standard** (Legitimation durch elektronische Signatur) für den/die Bevollmächtigte.

Sofern keine anders lautenden Limite vereinbart sind, gelten die folgenden Standardlimite: Auftragslimit pro Inlandsüberweisung (Euro) 100.000 Euro und 10.000 Euro Auftragslimit pro Auslandsüberweisung (Euro). Ein anderer Nutzungsumfang kann separat festgelegt werden. Die Freischaltung weiterer Konten, Kreditkarten, Depots und Kredite kann separat im Online Banking oder über das Beratungscenter beauftragt werden.

Bei der Nutzung von FinTS/HBCI erfolgt die Legitimation und Transaktionsautorisierung aller Datenübertragungen mittels einer elektronischen Signatur, die der/die Bevollmächtigte auf einem Datenträger (HBCI-Signaturchipkarte oder USB-Stick) gespeichert haben muss.

Vertretungsberechtigungen, Bankvollmachten und Unterschriftsproben

mit Digital Banking Vereinbarung für den/die Bevollmächtigte/n

IBAN
(Pflichtfeld)*: _____

(22-stellig, bitte ohne Leerzeichen eingeben)

III. Umfang der Vertretungsberechtigung und/oder Vollmacht

Vertretungsberechtigung und Bankvollmacht

Die in Abschnitt I aufgeführte Vertretungsberechtigung und erteilte Bankvollmacht gilt für alle bestehenden und künftigen Konten und Depots des Kunden, die unter der oben genannten Kundennummer geführt werden, sofern nicht etwas Abweichendes mitgeteilt wird.

Der Abschluss und die Änderung von Kredit- und Sicherheitenverträgen sind von dieser Vollmacht nicht umfasst. Sie bleiben den gesetzlich Vertretungsberechtigten vorbehalten.

Die in Abschnitt I genannte Person kann (einzeln oder gemeinsam) alle Handlungen im Geschäftsverkehr, die mit der Konto- und Depotführung in unmittelbarem Zusammenhang stehen, mit der Commerzbank AG vornehmen.

Eine Handlungs- oder Bankvollmacht berechtigt nicht zur Erteilung von Untervollmachten. Sie berechtigt ferner nicht zum Abschluss von Derivategeschäften nach § 2 Abs. 3 Wertpapierhandelsgesetz (WpHG).

IV. Sonstiges

Anerkennung von Schriftstücken

Die in Abschnitt I genannte Person ist berechtigt, im Zusammenhang mit den betreffenden Geschäften erteilte Bestätigungen, Abrechnungen, Kontoauszüge, Aufstellungen und sonstige Schriftstücke zu oben genannter Kundennummer für den Kunden entgegenzunehmen, zu prüfen und anzuerkennen.

Mitteilungspflichten

Zur ordnungsgemäßen Abwicklung des Geschäftsverkehrs ist es erforderlich, dass der Kunde der Commerzbank AG Änderungen seines Namens und seiner Anschrift, sowie das Erlöschen oder die Änderung gegenüber der Commerzbank AG erteilter Vertretungsberechtigungen und/oder Vollmachten zu oben genannter Kundennummer unverzüglich und aus Beweisgründen möglichst schriftlich mitteilt. Diese Mitteilungspflicht besteht auch dann, wenn die Vertretungsberechtigung in ein öffentliches Register (z. B. in das Handelsregister) eingetragen ist und ihr Erlöschen oder ihre Änderung in dieses Register eingetragen wird. Darüber hinaus können sich weitergehende gesetzliche Mitteilungspflichten, insbesondere aus dem Geldwäschegesetz, ergeben.

Beendigung, Änderungen und Widerruf der Vertretungsberechtigungen oder Vollmachten

Die Beendigung der Vertretungsberechtigung eines gesetzlichen Vertreters erfolgt durch Vorlage eines schriftlichen Stiftungsprotokolls, spätestens aber mit Eintragung im (Stiftungs-)Register und der Vorlage eines entsprechenden Registerauszugs bei der Commerzbank AG.

Gemäß dem im (Stiftungs-)Register aufgeführten Umfang der Vertretungsberechtigung (einzeln oder gemeinsam), dürfen gesetzliche Vertreter die Vertretungsberechtigungen für unter Ziffer 2 aufgeführte Personen (formfrei, aus Beweisgründen möglichst schriftlich) verändern oder widerrufen.

Der Widerruf dieser Vollmacht durch einen Vertragspartner lässt alle anderen Vollmachten im Verhältnis zur Bank unberührt.

Rechtswahl, Gerichtsstand

Für diese Vertretungsberechtigung, Vollmacht und Unterschriftenprobe gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Frankfurt am Main, Bundesrepublik Deutschland.

Geschäftsbedingungen und Datenschutz

Ergänzend zu den bisher vereinbarten allgemeinen und produktbezogenen Geschäftsbedingungen gelten die Digital Banking Bedingungen der Commerzbank AG. Die Hinweise zum Datenschutz (siehe www.commerzbank.de/datenschutzhinweise) sind zu beachten.

1523/12/31 – HD0724-01

Vertretungsberechtigungen, Bankvollmachten und Unterschriftsproben

mit Digital Banking Vereinbarung für den/die Bevollmächtigte/n

IBAN
(Pflichtfeld)*: _____

(22-stellig, bitte ohne Leerzeichen eingeben)

Unterschrift(en) und Stempel von lt. Stiftungsverzeichnis gesetzlich zur Vertretung berechtigter Person(en)[4]

Ort, Datum _____ _____

Als Vollmachtgeber/in erteile(n) ich/wir die Vollmacht und beantragen die Teilnahme am Digital Banking für den/die Bevollmächtigte(n) wie oben angegeben.

Unterschrift(en) und Stempel _____

Name(n) aller Unterzeichner in Klarschrift _____

Unterschrift Bevollmächtigte/r

Ort, Datum _____ _____

Die beigefügten Digital Banking Bedingungen der Commerzbank AG habe ich zur Kenntnis genommen.

Unterschrift (gilt gleichzeitig als Unterschriftsprobe) _____

Name Unterzeichner in Klarschrift _____

4) Das Formular ist stets entsprechend den Regelungen im (Stiftungs-)Registereintrag oder in der Vertretungsbescheinigung einer Genehmigungsbehörde/ Bestellungsausschuss (Einzel- oder Gesamtvertretung) zu unterschreiben. Einschränkend gilt, dass bei Erfassungen unter Abschnitt I, Ziffer 1 in jedem Fall gesetzliche Vertreter (Vorstandsmitglied/er) das Formular unterschreiben müssen.

Hinweis: Bei der Erfassung von gesetzlichen Vertretern (Abschnitt I, Ziffer 1 muss/müssen immer ein oder mehrere gesetzliche/r Vertreter (Vorstandsmitglied/er) das Formular gemäß der für ihn/sie geltenden Regelungen im (Stiftungs-)Registereintrag oder in der Vertretungsbescheinigung einer Genehmigungsbehörde/Bestellungsausschuss unterschreiben.

1523/12/31 – HD0724-01

Digital Banking Bedingungen

(Stand: 01.06.2024)

1. Leistungsangebot

(1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels Online Banking und Telefon Banking (beides zusammen „Digital Banking") in dem von der Bank angebotenen Umfang abwickeln. Für die Abwicklung gelten die Bedingungen für die jeweiligen Bankgeschäfte (z. B. Allgemeine Bedingungen für Zahlungsdienste, Sonderbedingungen für Wertpapiergeschäfte nebst den Ausführungsgrundsätzen). Zudem können sie Informationen der Bank mittels Digital Banking abrufen. Des Weiteren sind sie gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absätze 33 und 34 Zahlungsdiensteaufsichtsgesetz (ZAG) zu nutzen. Die Bank ist berechtigt, dem Kunden die Änderung ihrer Geschäftsbedingungen auf elektronischem Weg anzuzeigen und zum Abruf bereitzustellen. Wegen des Wirksamwerdens der Änderungen verbleibt es bei der Regelung in Nummer 1 Abs. 2 der Allgemeinen Geschäftsbedingungen oder den mit dem Kunden vereinbarten abweichenden Regelungen.

(2) Kunde und Bevollmächtigte werden einheitlich als „Teilnehmer", Konto und Depot einheitlich als „Konto" bezeichnet, es sei denn dies ist ausdrücklich anders bestimmt.

(3) Zur Nutzung des Digital Banking gelten die Standardlimite oder die mit der Bank gesondert vereinbarten Verfügungslimite für das Digital Banking.

2. Voraussetzungen zur Nutzung des Digital Banking

(1) Der Teilnehmer kann das Digital Banking nutzen, 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 vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers prüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummern 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen

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

3. Zugang zum Online Banking

(1) Der Teilnehmer erhält Zugang zum Online Banking der Bank, wenn
- er seine individuelle Teilnehmernummer (z. B. Kontonummer, Anmeldename) angibt und
- er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (siehe Nummern 10.1 und 11 dieser Bedingungen) vorliegt. Nach Gewährung des Zugangs zum Online Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge erteilt werden.

(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Abs. 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 Authentifizierungselements 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 Zahlungsdaten (§ 1 Abs. 26 Satz 2 ZAG).

4. Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss einen Auftrag (zum Beispiel Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (zum Beispiel Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden. Die Bank bestätigt den Eingang des Auftrags.

4.2 Meldung nach AWV

Bei Zahlungen zugunsten Gebietsfremder ist die Meldung gemäß Außenwirtschaftsverordnung (AWV) zu beachten.

4.3 Widerruf von Aufträgen

Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Allgemeine Bedingungen für Zahlungsdienste, Sonderbedingungen für Wertpapiergeschäfte nebst den Ausführungsgrundsätzen). Der Widerruf von Aufträgen kann nur außerhalb des Online Bankings erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Online Banking ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der Aufträge erfolgt nach den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung oder Wertpapierauftrag) geltenden Regelungen.

(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 (zum Beispiel Wertpapierorder) liegt vor.
- Das Online Banking Datenformat ist eingehalten.
- Das gesondert vereinbarte Digital Banking Verfügungslimit oder das Standardlimit ist nicht überschritten (vgl. Nummer 1 Absatz 3 dieser Bedingungen).
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Allgemeinen Bedingungen für Zahlungsdienste) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel gemäß den Allgemeinen Bedingungen für Zahlungsdienste) aus. Die Ausführung darf nicht gegen sonstige Rechtsvorschriften verstoßen.

(3) Liegen die Ausführungsbedingungen nach Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird dem Teilnehmer hierüber mittels Online Banking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können. Dies gilt nicht, wenn die Angabe von Gründen gegen sonstige Rechtsvorschriften verstößt. Führt die Bank den Auftrag aus, obwohl keine Kontodeckung vorhanden ist, entsteht eine geduldete Kontoüberziehung, für die ein vereinbarter Zins zu zahlen ist.

6. Telefon Banking

Der Teilnehmer erhält Zugang zum Telefon Banking, wenn
- dieser sich unter der ihm mitgeteilten Rufnummer für das Telefon Banking durch Eingabe von Teilnehmernummer und PIN über die Telefontastatur oder mittels photoTAN-App authentifiziert hat. Alternativ kann der Zugang durch einen Anruf des Kunden über die Commerzbank Banking App erfolgen.
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs vorliegt.

Nach Gewährung des Zugangs zum Telefon Banking kann der Teilnehmer Informationen erfragen oder Bankgeschäfte vereinbaren.

Der Teilnehmer erteilt seine Zustimmung und autorisiert eine Vereinbarung im Rahmen des Telefon Bankings durch mündliche Bestätigung oder Bestätigung per photoTAN-App

1523/12/31 – HD0724-01

7. Information des Kunden über Digital Banking Verfügungen

Die Bank unterrichtet den Kunden mindestens einmal monatlich über die mittels Digital Banking getätigten Verfügungen im Zahlungsverkehr oder bei Wertpapiergeschäften auf dem für Konto- und Depotinformationen vereinbarten Weg und gemäß den für den Auftrag geltenden Bedingungen.

8. Sorgfaltspflichten des Teilnehmers

8.1 Schutz der Authentifizierungselemente

(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungelemente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Digital Banking Verfahren 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 mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden
- nicht außerhalb des Digital Banking in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben werden
- nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. mobiles Endgerät) oder zur Prüfung des Seinselementes (z. B. mobiles Endgerät mit Anwendung für das Digital Banking und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z. B. ein mobiles Endgerät sind vor Missbrauch zu schützen. Dabei
- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät (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 Digital Banking (z. B. Commerzbank-Banking-App, Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für das Digital Banking (z. B. Commerzbank-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 oder Entsorgung des Mobiltelefons),
- dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Digital Bankings 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 Digital Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr 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 Digital 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 Digital Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Digital Banking das von der Bank ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Ungeachtet der Schutzpflichten nach den Absätzen 1 und 2 darf der Teil nehmer seine Authentifizierungselemente gegenüber einem von ihm aus gewählten Zahlungsauslösedienst und Kontoinformationsdienst verwenden (siehe Nummer 1 Absatz 1 dieser Bedingungen).

(4) Die App der Bank oder das Lesegerät zur Entschlüsselung der TAN-Grafik ist direkt von der Bank oder von einem von der Bank dem Kunden benannten Anbieter zu beziehen.

(5) Sofern PIN und die Teilnehmernummer vom Telefon des Teilnehmers automatisch gespeichert werden (z. B. Wahlwiederholungsfunktion des Telefons), sind, soweit technisch möglich, die gespeicherten Ziffernfolgen zu löschen oder zu überschreiben.

8.2 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise auf der Digital Banking-Seite der Bank, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

8.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (zum Beispiel mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

9. Ein- und Ausfuhr von Software im Ausland

In Ländern, in denen Nutzungs- oder Einfuhr- und Ausfuhrbeschränkungen für Verschlüsselungstechniken bestehen, darf eine von der Bank zur Verfügung gestellte Software nicht verwendet werden.

10. Anzeige und Unterrichtungspflichten

10.1 Sperranzeige

(1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. mobiles Endgerät) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungselements

fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann eine solche 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.

10.2 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.

11. Nutzungssperre

11.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 10.1 dieser Bedingungen,
- den Digital Banking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument zur Nutzung des Digital Banking.

11.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Digital Banking-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, den Digital Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungselements des Teilnehmers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des eines Authentifizierungselements besteht.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre schriftlich, in Textform (z. B. mittels, Telefax oder E-Mail) oder telefonisch unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

11.3 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.

11.4 Automatische Sperre eines chip-basierten Besitzelements sowie des Digital Banking-Zugang mittels PIN und TAN

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

(2) Wenn der Kontrollwert zur Freigabe der HBCI-Signatur dreimal falsch eingegeben wird, kommt es zur Sperrung der übermittelten Signatur. Der Teilnehmer muss eine neue elektronische Signatur erstellen und diese erneut an die Bank übermitteln.

(3) Die dreimalige Falscheingabe des PIN führt zu einer Sperre des Digital Banking-Zugangs.

(4) Das im Absatz 1 genannte Besitzelement kann dann nicht mehr für das Digital Banking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Digital Banking wiederherzustellen.

11.5 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.

12. Haftung[1]

12.1 Haftung der Bank bei Ausführung eines nicht autorisierten Digital Banking Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Bank bei einem nicht autorisierten Auftrag und einer nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich vorrangig nach Nummer 12.2 und nachrangig nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Allgemeine Bedingungen für Zahlungsdienste, Sonderbedingungen Wertpapiergeschäfte nebst den Ausführungsgrundsätzen).

12.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

12.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge 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 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach dem 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 Zahlungsvorgang zu 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 Sorgfalts- und Anzeigepflichten 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 8.1 Absatz 2
- Nummer 8.1 Absatz 4
- Nummer 8.1 Absatz 6
- Nummer 8.3 oder
- Nummer 10.1 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 im Sinne von § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Sein (siehe Nummer 2 Absatz 3 dieser Bedingungen).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Standardlimit oder das mit dem Kunden vereinbarte Digital Banking-Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf diese Limite.

(6) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz (1) und (3) verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 10.1 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 gelten nicht, 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 Euro in Absatz (1) und (3) hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- Die Haftungsbeschränkungen in Absatz (2) erster Spiegelstrich finden keine Anwendung.

12.2.2 Haftung des Kunden 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.

12.2.3 Haftung ab der Sperranzeige

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

12.2.4 Haftung beim Telefon Banking

Bis zur Sperranzeige haftet der Kunde außer in den Fällen nach Absatz 12.1 und 12.2 nach den rechtlichen Regelungen für vorsätzliches und fahrlässiges Verhalten unter Berücksichtigung eines eventuellen Mitverschuldens der Bank.

12.2.5 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.

13. Datenschutz

Die Verarbeitung personenbezogener Daten im Rahmen des Commerzbank Digital Banking erfolgt jeweils im Rahmen und unter Beachtung der geltenden anwendbaren datenschutzrechtlichen Vorschriften. Beachten Sie in diesem Zusammenhang bitte die nachfolgenden Datenschutzhinweise der Commerzbank AG (https://www.commerzbank.de/hinweise/datenschutz-hinweise/).

Commerzbank AG

[1] Ergänzend gelten die Regelungen der Sicherheits-Garantie der Bank.