COMMERZBANK
Die Bank an Ihrer Seite

Bedingungen für die Abwicklung von Bankgeschäften über das Firmenkundenportal und HBCI/FinTS-Service

(Stand 13.01.2018)

1. Leistungsangebot

(1) Der Kunde und dessen Bevollmächtigte können das Firmenkundenportal oder den HBCI/FinTS-Service nutzen und Bankgeschäfte in dem von der Bank angebotenen Umfang abwickeln. Für die Abwicklung gelten die Bedingungen für die jeweiligen Bankgeschäfte (z. B. Firmenkundenbedingungen für Zahlungsdienste, Sonderbedingungen für Commerzbank Online Banking, Wertpapierbedingungen, Sonderbedingungen für Wertpapiergeschäfte). Zudem kann der Kunde Informationen der Bank abrufen. Der Kunde ist zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrages einen Zahlungsauslösedienst gemäß § 1 Absatz 33 Zahlungsdiensteaufsichtsgesetz und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienstleister gemäß § 1 Absatz 34 Zahlungsdiensteaufsichtsgesetz zu nutzen.

(2) Kunde und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ oder „User“ bezeichnet. Hierzu gehört auch der „Nutzer“ gemäß den Bedingungen für die Datenfernübertragung, der die Datenfernübertragung im Rahmen des Firmenkundenportals nutzt. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.

(3) Kunde und Bank können Verfügungslimits für bestimmte Servicearten gesondert vereinbaren.

2. Voraussetzungen zur Nutzung des Firmenkundenportals und des HBCI/FinTS-Service

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

2.1 Personalisierte Sicherheitsmerkmale

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

- die Persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (photoTAN) und
- die Signatur-PIN/das Kennwort und die Daten des persönlichen elektronischen Schlüssels für die elektronische Signatur.

2.2 Authentifizierungsinstrumente

Die photoTAN kann für den Teilnehmer/User mittels eines mobilen End- oder Lesegeräts generiert und ihm zur Verfügung gestellt werden. Der Teilnehmer/User kann weitere Authentifizierungsinstrumente zur Freigabe von Transaktionen nutzen:

- eine Chipkarte mit Signaturfunktion oder
- ein sonstiges Authentifizierungsinstrument, auf dem sich der Signaturschlüssel befindet, einschließlich einer Speicherung der elektronischen Schlüssel in einer von der Bank (oder einem von der Bank zugelassenen Dienstleister) zur Verfügung gestellten technischen Umgebung, die vor unautorisiertem Zugriff geschützt ist,
- eine von der Bank im Initialisierungsprozess für den Teilnehmer/User personalisierte App.

2.3 Vereinbarung der Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente

Jeder Teilnehmer/User kann mit der Bank vereinbaren, welches Personalisierte Sicherheitsmerkmal und Autorisierungsinstrument von ihm verwendet werden soll .

3. Zugang zum Firmenkundenportal

Der Teilnehmer/User erhält Zugang zum Firmenkundenportal, wenn

- dieser die Teilnehmernummer/den Anmeldenamen und die PIN übermittelt,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers/Users ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 9.1 und 10) vorliegt.

Nach Gewährung des Zugangs zum Firmenkundenportal kann der Teilnehmer/User Informationen abrufen oder Aufträge erteilen. Die Sätze 1 und 2 gelten auch, wenn der Teilnehmer Zahlungsaufträge über einen Zahlungsauslösedienst auslöst und Zahlungskontoinformationen über einen Kontoinformationsdienst anfordert (siehe Nummer 1 Absatz 1 Satz 4).

22/93/28 (01/18)
Januar 2018

4. Auftragsabwicklung

4.1 Auftragserteilung und Autorisierung
Die Autorisierung zur Durchführung einzelner Geschäfte (z. B. Überweisung, Termingeld) erfolgt – abhängig von der gewählten Serviceart – mittels der vereinbarten Personalisierten Sicherheitsmerkmale

- photoTAN,
- PIN,
- elektronische Signatur,
- biometrische Signatur bzw.
- nach Anmeldung mit Teilnehmernummer bzw. Anmeldenamen und PIN durch einfache Freigabe.

Satz 1 gilt auch, wenn der Teilnehmer einen Zahlungsauftrag über einen Zahlungsauslösedienst (siehe Nummer 1 Absatz 1 Satz 4) auslöst und übermittelt.

4.2 Ergänzende Regelungen für die Datenfernübertragung im EBICS-Standard bei Einsatz des photoTAN-Verfahrens
4.2.1 Der Kunde beauftragt die Bank mit der Speicherung des persönlichen Schlüssels des Teilnehmers/Users in einer technischen Umgebung, die vor unautorisiertem Zugriff geschützt ist. Die Bank ist berechtigt, hierfür auch einen zuverlässigen Dienstleister zu beauftragen. Das zur Freigabe des persönlichen Schlüssels erforderliche Kennwort wird durch eine TAN im photoTAN-Verfahren ersetzt.

4.2.2 Die Bedingungen für die Datenfernübertragung werden wie folgt ergänzt:

- Ergänzend zu Ziffer 4(2) der Bedingungen für die Datenfernübertragung gilt, dass die Aufbewahrung der elektronischen Schlüssel in einer von der Bank (oder von einem von der Bank zugelassenen Dienstleister) zur Verfügung gestellten technischen Umgebung (vgl. Ziffer 2.2.1, (5) der Anlage 1a der Bedingungen für die Datenfernübertragung) erlaubt ist.
- Zu Ziffer 7 (3) wird vereinbart, dass die Bank die Legitimation auch daraufhin prüft, ob die richtige photoTAN eingegeben wurde.

4.2.3 Die Anlage 1a der Bedingungen für die Datenfernübertragung wird wie folgt ergänzt:

- Die Authentifikationssignatur kann in Ziffer 1.2 beim photoTAN-Verfahren auch in der technischen Umgebung der Bank oder des zugelassenen Dienstleisters geleistet werden. Diese nehmen für den Kunden die erforderliche Prüfung vor.
- Zu Ziffer 2.2 (5) wird vereinbart, dass die photoTAN anstelle des Passwortes verwendet wird, wenn das Sicherungsmedium des Teilnehmers bankseitig in einer technischen Umgebung gespeichert ist, die vor unautorisiertem Zugriff geschützt ist.
- Die Autorisierung von Aufträgen gemäß Ziffer 3 kann auch durch Eingabe der auf dem mobilen End- oder Lesegerät angezeigten photoTAN und der daraufhin in der gesicherten technischen Umgebung erzeugten elektronischen Signatur erteilt werden.
- Bei einer Verteilten Elektronischen Signatur (VEU) gemäß Ziffer 3.1 Absatz 1 kann die Freigabe und damit die Autorisierung mit der zweiten bankfachlichen Signatur durch Verwendung der photoTAN oder durch Freigabe eines Auftrages im Rahmen der personalisierten App-Anwendung der Bank erfolgen.

4.3 Meldung nach AWV
Bei Zahlungen zugunsten Gebietsfremder ist vom Teilnehmer/User die Meldung gemäß Außenwirtschaftsverordnung (AWV) zu beachten.

4.4 Widerruf von Aufträgen
Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen. Der Widerruf von Aufträgen kann nur außerhalb des Firmenkundenportals und des HBCI/FinTS-Service erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Firmenkundenportal oder beim HBCI/FinTS-Service ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

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

(2) Für Zahlungsaufträge (Überweisung, Lastschrift) gelten folgende Sonderregelungen: Die Bank wird den Zahlungsauftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer/User hat sich mit seinem Personalisierten Sicherheitsmerkmal legitimiert.
- Die Berechtigung des Teilnehmers/Users für die jeweilige Auftragsart liegt vor.
- Das für die vereinbarte Serviceart erforderliche Datenformat ist eingehalten.
- Das für die Serviceart gesondert vereinbarte Verfügungslimit ist nicht überschritten.
- Die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen liegen vor.
- Es ist eine ausreichende Kontodeckung (Guthaben oder eingeräumter Kredit) vorhanden.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank den Zahlungsauftrag aus. Die Ausführung darf nicht gegen sonstige Rechtsvorschriften verstoßen.

(3) Liegen die Ausführungsbedingungen nach Absatz (2) Satz 1 Spiegelpunkt 1–5 nicht vor, wird die Bank den Zahlungsauftrag nicht ausführen. Die Bank wird den Teilnehmer/User über die Nichtausführung informieren 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.

22/93/28 (01/18)

6. Information des Kunden über erteilte Verfügungen

Die Bank unterrichtet den Kunden über die im Rahmen des Firmenkundenportals oder des HBCI/FinTS-Service getätigten Verfügungen auf dem für Konto- und Depotinformationen vereinbarten Weg und gemäß den für den Auftrag geltenden Bedingungen.

7. Sorgfaltspflichten des Teilnehmers/Users

7.1 Technische Verbindung

Der Teilnehmer/User ist verpflichtet, die technische Verbindung über die von der Bank gesondert mitgeteilten Zugangskanäle (z. B. Internetadresse) herzustellen. Zur Auslösung eines Zahlungsauftrags und zum Abruf von Informationen über ein Zahlungskonto kann der Teilnehmer die technische Verbindung zum Firmenkundenportal auch über einen Zahlungsauslösedienst bzw. einen Kontoinformationsdienst (siehe Nummer 1 Absatz 1 Satz 4) herstellen. Der Teilnehmer/User ist dafür verantwortlich, dass er für seine eigenen Systeme eine angemessene Datensicherung unterhält und stets nach dem Stand der Technik ausreichende Vorkehrungen gegen Viren und andere schädliche Programme (z. B. Trojaner, Würmer etc.) trifft. Apps der Bank dürfen nur von App-Anbietern bezogen werden, die die Bank dem Kunden mitgeteilt hat. Der Teilnehmer/User hat eigenverantwortlich die landesspezifischen Regelungen für die Nutzung des Internets zu beachten.

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer/User hat

- seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten sowie
- sein Authentifizierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit der Kenntnis des dazugehörigen Personalisierten Sicherheitsmerkmals das Verfahren missbräuchlich nutzen. Die Geheimhaltungspflicht bezüglich der Personalisierten Sicherheitsmerkmale nach Satz 1 gilt nicht, wenn der Teilnehmer diese zur Erteilung eines Zahlungsauftrags oder zum Abruf von Informationen über ein Zahlungskonto an den von ihm ausgewählten Zahlungsauslösedienst beziehungsweise Kontoinformationsdienst übermittelt (siehe Nummer 1 Absatz 1 Satz 4).

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

- Die Personalisierten Sicherheitsmerkmale PIN und die Signatur-PIN/das Kennwort dürfen bei einem Teilnehmer/User nicht ungesichert elektronisch gespeichert werden. Der vom Teilnehmer/User erzeugte persönliche elektronische Schlüssel darf sich nur in der alleinigen Verfügungsgewalt des Teilnehmers/Users oder in einer von der Bank (oder von einem von der Bank zugelassenen Dienstleister) zur Verfügung gestellten technischen Umgebung, die vor unautorisiertem Zugriff geschützt ist, befinden.
- Wird im Rahmen einer vollautomatisierten Übertragung ein sog. „Technischer User“ eingesetzt, ist die elektronisch gespeicherte Signatur in einer sicheren und entsprechend geeigneten technischen Umgebung zu speichern. Der „Technische User“ ist nicht berechtigt, die Auftragserteilung selbst vorzunehmen. Er übermittelt lediglich die Auftragsdaten.
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- Das Personalisierte Sicherheitsmerkmal darf nicht per E-Mail weitergegeben werden.
- Die Signatur-PIN/das Kennwort für die elektronische Signatur darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer/User darf zur Autorisierung eines Auftrags nicht mehr als eine photoTAN verwenden.

7.3 Sicherheit des Kundensystems

Der Teilnehmer/User muss die Sicherheitshinweise auf der Internetseite der Bank, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software, beachten und aktuelle, dem Stand der Technik entsprechende Virenschutz und Firewall-Systeme installieren. Insbesondere dürfen das Betriebssystem und die Sicherheitsvorkehrungen des mobilen Endgerätes nicht modifiziert oder deaktiviert werden.

7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer/User Daten aus seinem über das Firmenkundenportal erteilten Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers/Users (z. B. photoTAN-Lesegerät, photoTAN-App, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer/User verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

7.5 Weitere Sorgfaltspflichten des Kunden

Der Kunde trägt dafür Sorge, dass die Sorgfaltspflichten aus diesem Vertrag auch von dem Bevollmächtigten (also von allen Teilnehmern/Usern) eingehalten werden.

8. Verschlüsselungstechnik im Ausland

In den Ländern, in denen Nutzungs-, Einfuhr-, und/oder Ausfuhrbeschränkungen für Verschlüsselungstechniken bestehen, darf der von der Bank zur Verfügung gestellte Online-Zugang nicht genutzt werden. Gegebenenfalls hat der Teilnehmer/User die erforderlichen Genehmigungen, Anzeigen oder sonst erforderlichen Maßnahmen zu veranlassen. Der Teilnehmer/User hat die Bank über ihm bekannt gewordene Verbote, Genehmigungs- und Anzeigepflichten zu informieren.

22/93/28 (01/18)

9. Anzeige- und Unterrichtungspflichten

9.1 Sperranzeige

(1) Stellt der Teilnehmer/User

- den Verlust oder den Diebstahl des Authentifizierungsinstruments,
- die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder eines seiner Personalisierten Sicherheitsmerkmale fest, muss der Teilnehmer/User die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer/User kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilte Sperrhotline abgeben.

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

(3) Hat der Teilnehmer/User den Verdacht, dass eine andere Person unberechtigt

- den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder
- das Authentifizierungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet, muss er ebenfalls eine Sperranzeige abgeben.

9.2 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.

10. Nutzungssperre

10.1 Sperre auf Veranlassung des Teilnehmers/Users

Die Bank sperrt auf Veranlassung des Teilnehmers/Users, insbesondere im Fall der Sperranzeige nach Nummer 9.1,

- den Zugang für ihn und, falls der Teilnehmer/User dies verlangt, den Zugang für alle Teilnehmer/User des Kunden oder
- sein Authentifizierungsinstrument.

10.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Zugang für einen Teilnehmer/User sperren, wenn

- sie berechtigt ist, den Vertrag über die Zusammenarbeit im Bereich Auslands- und Transaktionsgeschäft aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals besteht.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre in Textform (z. B. mittels Brief, Telefax oder E-Mail) oder telefonisch unterrichten.

10.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal bzw. das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

10.4 Automatische Sperre

(1) Die Chipkarte mit Signaturfunktion wird gesperrt, wenn dreimal in Folge der Nutzungscode falsch eingegeben wurde. Eine Wiederfreischaltung bzw. Entsperrung der Chipkarte durch die Bank ist nicht möglich. Der Teilnehmer/User muss mit einer neuen Chipkarte eine neue elektronische Signatur erstellen und diese erneut an die Bank übermitteln sowie mittels eines INI-Briefes bei der Bank freischalten lassen.

(2) Die PIN wird gesperrt, wenn dreimal in Folge die PIN falsch eingegeben wurde.

(3) Der Teilnehmer/User wird für das photoTAN-Verfahren gesperrt, wenn fünfmal hintereinander die TAN falsch eingegeben wurde.

(4) Der Teilnehmer/User kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Firmenkundenportals wiederherzustellen. Die Bank hat den Kunden unverzüglich nach der Sperrung von der Sperrung und den Gründen hierfür zu unterrichten, außer dies würde objektiven Sicherheitserwägungen oder gemeinschaftsrechtlichen oder innerstaatlichen Regelungen zuwiderlaufen oder gerichtliche oder verwaltungsbehördliche Anordnungen verletzen.

11. Haftung beim Einsatz von Personalisierten Sicherheitsmerkmalen und/oder Authentifizierungsinstrumenten

11.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments, haftet der Kunde für den der Bank hierdurch entstehenden Schaden, wenn dem Teilnehmer/User an Verlust, Diebstahl, sonstigem Abhandenkommen oder der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers nach diesen Bedingungen nicht regelmäßig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Kunde und Bank den Schaden zu tragen haben.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn der Teilnehmer/User die Sperranzeige nach Nummer 9.1 nicht abgeben konnte, weil die

Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(3) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das mit dem Kunden vereinbarte Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf dieses Limit.

(4) Die Absätze 2 und 3 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

11.2 Haftung bei nicht autorisierten Wertpapiertransaktionen oder bei anderen Servicearten vor der Sperranzeige
Beruhen nicht autorisierte Wertpapiertransaktionen oder nicht autorisierte Transaktionen bei den vereinbarten Servicearten vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haftet der Kunde für den der Bank hierdurch entstandenen Schaden, wenn den Teilnehmer/User an dem Verlust, Diebstahl, sonstigem Abhandenkommen oder der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers nach diesen Bedingungen nicht regelmäßig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Kunde und Bank den Schaden zu tragen haben.

11.3 Haftung der Bank ab der Sperranzeige
Sobald die Bank eine Sperranzeige eines Teilnehmers/Users erhalten hat, übernimmt sie alle danach durch nicht autorisierte Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer/User in betrügerischer Absicht gehandelt hat.

11.4 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.

12. Verfügbarkeit
Die Bank strebt an, die angebotenen Services möglichst umfassend verfügbar zu halten. Eine garantierte Verfügbarkeit ist damit nicht verbunden. Insbesondere aufgrund technischer Probleme, Wartungsarbeiten und aufgrund von Netzproblemen (z. B. Nichtverfügbarkeit von Servern Dritter), auf welche die Bank keinen Einfluss hat, kann es zu zeitweiligen Störungen kommen, die den Zugriff verhindern.

13. Verweis auf Internetseiten Dritter
Falls im Rahmen des Internetauftritts der Zugriff auf die Seiten Dritter ermöglicht wird, geschieht dies nur, um dem Kunden und dem User einen leichteren Zugriff auf das Informationsangebot im Internet zu ermöglichen. Die Inhalte der Seiten dieser Anbieter stellen nicht eigene Aussagen der Bank dar. Sie werden von der Bank auch nicht überprüft.

14. Nutzungsrechte
Dem Kunden wird durch diesen Vertrag nicht gestattet, Links oder Framelinks auf seinen Webseiten ohne vorherige schriftliche Zustimmung der Bank zu setzen. Der Kunde verpflichtet sich, die Webseiten und deren Inhalt nur für eigene Zwecke zu verwenden. Insbesondere ist der Kunde nicht berechtigt, ohne Zustimmung der Bank die Inhalte Dritten zur Verfügung zu stellen, in andere Produkte oder Verfahren einzubetten oder den Quellcode der einzelnen Webseiten zu entschlüsseln. Hinweise auf Rechte der Bank oder Dritter dürfen nicht entfernt oder unkenntlich gemacht werden. Der Kunde wird Marken, Domainnamen und andere Kennzeichen der Bank oder Dritter nicht ohne vorherige Zustimmung der Bank verwenden. Der Kunde erhält nach diesen Bedingungen keine unwiderruflichen, ausschließlichen und übertragbaren Nutzungsrechte.

15. Hotline (Helpdesk)
Die Bank bietet eine telefonische Hotline (sog. Helpdesk) für die Bearbeitung von Fragen zu Technik, Bedienung und Funktionalitäten der angebotenen Services an. Die Bank besetzt die Hotline während der für das deutsche Bankgewerbe geltenden Bankarbeitstage. Telefonnummern und Geschäftszeiten werden in den Zugangswegen kommuniziert.

16. Sonstiges
(1) Im Hinblick auf die ordnungsgemäße Abwicklung der Zusammenarbeit behält sich die Bank Änderungen im technischen bzw. organisatorischen Bereich vor, die auf einer allgemeinen, handelsüblichen Änderung der technischen Standards, der Vorgaben der Kreditwirtschaft oder der gesetzlichen bzw. aufsichtsbehördlichen Regelungen beruhen. Eine darüber hinausgehende wesentliche technische bzw. organisatorische Änderung, die erhebliche Auswirkungen auf die Rechte und Pflichten des Kunden oder der Bank hat, teilt die Bank dem Kunden mindestens sechs Wochen vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens mit. Die Zustimmung des Kunden gilt als erteilt, wenn er seine Ablehnung nicht innerhalb von sechs Wochen nach Erhalt der Mitteilung angezeigt hat.

(2) Diese Bedingungen richten sich nach deutschem Recht.

(3) Sollte dieser Vertrag eine Regelungslücke enthalten, eine Bestimmung unwirksam oder undurchführbar sein, so bleibt die Rechtswirksamkeit der übrigen Bestimmungen hiervon unberührt. Die Vertragsparteien verpflichten sich, in einem derartigen Fall eine wirksame oder durchführbare Regelung zu treffen, die dem Geist und Zweck der zu ergänzenden bzw. zu ersetzenden Bestimmung so weit wie möglich entspricht.

Commerzbank AG

22/93/28 (01/18)