COMMERZBANK

Geschäftsbedingungen für die Fernkommunikation (Dresdner Bank)

1. Leistungsangebot

(1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels Fernkommunikation in dem von der Bank angebotenen Umfang abwickeln. Für die Abwicklung gelten die Bedingungen für die jeweiligen Bankgeschäfte (zum Beispiel Allgemeine Bedingungen für Zahlungsdienste, Bedingungen für die Nutzung des Dresdner OnlineDepot, Sonderbedingungen für Wertpapiergeschäfte). Zudem kann er Informationen der Bank mittels Fernkommunikation abrufen. Die Bank ist berechtigt, dem Konto-/Depotinhaber 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) Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer" bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto" bezeichnet.

(3) Zur Nutzung der Fernkommunikation gelten die Standardlimite oder die mit der Bank gesondert vereinbarten Verfügungslimite für die Fernkommunikation.

2. Voraussetzungen zur Nutzung der Fernkommunikation

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels Fernkommunikation die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4).

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind:
- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN) (gilt nicht für Telefon-Banking),
- die Signatur-PIN/das Kennwort und die Daten des persönlichen elektronischen Schlüssels für die elektronische Signatur
- oder jedes andere Sicherheitsmerkmal, das die Bank mit dem Teilnehmer vereinbart.

2.2 Authentifizierungsinstrumente

Die TAN können dem Teilnehmer auf einer Liste mit einmal verwendbaren TAN zur Verfügung gestellt werden. Die Teilnehmer können weitere Authentifizierungsinstrumente zur Speicherung der elektronischen Signaturdaten nutzen:
- eine Chipkarte mit Signaturfunktion oder
- ein sonstiges Authentifzierungsinstrument, auf dem sich der Signaturschlüssel befindet
- oder jedes sonstige Authentifizierungsinstrument, das die Bank mit dem Teilnehmer vereinbart.

Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

3. Zugang zur Fernkommunikation

Der Teilnehmer erhält Zugang zur Fernkommunikation, wenn
- dieser seine persönliche Kundenkennung („Banking-ID") und seine PIN oder elektronische Signatur übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 9.1 und 10) vorliegt.

Nach Gewährung des Zugangs zur Fernkommunikation kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

4. Auftragsabwicklung im Rahmen der Fernkommunikation

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss einen im Rahmen der Fernkommunikation erteilten Auftrag (zum Beispiel eine Überweisung) zu deren Wirksamkeit mit dem vereinbarten personalisierten Sicherheitsmerkmal (zum Beispiel PIN und TAN oder die Signatur-PIN/das Kennwort und elektronische Signatur) autorisieren und der Bank mittels Fernkommunikation übermitteln. Die Bank bestätigt mittels Fernkommunikation 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. Der Widerruf von Aufträgen kann nur außerhalb der Fernkommunikation erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit in der Fernkommunikation ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der im Rahmen der Fernkommunikation erteilten Aufträge erfolgt nach den für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung oder Wertpapierauftrag) geltenden Regelungen.

(2) Für Zahlungsaufträge (Überweisung, Lastschrift) gelten folgende Sonderregelungen:

Die Bank wird den Zahlungsauftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- Der Teilnehmer hat sich mit seinem personalisierten Sicherheitsmerkmal legitimiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor.
- Das Fernkommunikations-Datenformat ist eingehalten.
- Das gesondert vereinbarte Fernkommunikations-Verfügungslimit oder das Standardlimit ist nicht überschritten.
- Die 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 1.–5. Spiegelstrich nicht vor, wird die Bank den Zahlungsauftrag nicht ausführen.

Führt sie den Auftrag nicht aus, wird sie 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 Fernkommunikation eine Information zur Verfügung stellen. 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 erhöhter Zins zu zahlen ist.

6. Information des Kontoinhabers über mittels Fernkommunikation erteilte Verfügungen

Die Bank unterrichtet den Kontoinhaber über die mittels Fernkommunikation getätigten Verfügungen auf dem für Konto- und Depotinformationen vereinbarten Weg und gemäß den für den Auftrag geltenden Bedingungen.

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zur Fernkommunikation

Der Teilnehmer ist verpflichtet, die technische Verbindung zur Fernkommunikation nur über die von der Bank gesondert mitgeteilten Fernkommunikations-Zugangskanäle (zum Beispiel Internetadresse) herzustellen.

7.2 Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer hat
- seine personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der Bank gesondert mitgeteilten Fernkommunikations-Zugangskanäle an diese zu übermitteln 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 dem dazugehörigen personalisierten Sicherheitsmerkmal das Fernkommunikations-Verfahren missbräuchlich nutzen.

(2) Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:
- Die personalisierten Sicherheitsmerkmale PIN und TAN sowie die Signatur-PIN/das Kennwort dürfen nicht elektronisch gespeichert werden (zum Beispiel im Kundensystem). Der vom Teilnehmer erzeugte persönliche elektronische Schlüssel darf sich nur in der alleinigen Verfügungsgewalt des Teilnehmers befinden.
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (zum Beispiel nicht auf Online-Händlerseiten).
- Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb des Fernkommunikations-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die Signatur-PIN/das Kennwort für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung eines Auftrags nicht mehr als eine TAN verwenden.

7.3 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem Fernkommunikations-Auftrag (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (zum Beispiel Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

8. 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.

Fassung November 2009

9. Anzeige- und Unterrichtungspflichten

9.1 Sperranzeige
(1) Stellt der Teilnehmer
– den Verlust oder den Diebstahl des Authentifizierungsinstruments,
– die missbräuchliche Verwendung oder
– die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines persönlichen Sicherheitsmerkmals
fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

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

(3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt
– den Besitz an 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 Kontoinhaber 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
Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 9.1
– den Fernkommunikations-Zugang für ihn oder alle Teilnehmer oder
– sein Authentifizierungsinstrument.

10.2 Sperre auf Veranlassung der Bank
(1) Die Bank darf den Fernkommunikations-Zugang für einen Teilnehmer sperren, wenn
– sie berechtigt ist, den Fernkommunikations-Vertrag 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 besteht.

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

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

10.4 Automatische Sperre eines chipbasierten Authentifizierungsinstruments
(1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge die Signatur-PIN/das Kennwort 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 von PIN oder TAN führt zu einer Sperre des Zugangs.

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

11. Haftung

11.1 Haftung der Bank bei einer nicht autorisierten Verfügung über Fernkommunikation und einer nicht oder fehlerhaft ausgeführten Verfügung über Fernkommunikation
Die Haftung der Bank bei einer nicht autorisierten Verfügung über Fernkommunikation und einer nicht oder fehlerhaft ausgeführten Verfügung über Fernkommunikation richtet sich vorrangig nach Nummer 11.2 und nachrangig nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen.

11.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

11.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige
(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigem Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen, gestohlen oder sonst abhandengekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 Euro nach Absatz 1 und 2 hinaus bis zu einem Höchstbetrag von der Hälfte des verfügten Betrags, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 9.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(5) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er
– den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 9.1 Absatz 1),
– das personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2 Absatz 2 1. Spiegelstrich),
– das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt oder das Autorisierungsinstrument einem Dritten zugänglich gemacht hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1 2. Spiegelstrich),
– das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2 3. Spiegelstrich),
– das personalisierte Sicherheitsmerkmal außerhalb des Fernkommunikations-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2 4. Spiegelstrich),
– das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 5. Spiegelstrich),
– mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2 6. Spiegelstrich) oder
– der Kunde die auf seinem Authentifizierungsinstrument angezeigten Auftragsdaten nicht prüft.

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

11.2.2 Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige
Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften der Kontoinhaber 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 über die Fernkommunikation durch nicht autorisierte Verfügungen 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.

12. Datenschutz
Alle im Rahmen von der Fernkommunikation entstehenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und der Commerz Direktservice GmbH nur innerhalb der Europäischen Union erhoben und verarbeitet.