

Bedingungen für die Abwicklung von Bankgeschäften über das Firmenkundenportal

(Stand 31.10.2009)

1. Leistungsangebot

(1) Der Kunde kann das Firmenkundenportal nutzen und Bankgeschäfte über das Firmenkundenportal in dem 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 er Informationen der Bank über das Firmenkundenportal abrufen.

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

(3) Zur Nutzung des Firmenkundenportals gelten die Standardlimes oder die mit der Bank gesondert vereinbarten Verfügungslimits für die vereinbarte Serviceart.

2. Voraussetzungen zur Nutzung des Firmenkundenportals

Der Teilnehmer/User benötigt für die Abwicklung von Bankgeschäften 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).

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

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

2.2 Authentifizierungsinstrumente

Die TAN können dem Teilnehmer/User auf einer Liste mit einmal verwendbaren TAN zur Verfügung gestellt werden. Die Teilnehmer/User können weitere Authentifizierungsinstrumente zur Speicherung der elektronischen Signaturdaten nutzen:

- eine Chipkarte mit Signaturfunktion oder
- ein sonstiges Authentifizierungsinstrument, auf dem sich der Signaturschlüssel befindet.

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 Zugangsbeziehung 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.

4. Auftragsabwicklung im Rahmen des Firmenkundenportals

4.1 Auftragserteilung und Autorisierung

Die Autorisierung zur Durchführung einzelner Geschäfte (z. B. Überweisung) erfolgt – abhängig von der gewählten Serviceart – mittels der vereinbarten personalisierten Sicherheitsmerkmale

- iTAN
- PIN
- elektr. Unterschrift bzw.
- nach Anmeldung mit Teilnehmernummer bzw. Anmeldenamen und PIN durch einfache Freigabe.

4.2 Meldung nach AWW

Bei Zahlungen zugunsten Gebietsfremder ist vom Teilnehmer/User 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 des Firmenkundenportals erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Firmenkundenportal ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der im Rahmen des Firmenkundenportals 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 Teilnehmer/Users für die jeweilige Auftragsart liegt vor.
- Das für die vereinbarte Serviceart erforderliche Datenformat ist eingehalten.
- Das für die Serviceart gesondert vereinbarte 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 Spiegelstrich 1–5 nicht vor, wird die Bank den Zahlungsauftrag nicht ausführen. Die Bank wird den Teilnehmer/User über die Nichtausführung und soweit möglich, über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, online oder auf anderem Weg eine Information zur Verfü-

gung 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 Kunden über im Rahmen des Firmenkundenportals erteilte Verfügungen

Die Bank unterrichtet den Kunden über die im Rahmen des Firmenkundenportals 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 zum Firmenkundenportal

Der Teilnehmer/User ist verpflichtet, die technische Verbindung zum Firmenkundenportal nur über die von der Bank gesondert mitgeteilten Zugangskanäle (z. B. Internetadresse) herzustellen. Der Kunde 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. Der Kunde 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 und nur über die von der Bank gesondert für das Firmenkundenportal mitgeteilten Zugangskanäle 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 Verfahren missbräuchlich nutzen.

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

- Die personalisierten Sicherheitsmerkmale PIN und iTAN sowie die Signatur-PIN/das Kennwort dürfen bei einem

Teilnehmer/User nicht elektronisch gespeichert werden (z.B. im Kundensystem). Der vom Teilnehmer/User erzeugte persönliche elektronische Schlüssel darf sich nur in der alleinigen Verfügungsgewalt des Teilnehmers/Users 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 auspähen können.
- Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf Online-Händlerseiten).
- Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb des Firmenkundenportals 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/User darf zur Autorisierung eines Auftrags nicht mehr als eine iTAN verwenden. Zwei TANs zu einem Vorgang werden von der Bank nur im Rahmen der Aktivierung einer neuen TAN-Liste erfragt (letzte TAN des alten TAN-Briefs und erste TAN des neuen TAN-Briefs).

7.3 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. 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.

7.4 Weitere Sorgfaltspflichten des Kunden

Der Kunde trägt dafür Sorge, dass die Sorgfaltspflichten aus diesem Vertrag auch von dem Bevollmächtigten (also von allen Teilnehmern/Users) 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 die erforderlichen Genehmigungen, Anzeigen oder sonst erforderlichen Maßnahmen zu veranlassen. Der Teilnehmer hat die Bank über ihm bekannt gewordene Verbote, Genehmigungs- und Anzeigepflichten zu informieren.

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 seines persönlichen Sicherheitsmerkmals

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 zum Firmenkundenportal 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 zum Firmenkundenportal 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 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 Kunden unverzüglich.

10.4 Automatische Sperre eines chip-basierten Authentifizierungsinstrument

(1) Die Chipkarte mit Signaturfunktion wird gesperrt, wenn dreimal in Folge die Signatur-PIN/das Kennwort für die elektronische Signatur falsch eingegeben wurde. Eine Wiederfreischaltung bzw. Entsperrung der Chipkarte durch die Bank ist nicht möglich.

(2) Die übermittelte Signatur wird gesperrt, wenn dreimal in Folge der Signatur-PIN/das Kennwort zur Freigabe der Signatur falsch eingegeben wurde. Der Teilnehmer/User muss eine neue elektronische Signatur erstellen und diese erneut an die Bank übermitteln sowie mittels eines INI-Briefes bei der Bank freigeben.

(3) Die PIN wird gesperrt, wenn dreimal in Folge die PIN falsch eingegeben wurde. Der TAN-Brief wird gesperrt, wenn dreimal in Folge eine TAN falsch eingegeben wurde.

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

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 verlorengegangenen, gestohlenen oder sonst abhanden gekommenen 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 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.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 2 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 und der Schaden dadurch eingetreten ist.

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

11.2 Haftung bei nicht autorisierten Wertpapiertransaktionen oder bei anderen Servicearten vor der Sperranzeige

Beruhend nicht autorisierte Wertpapiertransaktionen oder nicht autorisierte Transaktionen bei den vereinbarten Servicearten vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen 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 dem Teilnehmer/User an dem Verlust, Diebstahl, sonstigen 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 über durch nicht autorisierte Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer/User in betrügerischer Absicht gehandelt hat.

12. Verfügbarkeit

Die Bank strebt an, die im Firmenkundenportal 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 zur Technik, Bedienung und Funktionalitäten der im Firmenkundenportal angebotenen Services an. Die Bank besetzt die Hotline während der für das deutsche Bankgewerbe geltenden Bankarbeitstage. Telefonnummern und Geschäftszeiten werden in den Zugangswegen (z. B. firmenkundenportal.de/kontakt) kommuniziert.