

Bedingungen für DKB-Onlinebanking mit HBCI-Chipkarte

für die konto-/ depotbezogene Nutzung des Onlinebanking mit elektronischer Signatur (HBCI)

1. Leistungsangebot

Der Konto-/ Depotinhaber (im Folgenden „Kunde“ genannt) und etwaige Bevollmächtigte können Bankgeschäfte mittels Onlinebanking in dem von der Deutschen Kreditbank AG (im Folgenden „Bank“ genannt) angebotenen Umfang abwickeln. Der Kunde und etwaige Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet.

2. Technische Voraussetzungen beim Teilnehmer

Der Teilnehmer benötigt ein Onlinebanking-fähiges Endgerät (Kundensystem). Dieses Kundensystem kann ein PC mit installierter Onlinebankingsoftware, einem Chipkartenleser und einem Zugang zum Internet sein.

3. Zugangsmedien

- (1) Zur Abwicklung von Bankgeschäften mittels Onlinebanking unter Verwendung von einer HBCI-Chipkarte erhält der Teilnehmer ein persönliches Sicherheitsmerkmal sowie Authentifizierungsinstrument, um sich der Bank gegenüber als berechtigter Teilnehmer auszuweisen und Aufträge zu autorisieren.
- (2) Authentifizierungsinstrument ist eine Chipkarte, personalisiertes Sicherheitsmerkmal ist die für diese Chipkarte zu deren Schutz dienende PIN (Persönliche Identifikations-Nummer) sowie ein Nutzungscode für die elektronische Signatur. Für diese Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.
- (3) Zur Aufnahme der Verbindung per Onlinebanking teilt die Bank dem Teilnehmer ferner folgende erforderliche Zugangsdaten mit:
 - die Benutzerkennung
 - und
 - die Kommunikationszugangsadresse.

Der Teilnehmer muss bei der Initialisierung die Benutzerkennung und Kommunikationszugangsadresse auf der Chipkarte speichern. Die Art und Weise der Initialisierung ist abhängig vom eingesetzten Kundensystem und Kartenlesegerät.

4. Verfahren

- (1) Der Teilnehmer hat mittels Onlinebanking Zugang zu allen gegenwärtigen und künftigen Konten und Depots. Dafür ist die Eingabe seiner elektronischen Signatur unter Verwendung seiner Chipkarte und der dazugehörigen PIN erforderlich.

- (2) Der Teilnehmer ist verpflichtet, die technische Verbindung zum Onlinebanking-Angebot der Bank nur über die Internetseiten der Bank (www.dkb.de) oder die ihm gesondert mitgeteilten Kommunikationswege herzustellen.

5. Erteilung, Widerruf und Bearbeitung von Aufträgen im Onlinebanking

- (1) Der Teilnehmer muss mittels Onlinebanking erteilte Aufträge (z.B. Überweisungen) zu deren Wirksamkeit mit dem personalisierten Sicherheitsmerkmal (elektronische Signatur) autorisieren und der Bank mittels Onlinebanking übermitteln. Die Bank bestätigt mittels Onlinebanking den Eingang des Auftrags.
- (2) Die Widerrufbarkeit eines Onlinebanking-Auftrages richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z.B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Onlinebanking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Onlinebanking ausdrücklich vor.
- (3) Die Bearbeitung der mittels Onlinebanking erteilten Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z.B. Überweisung) im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.
- (4) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
 - Der Teilnehmer hat sich mit seinem personalisierten Sicherheitsmerkmal legitimiert.
 - Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z.B. Wertpapierorder) liegt vor.
 - Das Onlinebanking-Verfügungslimit (vgl. Ziffer 8) ist nicht überschritten.
 - Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z.B. ausreichende Kontodeckung gemäß den Überweisungsbedingungen) liegen vor.
- (5) Liegen die Ausführungsbedingungen nach Ziffer 5.4) vor, führt die Bank die mittels Onlinebanking erteilten Aufträge nach Maßgabe der Bestimmungen der für den jeweiligen Geschäftsvorfall geltenden Sonderbedingungen (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das

Wertpapiergeschäft) aus.

- (6) Liegen die Ausführungsbedingungen nach Ziffer 5.4) nicht vor, wird die Bank den Onlinebanking-Auftrag nicht ausführen und den Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Onlinebanking informieren.

6. Elektronischer Kommunikationsweg

- (1) Durch die Teilnahme am Onlinebanking und Nutzung des gesicherten Bereiches im Internet-Banking inklusive des elektronischen Postfachs erhält der Teilnehmer Konto-/ Depotinformationen (z.B. Kreditkartenabrechnungen, Konto- und Depotauszüge, Rechnungsabschlüsse), Allgemeine Geschäftsbedingungen und Sonderbedingungen (im Folgenden zusammen „Bedingungen“ genannt) oder sonstige Informationen und Mitteilungen, die seine Geschäftsverbindung zur Bank betreffen, grundsätzlich nur in elektronischer Form.
- (2) Die Inhalte des elektronischen Postfachs kann der Teilnehmer über die Schaltfläche „Briefkasten“ im Internet-Banking abrufen.
- (3) Kontoauszüge und Kreditkartenabrechnungen werden dem Teilnehmer einmal monatlich bereitgestellt, sofern Konto- oder Kreditkartenumsätze vorliegen. Rechnungsabschlüsse werden nach Abschluss eines Quartals bereitgestellt. Etwas anderes gilt nur, wenn vertraglich mit dem Teilnehmer abweichende Vereinbarungen getroffen wurden. Im Zeitraum zwischen zwei Kontoauszügen kann der Teilnehmer seine Kontobewegungen mittels Umsatzabfrage in der Onlinebanking-Anwendung einsehen.
- (4) Konto-/ Depotinformationen, Bedingungen, sonstige Informationen und Mitteilungen werden im Internet-Banking in Textform bereitgestellt. Für die dauerhafte Speicherung der Konto-/ Depotinformationen, Bedingungen, sonstigen Informationen und Mitteilungen ist der Teilnehmer verantwortlich.
- (5) Die Bank übernimmt keine Gewähr, dass aufgrund der Systemumgebung des Teilnehmers ein Ausdruck der Konto-/ Depotinformationen, der Bedingungen und der sonstigen Informationen und Mitteilungen mit der Darstellung auf dem Bildschirm übereinstimmt.
- (6) Die im Internet-Banking eingestellten Konto-/ Depotinformationen, Bedingungen, sonstigen Informationen und Mitteilungen sind mit Einstellung im Internet-Banking zugegangen.
- (7) Der Teilnehmer ist verpflichtet, seine Konto-/ Depotinformationen, Bedingungen, sonstigen Informationen und Mitteilungen zeitnah abzurufen und sie unverzüglich auf ihre Richtigkeit zu überprüfen. Etwaige Einwendungen sind unverzüglich schriftlich (§ 126 BGB) zu erheben.

7. Dokumentenmappe/ Tresor

- (1) Im Rahmen der Nutzung des Internet-Bankings kann der Teilnehmer u.a. die Funktion Dokumentenmappe/ Tresor nutzen.
- (2) Mit der Funktion Dokumentenmappe/ Tresor erhält der Teilnehmer Gelegenheit, persönliche Dokumente digital zu speichern und zu verwahren. Die Inhalte der Dokumentenmappe/ des Tresors kann der Teilnehmer über die Schaltfläche „Dokumentenmappe“ aus seiner Onlinebanking-Anwendung abrufen.
- (3) Die Bank ist berechtigt, aber nicht verpflichtet, sich Kenntnis über den Inhalt der Dokumentenmappe/ des Tresors des Teilnehmers zu verschaffen.
- (4) Die Bank speichert die in der Dokumentenmappe/ im Tresor enthaltenen Dokumente für die Dauer der Teilnahme des Teilnehmers am Internet-Banking. Für den Fall der Kündigung der Geschäftsbeziehung verpflichtet sich der Teilnehmer, unmittelbar alle Dokumente aus der Dokumentenmappe/ dem Tresor auszulesen. Nach Wirksamwerden der Kündigung werden die Dokumente aus der Dokumentenmappe/ dem Tresor gelöscht.

8. Finanzielle Nutzungsgrenze

Der Teilnehmer darf Verfügungen nur im Rahmen des Kontoguthabens oder eines vorher für das Konto eingeräumten Kredites vornehmen. Auch wenn der Teilnehmer diese Nutzungsgrenze bei seinen Verfügungen nicht einhält, ist die Bank berechtigt, den Ersatz der Aufwendungen zu verlangen, die aus der Nutzung des Onlinebanking entstehen. Die Buchung solcher Verfügungen auf dem Konto führt lediglich zu einer geduldeten Kontoüberziehung. Die Bank ist berechtigt, in diesem Fall den höheren Zinssatz für geduldete Kontoüberziehungen zu verlangen.

Eine Änderung dieser Verfügungsmitel kann der Teilnehmer mit der Bank gesondert vereinbaren.

9. Geheimhaltung der personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente

- (1) Der Teilnehmer hat dafür Sorge zu tragen, dass keine andere Person in den Besitz der Chipkarte kommt sowie Kenntnis von der zu deren Schutz dienenden PIN oder dem Nutzungscod für die elektronische Signatur erlangt. Jede Person, die im Besitz der Chipkarte ist und die PIN oder den Nutzungscod für die elektronische Signatur kennt, hat die Möglichkeit, das Onlinebanking-Leistungsangebot einschließlich der dem Teilnehmer eingeräumten sonstigen Anwendungen missbräuchlich zu nutzen. Sie kann z. B. Aufträge zu Lasten des Kontos/ Depots erteilen.
- (2) Insbesondere ist Folgendes zum Schutz der Chipkarte und der PIN zu beachten:
- die zum Schutz der Chipkarte dienende PIN oder der Nutzungscod für die elektronische Signatur dürfen nicht elektronisch gespeichert werden;
 - die PIN und der Nutzungscod für die elektronische Signatur

natur dürfen nicht zusammen mit der Chipkarte aufbewahrt werden;

- bei der Eingabe der PIN oder des Nutzungscodes ist sicherzustellen, dass Dritte diese nicht ausspähen können;
 - die PIN oder der Nutzungscode dürfen nicht außerhalb des Onlinebanking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail;
 - die PIN oder der Nutzungscode dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf Online-Händlerseiten);
 - die Chipkarte ist nach Beendigung der Onlinebanking-Nutzung aus dem Lesegerät zu entnehmen und sicher und getrennt von der PIN zu verwahren.
- (3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt in den Besitz seiner Chipkarte gelangt ist oder von seiner zum Schutz der Chipkarte dienenden PIN Kenntnis erhalten hat oder beides oder besteht der Verdacht der missbräuchlichen Nutzung der Chipkarte und/ oder PIN oder stellt der Teilnehmer den Verlust oder den Diebstahl seiner Chipkarte oder PIN, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seiner Chipkarte oder PIN fest, so ist er verpflichtet, unverzüglich die Bank hierüber zu unterrichten. Im Fall der vorgenannten Anzeige wird die Bank den Onlinebanking-Zugang zum Konto/ Depot sperren. Der Teilnehmer ist verpflichtet, jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen und dies der Bank nachzuweisen.

10. Weitere Sorgfalts- und Mitwirkungspflichten

- (1) Der Teilnehmer hat sich Gewissheit über die Sicherheit der von ihm benutzten Technik und Software zu verschaffen und Risiken (z.B. Computerviren, Trojaner) im Rahmen des Möglichen (z.B. durch die Installation und Aktualisierung eines handelsüblichen Virenschutzprogramms, einer Firewall und der regelmäßigen Sicherheits-Updates für den von ihm verwendeten Browser) auszuschließen. Weitere zu beachtende Sicherheitshinweise erhält der Teilnehmer über die Internetseiten der Bank.
- (2) Bei jedem Login in das Internet-Banking hat der Teilnehmer das Sicherheitszertifikat zu überprüfen, um sicherzustellen, dass er auch tatsächlich mit der Bank kommuniziert. Bei Auffälligkeiten und Zweifeln an der Echtheit hat der Teilnehmer die Bank unverzüglich hierüber zu informieren.
- (3) Der Teilnehmer hat alle von ihm eingegebenen Daten auf Vollständigkeit und Richtigkeit zu überprüfen. Soweit die Bank dem Teilnehmer Daten aus seinem Onlinebanking-Auftrag (z.B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.
- (4) Der Teilnehmer hat die Bank unverzüglich nach Feststellung eines nicht autorisierten Auftrags hierüber in Textform zu unterrichten.

11. Sperre des Onlinebanking-Zugangs

- (1) Werden dreimal hintereinander Aufträge mit einer falschen elektronischen Signatur an die Bank übermittelt, so sperrt die Bank den Onlinebanking-Zugang zum Konto/ Depot. In diesem Falle muss sich der Teilnehmer mit der Bank in Verbindung setzen.
- (2) Die Bank wird den Onlinebanking-Zugang zum Konto/ Depot sperren, wenn der Verdacht einer missbräuchlichen Nutzung des Onlinebanking besteht. Zur Aufhebung der Sperre muss sich der Teilnehmer mit der Bank in Verbindung setzen.
- (3) Im Übrigen kann die Bank den Onlinebanking-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, die Geschäftsbeziehung 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 eines persönlichen Sicherheitsmerkmals besteht.
- (4) Die Bank wird den Teilnehmer unter Angabe der für die Sperrung maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten. Die Bank wird eine Sperre aufheben, wenn Gründe für die Sperre nicht mehr gegeben sind. Auch hierüber wird sie den Teilnehmer unverzüglich unterrichten.
- (5) Die Bank wird den Onlinebanking-Zugang zum Konto/ Depot auf Wunsch des Teilnehmers sperren. Auch diese Sperre kann nicht mittels Onlinebanking aufgehoben werden. Der Teilnehmer muss sich zur Aufhebung der Sperre mit der Bank in Verbindung setzen.

12. Haftung

12.1 Haftung der Bank bei nicht autorisierten und nicht oder fehlerhaft ausgeführten Onlinebanking-Verfügungen

Die Haftung der Bank bei nicht autorisierten und nicht oder fehlerhaft ausgeführten Onlinebanking-Verfügungen richtet sich nach den für den jeweiligen Geschäftsvorfall vereinbarten Bedingungen (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft.)

12.2 Haftung des Kunden bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

12.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Verdachts- oder Sperranzeige

- (1) Beruht ein nicht autorisierter Zahlungsvorgang vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments, haftet der Kunde 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 oder Diebstahl des Authentifizierungsinstruments ein Verschulden trifft. Die Haftung nach Absatz 5 für vorsätzliches und grob fahrlässiges Verhalten bleibt hiervon unberührt.

- (2) Kommt es vor der Sperranzeige zu einem nicht autorisierten Zahlungsvorgang aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen oder gestohlen worden ist, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Teilnehmer die personalisierten Sicherheitsmerkmale nicht sicher aufbewahrt hat. Die Haftung nach Absatz 5 für vorsätzliches und grob fahrlässiges Verhalten bleibt hiervon unberührt.
- (3) Ist der Kunde kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungen über die Haftungsgrenze von 150 Euro nach Absatz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- (4) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn er eine Sperranzeige 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 Verdachts- oder Sperranzeige zu einer nicht autorisierten Verfügung und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kunde 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,
 - das personalisierte Sicherheitsmerkmal elektronisch gespeichert hat,
 - das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde,
 - das personalisierte Sicherheitsmerkmal außerhalb des Onlinebanking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat,
 - das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (z. B. im Originalbrief, in dem es dem Teilnehmer mitgeteilt wurde).

12.2.2. Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhet eine nicht autorisierte Wertpapiertransaktion vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstruments oder auf der sonsti-

gen missbräuchlichen Nutzung des personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften Kunde und Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

12.2.3 Haftung der Bank ab der Verdachts- oder Sperranzeige

Sobald der Bank

- die Kenntniserlangung des personalisierten Sicherheitsmerkmals oder Besitzerlangung des Authentifizierungsinstruments durch andere Personen
- oder
- der Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments angezeigt wurde, übernimmt die Bank alle nach dem Zeitpunkt des Zugangs der Verdachts- oder Sperranzeige durch nicht vom Teilnehmer autorisierte Onlinebanking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

12.2.4 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
- oder
- von der Bank aufgrund einer gesetzlichen Verpflichtung herbeigeführt wurden.

13. Anwendbares Recht

Auf die Geschäftsbeziehung zwischen dem Kunden und der Bank findet deutsches Recht Anwendung, es sei denn, dieses verweist auf eine ausländische Rechtsordnung.