Bedingungen für das Onlinebanking – HBCIbanking mit Chipkarte

Fassung Oktober 2009

BW|Bank
Baden-Württembergische Bank

Die Allgemeinen Geschäftsbedingungen und die besonderen Bedingungen der LBBW gelten für die Geschäftsverbindung des Kunden mit der Landesbank Baden-Württemberg und ihren unselbstständigen Anstalten, der Baden-Württembergischen Bank, der Rheinland-Pfalz Bank und der Sachsen Bank. Erklärungen der Baden-Württembergischen Bank, der Rheinland-Pfalz Bank und der Sachsen Bank im Rahmen der Geschäftsverbindung berechtigen und verpflichten ausschließlich die Landesbank Baden-Württemberg.

1. Leistungsangebot

(1) Der Konto-/Depotinhaber sowie etwaige Bevollmächtigte am Onlinebanking (im Folgenden Teilnehmer genannt) können Bankgeschäfte mittels HBCIbanking mit Chipkarte (nachfolgend HBCIbanking) in dem von der Bank angebotenen Umfang abwickeln. Zudem kann der Teilnehmer Informationen der Bank mittels HBCIbanking abrufen. Konto und Depot werden im Folgenden einheitlich als „Konto" bezeichnet.

(2) Zur Nutzung des HBCIbanking gelten die mit der Bank ggf. gesondert vereinbarten Verfügungslimite (beispielsweise pro Auftrag).

2. Voraussetzungen zur Nutzung des HBCIbanking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels HBCIbanking 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 Personalisiertes Sicherheitsmerkmal

Personalisiertes Sicherheitsmerkmal ist die Persönliche Identifikationsnummer (PIN), welche für die HBCI-Chipkarte erstmals bei Erstzugang zu vergeben ist.

2.2 Authentifizierungsinstrument

Jeder Teilnehmer erhält als Authentifizierungsinstrument eine HBCI-Chipkarte (nachfolgend auch Chipkarte). Für die Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

3. Zugang zum HBCIbanking

Der Teilnehmer erhält Zugang zum HBCIbanking, wenn
- er sich mit Hilfe der HBCI-Chipkarte und der zugehörigen PIN identifiziert und legitimiert hat und
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9) oder des Kontos vorliegt.

Nach erfolgreichem Zugang zum HBCIbanking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

4. HBCIbanking-Aufträge durch den Teilnehmer

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss HBCIbanking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal in Verbindung mit der HBCI-Chipkarte autorisieren und der Bank mittels HBCIbanking übermitteln. Die Bank bestätigt mittels HBCIbanking den Eingang des Auftrags. Der Teilnehmer erhält Hinweise darüber, ob der Auftrag angenommen bzw. ausgeführt wurde. Der Hinweis "Auftrag angenommen" bedeutet, dass sich der Auftrag noch in Bearbeitung befindet. Der Hinweis "Auftrag ausgeführt" gilt als Bestätigung für den Vollzug z. B. der Buchung.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines HBCIbanking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Bedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des HBCIbanking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im HBCIbanking ausdrücklich vor.

5. Bearbeitung von HBCIbanking-Aufträgen durch die Bank

(1) Die Bearbeitung der HBCIbanking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) im „Preis- und Leistungsverzeichnis" bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. 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. Über den Zeitpunkt der tatsächlichen Ausführung wird der Teilnehmer in den Umsatzinformationen im HBCIbanking und im Kontoauszug informiert.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- Der Teilnehmer hat sich mit seinem Personalisierten Sicherheitsmerkmal autorisiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor.
- Das HBCIbanking-Datenformat ist eingehalten.
- Das ggf. gesondert vereinbarte HBCIbanking-Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Bedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen vor, führt die Bank die HBCIbanking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Bedingungen (z. B. Bedingungen für den Überweisungsverkehr) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 nicht vor, wird die Bank den HBCIbanking-Auftrag nicht ausführen und dem Kontoinhaber und/oder Teilnehmer eine Information über die Nichtausführung und – soweit möglich – über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, außerhalb des HBCIbanking zur Verfügung stellen.

6. Information des Kontoinhabers über HBCIbanking-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels HBCIbanking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg. Mit Kontoinhabern, die nicht Verbraucher sind, kann die Art und Weise sowie die zeitliche Folge der Unterrichtung gesondert vereinbart werden.

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum HBCIbanking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum HBCIbanking nur über den von der Bank gesondert mitgeteilten HBCIbanking-Zugangskanal (z. B. IP-Adresse) herzustellen.

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer hat
- sein Personalisiertes Sicherheitsmerkmal (siehe Nummer 2.1) geheim zu halten und nur über den von der Bank gesondert mitgeteilten HBCIbanking-Zugangskanal 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 HBCIbanking missbräuchlich nutzen.

(2) Insbesondere ist Folgendes zum Schutz der HBCI-Chipkarte und der PIN zu beachten:
- Die PIN darf nicht elektronisch gespeichert werden.
- Bei Eingabe der PIN ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- Die PIN darf nicht zusammen mit dem Authentifizierungsinstrument (HBCI-Chipkarte) verwahrt werden.

- Die HBCI-Chipkarte ist nach Beendigung der HBCIbanking-Nutzung aus dem Lesegerät zu entnehmen und sicher zu verwahren.
- Personalisiertes Sicherheitsmerkmal und Authentifizierungsinstrument dürfen nicht außerhalb des HBCIbanking der Bank verwendet werden.
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des HBCIbanking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.

7.3 Sicherheit des Kundensystems
Der Teilnehmer muss die Sicherheitshinweise der Bank zum Onlinebanking auf der Internetseite der Bank, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten
Soweit die Bank dem Teilnehmer Daten aus seinem HBCIbanking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät des Teilnehmers 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. Anzeige- und Unterrichtungspflichten

8.1 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 Personalisierten 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 aufgeben.

(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.

8.2 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.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers
Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1, den HBCIbanking-Zugang oder sein Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Bank
(1) Die Bank darf den HBCIbanking-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, den HBCIbanking-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 Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

9.3 Aufhebung der Sperre
Die Bank wird eine Sperre aufheben und soweit erforderlich die Chipkarte austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber und/oder Teilnehmer.

9.4 Automatische Sperre
Werden dreimal hintereinander Aufträge mit falscher Signatur an die Bank übermittelt, so sperrt die Bank automatisch den Zugang zum HBCIbanking für das Konto. In diesem Fall sollte sich der Teilnehmer mit der Bank in Verbindung setzen.

10. Haftung

10.1 Haftung der Bank bei einer nicht autorisierten HBCIbanking-Verfügung und einer nicht oder fehlerhaft ausgeführten HBCIbanking-Verfügung
Die Haftung der Bank bei einer nicht autorisierten HBCIbanking-Verfügung und einer nicht oder fehlerhaft ausgeführten HBCIbanking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Bedingungen (z. B. Bedingungen für den Überweisungsverkehr).

10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige
(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhanden gekommenen 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 verloren gegangen, gestohlen worden oder sonst abhanden gekommen 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, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen gehandelt 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 8.1 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 dann 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 8.1),
- das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2),
- das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2),
- Personalisiertes Sicherheitsmerkmal und Authentifizierungsinstrument erkennbar außerhalb des HBCIbanking der Bank verwendet hat (siehe Nummer 7.2),
- das Personalisierte Sicherheitsmerkmal außerhalb des HBCIbanking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2),

- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2).

(6) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

10.2.2 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige des Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte HBCIbanking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.2.3 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.

.

11. Bereitstellung von Informationen

(1) Alle dem Teilnehmer übermittelten Kursdaten und Börseninformationen werden von Dritten bereitgestellt und von der Bank nicht auf Ihre Richtigkeit überprüft. Die Bank haftet daher nicht für die Richtigkeit, Vollständigkeit und Aktualität der Daten.

(2) Die zur Verfügung gestellten Informationen sind nur für den Teilnehmer bestimmt. Jede weiter gehende Verwendung, insbesondere die Speicherung in Datenbanken, Veröffentlichung, Vervielfältigung und jede Form der gewerblichen Nutzung sowie Weitergabe an Dritte ist nicht zulässig.

12. Speicherung Teilnehmerdaten

Aufgrund gesetzlicher Vorschriften werden die Teilnehmerdaten von der Bank gespeichert.

13. Außergerichtliche Streitschlichtung und Beschwerdemöglichkeit

Für die Beilegung von Streitigkeiten mit der Bank kann sich der Kontoinhaber an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.