

Fassung Oktober 2010

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 BW Onlinebanking mit Direktbrokerage, Mobilbanking und HBCIbanking mit PIN/TAN (nachfolgend Onlinebanking) in dem von der Bank angebotenen Umfang abwickeln. Zudem kann der Teilnehmer Informationen der Bank mittels Onlinebanking abrufen. Konto, Kreditkarte und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.

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

2. Voraussetzungen zur Nutzung des Onlinebanking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels Onlinebanking 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 sind

- die Persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN)

2.2 Authentifizierungsinstrument

Dem Teilnehmer wird für die Erzeugung der TAN ein TAN-Generator zur Verfügung gestellt. Mit dem TAN-Generator wird die „Checkliste für den ersten Zugang“ mit allen Zugangs-Informationen sowie Anweisungen zur Verwendung des TAN-Generators versandt.

3. Zugang zum Onlinebanking

Der Teilnehmer erhält Zugang zum Onlinebanking, wenn er

- die Kontonummer und seine PIN übermittelt hat,
- 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 Onlinebanking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

4. Onlinebanking-Aufträge durch den Teilnehmer

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Onlinebanking-Aufträge zu deren Wirksamkeit der Bank mittels Onlinebanking übermitteln. Bei Vorgängen, die zusätzlich der Eingabe einer TAN bedürfen (z.B. Überweisungen) muss der Teilnehmer diese außerdem mit dem vereinbarten Personalisierten Sicherheitsmerkmal (TAN) autorisieren. Nach Erteilung eines Auftrags bestätigt die Bank den Eingang des Auftrags mittels Onlinebanking. 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 oder des Kauf- bzw. Verkaufauftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Onlinebanking-Auftrags 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.

5. Bearbeitung von Onlinebanking-Aufträgen durch die Bank

(1) Die Bearbeitung der Onlinebanking-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 Onlinebanking und im Kontoauszug informiert. Der Ausführungszeitpunkt bei Wertpapieraufträgen ist von der technischen Verfügbarkeit des am Börsenplatz verwendeten Börsensystems abhängig.

(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 Onlinebanking-Datenformat ist eingehalten.
- Das ggf. gesondert vereinbarte Onlinebanking-Verfügungslimit ist nicht überschritten.

- Die Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z.B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

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

(3) Liegen die Ausführungsbedingungen nach Abs. 2 S. 1 nicht vor, wird die Bank den Onlinebanking-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 Onlinebanking zur Verfügung stellen.

6. Information des Kontoinhabers über Onlinebanking-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Onlinebanking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum Onlinebanking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum Onlinebanking nur über die von der Bank gesondert mitgeteilten Onlinebanking-Zugangskanäle (z.B. Internetadresse) herzustellen.

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer hat

- seine Personalisierten Sicherheitsmerkmale geheim zu halten und nur im Rahmen einer Auftragserteilung über die von der Bank gesondert mitgeteilten Onlinebanking-Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument 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 Onlinebanking-Verfahren missbräuchlich nutzen.

(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals (PIN/TAN) sowie des Authentifizierungsinstruments (TAN-Generator) zu beachten:

- PIN und TAN dürfen nicht elektronisch gespeichert werden.
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- PIN und TAN dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z.B. nicht auf Online Händlerseiten).
- PIN und TAN dürfen nicht außerhalb des Onlinebanking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die PIN darf nicht zusammen mit dem Authentifizierungsinstrument (TAN-Generator) verwahrt werden.

7.3 Sicherheit des Kundensystems

Der Teilnehmer muss die Sicherheitshinweise auf der Internetseite der Bank zum Onlinebanking, 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 Onlinebanking-Auftrag (z.B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem 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 des Teilnehmers

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

Fassung Oktober 2010

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.

8.2 Unterrichtungspflicht des Kontoinhabers über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Kontoinhaber hat das Kreditinstitut 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 Onlinebanking-Zugang für ihn oder alle Teilnehmer oder sein Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Onlinebanking-Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den Onlinebanking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der PIN oder der TAN 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.

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die PIN bzw. den TAN-Generator austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber und/oder Teilnehmer unverzüglich.

9.4 Automatische Sperre eines Authentifizierungsinstruments

(1) Wird dreimal hintereinander eine falsche PIN eingegeben, so sperrt die Bank automatisch den Zugang zum Onlinebanking für das Konto. Die Sperre kann durch Eingabe der richtigen PIN und einer gültigen TAN aufgehoben werden.

(2) Wird dreimal hintereinander eine falsche TAN eingegeben, so wird der Onlinebanking-Zugang des betroffenen Teilnehmers gesperrt. In diesem Falle sollte sich der Teilnehmer mit der Bank in Verbindung setzen.

10. Haftung

10.1 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 die jeweilige Auftragsart vereinbarten Bedingungen (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruht ein nicht autorisierter Zahlungsvorgang vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen 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 oder Diebstahl des Authentifizierungsinstruments ein Verschulden trifft.

(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 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.

(5) Kommt es vor der 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 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, nach dem 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 und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2),
- das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2),
- das Personalisierte Sicherheitsmerkmal außerhalb des Onlinebanking-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).

(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungen über die Haftungsgrenze von 150 Euro hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

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

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens 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.

10.2.2 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 sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haftet der Kontoinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung der Bank ab der Sperranzeige

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

10.2.4 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.

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 Landesbank Baden-Württemberg gespeichert.

13. Außergerichtliche Streitschlichtung

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