

Schwäbische Bank

Bedingungen für die konto-/depotbezogene Nutzung des Universal-Banking (HBCI) mit PIN/TAN

1. Leistungsumfang

- (1) Die Bank steht ihrem Kunden für die elektronische Datenübermittlung im Wege des Universal-Banking-Dialogs zur Verfügung.
- (2) Sie gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen des Universal-Bankings nutzen kann. Sofern die Bank für Verfügungen mittels Universal-Banking eine Betragsbegrenzung vorsieht, informiert sie ihn hierüber.

2. Nutzungsberechtigte

Zur Abwicklung von Bankgeschäften verwenden Konto-/Depotinhaber und etwaige Bevollmächtigte jeweils individuelle Identifikations- und Legitimationsmedien. Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als Nutzer bezeichnet.

3. Allgemeine Verfahrensbestimmungen

- (1) Der Nutzer ist verpflichtet, die mit der Bank vereinbarten Übertragungs- und Sicherungsverfahren sowie Datenformate einzuhalten.
- (2) Soweit die Bank dem Nutzer Daten über Aufträge zur Verfügung stellt, die noch nicht endgültig bearbeitet sind, stellen diese lediglich eine unverbindliche Information dar. Die Daten sind jeweils besonders gekennzeichnet.

4. Finanzielle Nutzungsgrenze

- (1) Der Nutzer darf Verfügungen nur im Rahmen des Kontoguthabens oder eines vorher für das Konto eingeräumten Kredites vornehmen.
- (2) Auch wenn der Nutzer diese Nutzungsgrenze bei seinen Verfügungen nicht einhält, ist die Bank berechtigt, den Ersatz der Aufwendungen zu verlangen, die aus der Nutzung des Universal-Banking entstehen. Verfügungen mittels Universal-Banking über das eingeräumte Kreditvolumen hinaus führen weder zur Einräumung eines Kredits noch zur Erhöhung eines zuvor eingeräumten Kredits; die Bank ist berechtigt, in diesem Fall den höheren Zinssatz für geduldete Kontoüberziehungen zu verlangen.

5. Legitimationsverfahren/Geheimhaltung

- (1) Der Nutzer ist verpflichtet, die mit der Bank vereinbarten Sicherungsmaßnahmen durchzuführen.
- (2) Mit Hilfe der mit der Bank vereinbarten Medien identifiziert und legitimiert sich der Nutzer gegenüber der Bank. Der Nutzer hat dafür Sorge zu tragen, dass kein unbefugter Dritter in den Besitz der Identifikations- und Legitimationsmedien kommt sowie Kenntnis von dem zu deren Schutz dienenden Passwort erlangt. Denn jede Person, die im Besitz der Medien ist und das Passwort kennt, kann die vereinbarten Dienstleistungen nutzen. Insbesondere Folgendes ist zur Geheimhaltung der Identifikations- und Legitimationsmedien zu beachten:
 - Die den Nutzer identifizierenden Daten dürfen nicht außerhalb der Sicherheitsmedien, z. B. auf der Festplatte des Rechners, gespeichert werden;
 - das zum Schutz der Identifikations- und Legitimationsmedien dienende Passwort darf nicht notiert oder elektronisch abgespeichert werden;
 - bei Eingabe des Passwortes ist sicherzustellen, dass Dritte dieses nicht ausspähen können.
 - Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht gleichzeitig für das Universal-Banking genutzt werden.
- (3) Der Teilnehmer muß die Sicherheitshinweise auf der Internetseite der Bank zum Universal-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

6. Zugangssperre

- (1) Gehen die zur Identifikation und Legitimation dienenden Medien verloren, werden sie anderen Personen bekannt oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so hat der Nutzer den Universal-Banking-Zugang zum Konto/Depot durch die Bank unverzüglich sperren zu lassen.
- (2) Hat der Nutzer seiner Bank eine Sperre übermittelt, so haftet die Bank ab dem Zugang der Sperrnachricht für alle Schäden, die aus ihrer Nichtbeachtung entstehen.
- (3) Die Bank wird den Universal-Banking-Zugang zum Konto/Depot sperren, wenn der Verdacht einer missbräuchlichen Nutzung des Kontos/Depots über Universal-Banking besteht. Sie wird den Kontoinhaber hierüber außerhalb des Universal-Banking informieren. Diese Sperre kann mittels Universal-Banking nicht aufgehoben werden.

7. Behandlung der vom Nutzer übermittelten Daten durch die Bank

- (1) Die der Bank mittels Universal-Banking erteilten Aufträge, deren Eingang von der Bank elektronisch bestätigt wird, werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet.
- (2) Die Bearbeitung der Universal-Banking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Universal-Banking-Seite der Bank oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der Universal-Banking-Seite der Bank angegebenen oder 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.

- (3) 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 Universal-Banking-Datenformat ist eingehalten.
 - Das gesondert vereinbarte Universal-Banking-Verfügungslimit ist nicht überschritten.
 - Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.
- Liegen die Ausführungsbedingungen nach Satz 2 vor, führt die Bank die Universal-Banking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.
- (4) Ergibt die Legitimationsprüfung Unstimmigkeiten, wird die Bank den betreffenden Auftrag nicht bearbeiten und dem Nutzer hierüber unverzüglich eine Information mittels Universal-Banking zur Verfügung stellen.
- (5) Ergeben sich bei den von der Bank durchgeführten Prüfungen Fehler, so wird die Bank die fehlerhaften Daten nachweisen und sie dem Nutzer unverzüglich bereitstellen. Die Bank ist berechtigt, die fehlerhaften Daten von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrages nicht sichergestellt werden kann.

8. Rückruf oder Änderung von Aufträgen

Der Rückruf oder die Änderung von Aufträgen kann nur außerhalb des Universal-Banking-Verfahrens erfolgen, es sei denn, die Bank sieht eine solche Möglichkeit innerhalb des Verfahrens ausdrücklich vor. Die Bank kann einen Rückruf oder eine Änderung allerdings nur beachten, wenn ihr diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufes möglich ist.

9. Haftung

- (1) Die Haftung der Bank bei einer nicht autorisierten Universal-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Universal-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft.)
- (2) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, 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.
- (3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen, gestohlen 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.
- (4) 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 verstoßen hat.
- (5) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 7.2 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.
- (6) 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 7.2),
 - das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat
 - das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde
 - das Personalisierte Sicherheitsmerkmal außerhalb des Universal-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat
- (7) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.
- (8) Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Universal-Banking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.
- (9) 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.

10. Anwendbares Recht

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