

Bedingungen

für die Nutzung des Online Banking

1. Leistungsangebot

Der Kontoinhaber kann Bankgeschäfte mittels Online Banking in dem von der Hanseatic Bank (nachfolgend „Bank“) angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Online Banking abrufen. Im Rahmen des Online Banking ist der Kontoinhaber zusätzlich berechtigt, Zahlungsauslösedienste gemäß Zahlungsdienstleistungsaufsichtsgesetz und Kontoinformationsdienste gemäß Zahlungsdienstleistungsaufsichtsgesetz zu nutzen. Darüber hinaus kann der Kontoinhaber von ihm ausgewählte Drittdienste nutzen.

2. Voraussetzungen zur Nutzung des Online Banking

(1) Nutzungsberechtigter des Online-Banking-Angebotes der Bank ist der Kontoinhaber. Die Stellvertretung durch andere Personen ist nicht gestattet, um Missbrauch auszuschließen.

(2) Der Kontoinhaber muss für die Abwicklung von Bankgeschäften mittels Online Banking durch die Bank authentifiziert werden. Mit der Authentifizierung überprüft die Bank die Identität des Kontoinhabers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments. Der Kontoinhaber weist sich mit den vereinbarten Authentifizierungselementen als berechtigter Teilnehmer aus und kann Informationen erhalten sowie Aufträge erteilen.

Ein Authentifizierungselement ist:

- ein Element aus der Kategorie Wissen, welches nur dem Kontoinhaber bekannt ist (z. B. Online-Banking-Passwort),
- ein Element aus der Kategorie Besitz als ein Gegenstand, den nur der Kontoinhaber besitzt (z. B. das Mobiltelefon zum Empfang von smsTAN) oder
- ein Element aus der Kategorie Inhärenz als ein nur dem Kontoinhaber innewohnendes persönliches Merkmal (z. B. Fingerabdruck).

(3) Zur Abwicklung von Bankgeschäften mittels Online Banking unter Verwendung von Online-Banking-Passwort und smsTAN dient ein zum Empfang von smsTAN per Textnachricht (SMS) geeignetes Empfangsgerät (z. B. Mobiltelefon). Für das smsTAN-Verfahren wird die Mobilnummer des Kontoinhabers registriert. Sofern Online-Banking-Vorgänge der Eingabe einer smsTAN bedürfen, erhält der Nutzungsberechtigte von der Bank eine Textmeldung (SMS) mit einer smsTAN an die registrierte Mobilnummer. Die so übermittelte smsTAN ist nur für den Vorgang mit der entsprechenden Vorgangsnummer zu nutzen und kann nicht für weitere Vorgänge verwendet werden. Eine nicht genutzte smsTAN verliert zehn Minuten nach ihrer Absendung durch die Bank ihre Gültigkeit und kann auch nicht mehr verwendet werden.

3. Zugang zum Online Banking und Verfahren

(1) Der Kontoinhaber hat mittels Online Banking Zugang zum Konto, wenn er zuvor die Benutzerkennung und das Online-Banking-Passwort und gegebenenfalls jeweils zusätzlich eine smsTAN eingegeben hat.

(2) Es wird ausschließlich das smsTAN-Verfahren angeboten.

4. Bearbeitung von Aufträgen beim Online Banking

(1) Mittels Online Banking erteilte Aufträge werden im Rahmen der Annahme- und Ausführungsfristen im Anschluss an deren Zugang bearbeitet. Der Kontoinhaber muss einem Auftrag zu dessen Wirksamkeit zustimmen (Autorisierung).

(2) Die Bank wird den Auftrag ausführen, wenn

- er durch Eingabe einer gültigen smsTAN vom Kontoinhaber autorisiert wurde,
- das festgelegte Dateiformat eingehalten ist,
- das Konto einen ausreichenden Verfügungshöchstbetrag gemäß Vereinbarung über die Nutzung des Online Banking aufweist und die finanzielle Nutzungsgrenze eingehalten wird.

(3) Sofern die Voraussetzungen nicht vorliegen, wird die Bank den Auftrag nicht ausführen und den Kontoinhaber mittels Online Banking darüber und soweit möglich über die Gründe informieren.

5. Sorgfaltspflichten des Kontoinhabers

(1) Der Kontoinhaber ist verpflichtet, alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (z. B. Online-Banking-Passwort, smsTAN, Mobiltelefon oder mobiles Endgerät, App auf einem mobilen Endgerät) sicher zu verwahren und so vor dem Zugriff anderer Personen zu schützen. Anderenfalls besteht die Gefahr, dass das Online Banking missbräuchlich genutzt wird.

(2) Insbesondere ist zum Schutz der Authentifizierungselemente zu beachten, dass

- Authentifizierungselemente aus dem Bereich Wissen (z. B. Online-Banking-Passwort) geheim zu halten sind und nicht mündlich, in Textform (z. B. E-Mail) oder auf sonstige Weise weitergegeben oder ungesichert gespeichert werden dürfen (z. B. darf das Online-Banking-Passwort nicht auf dem PC oder dem mobilen Endgerät gespeichert werden),
- Authentifizierungselemente nicht auf dem mobilen Endgerät notiert oder zusammen mit dem mobilen Endgerät aufbewahrt werden dürfen,
- Authentifizierungselemente aus dem Bereich Besitz (z. B. mobiles Endgerät zum Empfang der smsTAN) vor dem unbefugten Zugriff Dritter sicher zu verwahren sind,
- Der Kontoinhaber hat sicherzustellen, dass unberechtigte Personen nicht auf das mobile Endgerät zugreifen können,
- mit dem mobilen Endgerät empfangene smsTAN nicht mündlich oder per E-Mail weitergegeben werden dürfen,
- beim smsTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden darf.

(3) Der Kontoinhaber muss die im Verkehr erforderliche Sorgfalt bei der Nutzung des

Online Banking beachten und insbesondere angemessene Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem) treffen. Soweit dem Kontoinhaber Daten aus seinem Online-Banking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät (z. B. Mobiltelefon) zur Bestätigung angezeigt werden, ist der Kontoinhaber verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen. Bei Abweichungen hat der Kontoinhaber die Transaktion abzubrechen.

(4) Die für das smsTAN-Verfahren hinterlegte Mobilnummer ist auf eine neue Mobilnummer zu ändern, wenn der Kontoinhaber diese Telefonnummer nicht mehr für das Online Banking nutzt. Zudem ist in diesem Fall eine installierte App zu deaktivieren.

(5) Ungeachtet der Schutzpflichten ist der Kontoinhaber eines Kartenkontos gegenüber Zahlungsauslösediensten und Kontoinformationsdiensten oder sonstigen Drittdiensten zur Verwendung der erforderlichen Authentifizierungselemente berechtigt, wenn diese Zahlungsaufträge über einen Zahlungsauslösedienst auslösen oder Zahlungskontoinformationen über einen Kontoinformationsdienst anfordern. Der Kontoinhaber hat bei der Auswahl sonstiger Drittdienste die im Verkehr erforderliche Sorgfalt einzuhalten.

6. Änderung des Online-Banking-Passworts

Der Kontoinhaber ist berechtigt, sein Online-Banking-Passwort unter Verwendung einer smsTAN jederzeit zu ändern. Bei Änderung des Online-Banking-Passworts wird sein bisheriges Online-Banking-Passwort ungültig.

7. Sperre des Online-Banking-Angebotes

(1) Stellt der Kontoinhaber den Verlust oder Diebstahl eines Authentifizierungselements aus dem Bereich Besitz, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seiner Authentifizierungselemente fest, muss er die Bank hierüber unverzüglich unterrichten (Sperranzeige).

(2) Der Kontoinhaber hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei anzuzeigen.

(3) Hat der Kontoinhaber den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben und hat sein persönliches Online-Banking-Passwort unverzüglich zu ändern.

8. Nutzungssperre

(1) Die Hanseatic Bank sperrt auf Veranlassung des Kontoinhabers, insbesondere im Fall der Sperranzeige nach Ziffer 7, den Online-Banking-Zugang.

(2) Wird dreimal hintereinander ein falsches Online-Banking-Passwort eingegeben, so sperrt die Bank den Online-Banking-Zugang. Die Sperre kann nur von der Bank wieder aufgehoben werden.

(3) Werden dreimal hintereinander falsche smsTAN eingegeben, so sind keine weiteren smsTAN-Anforderungen möglich. In diesen Fällen sollte sich der Kontoinhaber mit der Bank in Verbindung setzen. Nicht smsTAN-pflichtige Transaktionen sind weiterhin möglich.

(4) Die Bank wird den Online-Banking-Zugang sperren,

- wenn der Verdacht einer missbräuchlichen oder betrügerischen Nutzung des Kontos über den Online-Banking-Zugang besteht,
- wenn sachliche Gründe im Zusammenhang mit der Sicherheit eines Authentifizierungselements dies rechtfertigen, oder
- wenn die Bank berechtigt ist, den Vertrag aus wichtigem Grund zu kündigen.

Die Bank wird den Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre, unterrichten.

(5) Die Bank wird den Online-Banking-Zugang auf Wunsch des Kontoinhabers sperren. Auch diese Sperre kann nicht mittels Online Banking aufgehoben werden.

(6) Die Bank wird eine Sperre aufheben oder das betroffene Authentifizierungselement austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber.

(7) Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zum Konto verweigern, wenn objektive und ausreichend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters zum Konto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Bank wird den Kontoinhaber auf dem vereinbarten Weg möglichst vor, spätestens unverzüglich nach der Verweigerung des Zugangs, unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Pflichten verstoßen würde. Sofern die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Bank die Zugangssperre auf und informiert den Kontoinhaber hierüber unverzüglich.

9. Postbox

(1) Im Rahmen der Geschäftsbeziehung zwischen der Hanseatic Bank und dem Kontoinhaber gilt die Nutzung der Postbox als vereinbarter Kommunikationsweg. In der Postbox werden dem Kontoinhaber Nachrichten der Bank online zur Verfügung gestellt.

(2) Der Kontoinhaber verzichtet durch die Nutzung der Postbox ausdrücklich auf den postalischen Versand aller Dokumente und Nachrichten durch die Bank in papiergebundener Form. Dokumente, die aufgrund rechtlicher Anforderungen von der Bank erstellt werden müssen, insbesondere Kontoauszüge und Kontoabschlüsse, sowie Nachrichten, die den Geschäftsverkehr mit der Bank betreffen, werden dem Kontoinhaber daher grundsätzlich nur in elektronischer Form auf verschlüsselten Seiten in die Postbox im Rahmen des Online Banking übermittelt. Hierbei werden Nachrichten der Bank an den

Kontoinhaber direkt in der Postbox und Kontoauszüge in der Funktion „Eingang“ (Menüpunkt „Postbox“) zur Verfügung gestellt. Die Bank ist berechtigt, dem Kontoinhaber die hinterlegten Dokumente und Nachrichten auf dem Postweg oder auf andere Weise zu übermitteln, wenn gesetzliche Vorgaben dies erforderlich machen oder die Bank dies aufgrund anderer Umstände (z. B. technischer Probleme) unter Berücksichtigung des Kundeninteresses als zweckmäßig erachtet.

(3) Die Bank stellt die Dokumente in der Postbox zur Verfügung und benachrichtigt den Kontoinhaber per E-Mail oder auf sonstige Weise, sobald ein neues Dokument online zur Verfügung steht. Der Kontoinhaber kontrolliert die hinterlegten Dokumente auf Richtigkeit und Vollständigkeit. Beanstandungen sind der Bank unverzüglich, spätestens jedoch sechs Wochen nach Zugang der Dokumente, textlich mitzuteilen. Dokumente, die die Bank in die Postbox eingestellt hat, gelten – soweit sie der Kontoinhaber nicht bereits vorher abgerufen hat – drei Kalendertage nach der Einstellung in die Postbox und Zugang der Nachricht über die Einstellung dem Kontoinhaber als zugegangen. Unbeschadet dessen gehen dem Kontoinhaber eingestellte Dokumente spätestens in dem Zeitpunkt zu, in dem dieser die Dokumente abgerufen hat.

10. Haftung

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstrumentes oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungsinstrumentes, haftet der Kontoinhaber für den hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob ihn ein Verschulden trifft.

(2) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz (1) verpflichtet, wenn

- es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungsinstrumentes vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Authentifizierungsinstrumentes durch einen Angestellten, einen Agenten, eine Zweigniederlassung/Zweigstelle eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten der Bank ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Kontoinhaber in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt

der Kontoinhaber abweichend von Absatz (1) und (2) den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Kontoinhabers kann insbesondere dann vorliegen, wenn er eine seiner unter Ziffer 5 aufgeführten Sorgfaltspflichten verletzt hat.

(4) Abweichend von Absatz (1)–(3) ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Bank eine starke Kundenauthentifizierung nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen. Der Kontoinhaber haftet jedoch, wenn er in betrügerischer Absicht gehandelt hat.

(5) Hat die Bank die Möglichkeit einer Sperre gemäß Ziffer 7 nicht sichergestellt und konnte der Kontoinhaber eine Sperre aus diesem Grunde nicht durchführen, ist er nicht zum Ersatz des Schadens verpflichtet, es sei denn, der Kontoinhaber hat in betrügerischer Absicht gehandelt.

(6) Sobald die Bank eine Sperranzeige eines Kontoinhabers erhalten hat, haftet sie für alle danach durch nicht autorisierte Online-Banking-Verfügungen entstehenden Schäden. Die Haftung der Bank ist ausgeschlossen, wenn der Kontoinhaber in betrügerischer Absicht gehandelt hat.

(7) Beruhen die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis, auf das die 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, sind Haftungsansprüche ausgeschlossen.

11. Anwendbares Recht

Für die Geschäftsbeziehung zwischen dem Kontoinhaber und der Bank gilt deutsches Recht.