Online Banking

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 und Kontoinformationsdienste 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) oder
- ein Element aus der Kategorie Inhärenz als ein nur dem Kontoinhaber innewohnendes persönliches Merkmal (z. B. Fingerabdruck).

(3) Die Authentifizierung des Kontoinhabers erfolgt, indem der Kontoinhaber gemäß der Anforderung der Bank das gesondert vereinbarte Element der Kategorie Wissen, den Nachweis des Elements aus der Kategorie Besitz und/oder den Nachweis des Elements aus der Kategorie Inhärenz an die Bank übermittelt.

3. Zugang zum Online Banking und Freigabeverfahren

(1) Der Kontoinhaber hat mittels Online Banking Zugang zum Konto, wenn er zuvor die Benutzerkennung eingegeben hat und sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselements/Authentifizierungselemente ausweist und keine Sperre des Zugangs vorliegt. Nach Gewährung des Zugangs zum Online Banking kann auf Informationen zugegriffen und können Aufträge erteilt werden. Für den Zugriff auf sensible Zahlungsdaten fordert die Bank den Kontoinhaber auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Online Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kontoinhabers und die IBAN sind für den vom Kontoinhaber genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Daten. Der Kontoinhaber muss einem Auftrag zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu ein Authentifizierungselement zu verwenden. Die Bank bestätigt mittels Online Banking den Eingang des Auftrags. Nach der Erteilung der Zustimmung kann der Kontoinhaber den Auftrag nicht mehr widerrufen.

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 gemäß dem vereinbarten Freigabeverfahren vom Kontoinhaber autorisiert wurde.
- 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 darüber und soweit möglich über die Gründe informieren.

(4) Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Online Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

5. Sorgfaltspflichten des Kontoinhabers

(1) Der Kontoinhaber ist verpflichtet, alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (z. B. Online-Banking-Passwort, Mobiltelefon oder mobiles Endgerät, App auf einem mobilen Endgerät) sicher zu verwahren und 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) vor dem unbefugten Zugriff Dritter sicher zu verwahren sind.
- der Kontoinhaber sicherzustellen hat, dass unberechtigte Personen nicht auf das mobile Endgerät zugreifen können.
- mit dem mobilen Endgerät empfangene Benachrichtigungen nicht mündlich oder per E-Mail weitergegeben werden dürfen.

Weiterhin

- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindlichen Anwendungen (z. B. Karten-App, Authentifizierungs-App) nicht nutzen können
- ist die Anwendung (z.B. Karten-App, Authentifizierungs-App) auf dem mobilen Endgerät des Karteninhabers zu deaktivieren, bevor der Karteninhaber den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons) und
- dürfen die Nachweise des Besitzelements (z. B. TAN, Code) nicht mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden
- dürfen Authentifizierungselemente aus dem Bereich Inhärenz (z.B. der Fingerabdruck des Kontoinhabers) auf einem mobilen Endgerät des Kontoinhabers nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Authentifizierungselemente aus dem Bereich Inhärenz anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, welches für das Online Banking genutzt wird, Authentifizierungselemente aus dem Bereich Inhärenz anderer Personen gespeichert, ist für das Online Banking das von der Bank ausgegebene Wissenselement (z. B. Online-Passwort) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Authentifizierungselement aus dem Bereich Inhärenz.

(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 vereinbarte Authentifizierungsverfahren hinterlegte Mobilfunknummer ist auf eine neue Mobilfunknummer zu ändern, wenn der Kontoinhaber diese Telefonnummer nicht mehr für das Online Banking nutzt.

(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 des vereinbarten Freigabeverfahrens 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. Der Kontoinhaber hat die Bank unverzüglich nach Feststellen eines nicht autorisierten oder fehlerhaft ausgeführten Auftrages hierüber zu unterrichten.

8. Nutzungssperre

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

(2) 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. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

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

(4) 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.

(5) 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 Darlehensnehmer gilt die Nutzung der Postbox als vereinbarter Kommunikationsweg. In der Postbox werden dem Darlehensnehmer Nachrichten der Hanseatic Bank online zur Verfügung gestellt.

2) Der Darlehensnehmer verzichtet durch die Nutzung der Postbox grundsätzlich auf den postalischen Versand von Dokumenten und Nachrichten durch die Hanseatic Bank in papiergebundener Form, so-

weit gesetzliche Vorgaben oder individuelle Vereinbarungen nichts anderes bestimmen. Dokumente, die aufgrund rechtlicher Anforderungen von der Hanseatic Bank erstellt werden müssen, insbesondere Kontoauszüge und Kontoabschlüsse, sowie Nachrichten, die den Geschäftsverkehr mit der Hanseatic Bank betreffen, werden dem Darlehensnehmer daher grundsätzlich nur in elektronischer Form auf verschlüsselten Seiten in die Postbox im Rahmen des Online Banking übermittelt. Die Hanseatic Bank ist berechtigt, dem Darlehensnehmer die hinterlegten Dokumente und Nachrichten auf dem Postweg oder auf andere Weise zu übermitteln, wenn gesetzliche Vorgaben dies erforderlich machen oder die Hanseatic Bank dies aufgrund anderer Umstände (z. B. technischer Probleme) unter Berücksichtigung des Kundeninteresses als zweckmäßig erachtet.
3) Die Hanseatic Bank stellt die Dokumente in der Postbox zur Verfügung und benachrichtigt den Darlehensnehmer per E-Mail oder auf sonstige Weise, sobald ein neues Dokument online zur Verfügung steht. Der Darlehensnehmer kontrolliert die hinterlegten Dokumente auf Richtigkeit und Vollständigkeit. Beanstandungen sind der Hanseatic Bank unverzüglich, in Textform mitzuteilen. Soweit für bestimmte Dokumente besondere Einwendungsfristen gelten, bleiben diese unberührt. Gesetzliche Rechte des Darlehensnehmers bleiben ebenfalls unberührt. Für den Zugang der in die Postbox eingestellten Dokumente und Nachrichten gelten die gesetzlichen Bestimmungen.
4) Ergänzend gelten die Allgemeinen Geschäftsbedingungen sowie die Bedingungen für das Online-Banking der Hanseatic Bank. Soweit diese von den vorstehenden Regelungen zur Postbox abweichen, gehen die vorstehenden Regelungen insoweit vor.

10. Haftung, Berichtigungs- und Erstattungsansprüche

10.1 Haftung der Bank
(1) Im Falle einer nicht autorisierten Online-Banking-Verfügung hat die Bank keinen Anspruch auf Erstattung ihrer Aufwendungen. Die Bank ist verpflichtet, den Betrag unverzüglich zu erstatten und, sofern der Betrag dem Konto belastet worden ist, dieses Konto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung mit der nicht autorisierten Online-Banking-Verfügung befunden hätte. Diese Verpflichtung wird die Bank spätestens bis zum Ende des Geschäftstags erfüllen, an welchem der Kontoinhaber einen nicht autorisierten Zahlungsvorgang angezeigt hat oder die Bank auf andere Weise davon Kenntnis erhalten hat. Hat die Bank einer zuständigen Behörde berechtigte Gründe für den Verdacht, dass ein betrügerisches Verhalten des Zahlers vorliegt, schriftlich mitgeteilt, hat die Bank die Verpflichtung zur Erstattung unverzüglich zu prüfen und zu erfüllen, wenn sich der Betrugsverdacht nicht bestätigt.
(2) Im Falle einer nicht erfolgten oder fehlerhaften Ausführung einer autorisierten Online-Banking-Verfügung kann der Kontoinhaber von der Bank die unverzügliche und ungekürzte Erstattung des Betrages insoweit verlangen, als die Zahlung nicht erfolgte oder fehlerhaft war. Wurde der Betrag dem Konto belastet, bringt die Bank dieses wieder auf den Stand, auf dem es sich ohne den nicht erfolgten oder fehlerhaft ausgeführten Zahlungsvorgang befunden hätte. Soweit von dem Betrag von der Bank oder zwischengeschalteten Stellen Entgelte abgezogen worden sein sollten, übermittelt die Bank zu Gunsten des Kontoinhabers unverzüglich den abgezogenen Betrag. Der Kontoinhaber kann darüber hinaus von der Bank die Erstattung derjenigen Entgelte und Zinsen insoweit verlangen, als dem Kontoinhaber diese im Zusammenhang mit der nicht erfolgten oder fehlerhaften Ausführung der Überweisung in Rechnung gestellt oder dem Konto belastet wurden.
(3) Geht die Online-Banking-Verfügung beim Zahlungsdienstleister des Zahlungsempfängers erst nach Ablauf der Ausführungsfrist ein (Verspätung), kann der Kontoinhaber von der Bank verlangen, dass diese den Zahlungsdienstleister des Empfängers darauf in Anspruch nimmt, dass dieser die Gutschrift auf dem Zahlungskonto des Empfängers so vornimmt, als sei die Online-Banking-Verfügung ordnungsgemäß ausgeführt worden.
(4) Der Kontoinhaber kann im Falle einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung verlangen, dass die Bank den Zahlungsvorgang nachvollzieht und den Kontoinhaber über das Ergebnis unterrichtet.
(5) Im Falle einer nicht erfolgten oder fehlerhaften oder verspäteten Ausführung einer autorisierten Online-Banking-Verfügung ist die Haftung der Bank – unabhängig von dem möglicherweise bestehenden gesetzlichen Erstattungsanspruch – für den über den Erstattungsanspruch hinausgehenden Schaden auf 12.500 € begrenzt, sofern die Bank überhaupt ein Verschulden trifft. Diese Haftungsbegrenzung gilt nicht bei Vorsatz und grober Fahrlässigkeit, für den Zinsschaden und für Gefahren, die die Bank besonders übernommen hat.
(6) Die Haftung der Bank ist ausgeschlossen, wenn im Falle einer nicht erfolgten oder fehlerhaften Ausführung der Online-Banking-Verfügung durch die Bank nachgewiesen wird, dass der Betrag ungekürzt eingegangen ist, oder im Falle einer Verspätung durch die Bank nachgewiesen wird, dass der Betrag rechtzeitig eingegangen ist. Für den Fall, dass eine Online-Banking-Verfügung mit einer vom Kontoinhaber angegebenen fehlerhaften Kundenkennung ausgeführt wurde, ist die Haftung der Bank ebenfalls ausgeschlossen. Der Kontoinhaber kann in diesem Fall jedoch verlangen, dass sich die Bank im Rahmen der eigenen Möglichkeiten darum bemüht, den Zahlungsbetrag wieder zu erlangen. Ist dies nicht möglich, teilt die Bank auf Antrag des Kontoinhabers alle verfügbaren Informationen mit, damit der Kontoinhaber einen Anspruch auf Erstattung geltend machen kann.
(7) Der Kontoinhaber hat die Bank unverzüglich zu unterrichten, falls er feststellt, dass eine Online-Banking-Verfügung nicht autorisiert war oder fehlerhaft ausgeführt worden ist. Ein Erstattungsanspruch ist ausgeschlossen, wenn er nicht innerhalb von 13 Monaten ab dem Tag der Belastung des betreffenden Zahlungsvorgangs gegenüber der Bank angezeigt wird. Für andere Ansprüche als die aus §§ 675u und 675y BGB wegen eines nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorgangs kann der Kontoinhaber den Anspruch auch nach Ablauf der Frist geltend machen, wenn er ohne Verschulden an der Einhaltung der Frist verhindert war. Der Lauf der Frist beginnt nur, wenn die Bank den Kontoinhaber entsprechend den vereinbarten Bedingungen über die resultierende Belastungsbuchung mit dem monatlichen Abschluss (Kontoauszug) auf dem vereinbarten Weg unterrichtet hat, anderenfalls ist für den Fristbeginn der Tag der Unterrichtung maßgeblich.

10.2 Haftung des Kontoinhabers
(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, 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 Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken oder
- der Verlust des Authentifizierungselements 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, eine Sperranzeige gemäß Ziffer 7. vorzunehmen, nicht durch geeignete Mittel 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 des Kontoinhabers erhalten hat, haftet sie für alle danach durch nicht autorisierte Online-Banking-Verfügungen entstehende 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. Änderungen
a) Änderungsangebot
Änderungen der Allgemeinen Geschäfts- und Nutzungsbedingungen und der Sonderbedingungen werden dem Karteninhaber spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in Textform angeboten. Hat der Karteninhaber mit der Bank im Rahmen der Geschäftsbeziehung einen elektronischen Kommunikationsweg vereinbart (zum Beispiel das Online Banking), können die Änderungen auch auf diesem Wege angeboten werden.
b) Annahme durch den Karteninhaber
Die von der Bank angebotenen Änderungen werden nur wirksam, wenn der Karteninhaber diese annimmt, gegebenenfalls im Wege der nachfolgend geregelten Zustimmungsfiktion.
c) Annahme durch den Karteninhaber im Wege der Zustimmungsfiktion
Das Schweigen des Karteninhabers gilt nur dann als Annahme des Änderungsangebots (Zustimmungsfiktion), wenn
cc) das Änderungsangebot erfolgt, um eine Übereinstimmung der vertraglichen Bestimmungen mit einer veränderten Rechtslage wiederherzustellen, weil eine Bestimmung dieser Allgemeinen Geschäfts- und Nutzungsbedingungen
- aufgrund einer Änderung von Gesetzen, einschließlich unmittelbar geltender Rechtsvorschriften der Europäischen Union, nicht mehr der Rechtslage entspricht oder
- durch eine rechtskräftige gerichtliche Entscheidung, auch durch ein Gericht erster Instanz, unwirksam wird oder nicht mehr verwendet werden darf oder
- aufgrund einer verbindlichen Verfügung einer für die Bank zuständigen nationalen oder internationalen Behörde (zum Beispiel der Bundesanstalt für Finanzdienstleistungsaufsicht oder der Europäischen Zentralbank) nicht mehr mit den aufsichtsrechtlichen Verpflichtungen der Bank in Einklang zu bringen ist, und

ccc) der Karteninhaber das Änderungsangebot nicht vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen abgelehnt hat.
Die Bank wird den Karteninhaber im Änderungsangebot auf die Folgen seines Schweigens hinweisen.
d) Ausschluss der Zustimmungsfiktion
Die Zustimmungsfiktion findet keine Anwendung
- bei Änderungen dieser Regelung oder
- bei Änderungen von Entgelten für Bankleistungen, die vom Karteninhaber im Rahmen der Geschäftsverbindung typischerweise dauerhaft in Anspruch genommen werden, oder
- bei Änderungen, die die Hauptleistungspflichten des Vertrages und die Entgelte für Hauptleistungen betreffen, oder
- bei Änderung von Entgelten, die auf eine über das vereinbarte Entgelt für die Hauptleistung hinausgehende Zahlung des Verbrauchers gerichtet sind, oder
- bei Änderungen, die dem Abschluss eines neuen Vertrages gleichkommen, oder
- bei Änderungen, die das bisher vereinbarte Verhältnis von Leistung und Gegenleistung erheblich zu Gunsten der Bank verschieben würden.

In diesen Fällen wird die Bank die Zustimmung des Karteninhabers zu den Änderungen auf andere Weise einholen.
e) Kündigungsrecht des Karteninhabers bei der Zustimmungsfiktion
Macht die Bank von der Zustimmungsfiktion Gebrauch, kann der Karteninhaber den von der Änderung betroffenen Vertrag vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderung auch fristlos und kostenfrei kündigen. Auf dieses Kündigungsrecht wird die Bank den Karteninhaber in ihrem Änderungsangebot besonders hinweisen.

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

BIBV11.11.2026