GABLER-SALITER-BANK

Privatbankiers seit 1828

Erläuterungen zu den Änderungen der Geschäftsbedingungen der Bank für den Zahlungsverkehr zum 14. September 2019

unsere Geschäftsbedingungen zum Zahlungsverkehr haben wir zuletzt zum 13. Januar 2018 angepasst, um die erste Stufe der neuen gesetzlichen Vorgaben zum Zahlungsdiensterecht umzusetzen. Diese beruhen auf der Zweiten EU-Zahlungsdiensterichtlinie und dem diesbezüglichen deutschen Umsetzungsgesetz.

Nunmehr wird am 14. September 2019 die zweite Stufe des Gesetzes in Kraft treten. Damit soll vor allem die Sicherheit im Online Banking und bei Kartenzahlungen gewährleistet werden. Für Zahlungsauslöse- und Kontoinformationsdienste gelten neue Rahmenbedingungen. Zur Umsetzung dieser gesetzlichen Vorgaben und zur Berücksichtigung der technischen Entwicklungen ändern wir mit Wirkung zum 14. September 2019 die Bedingungen für das Online Banking[1], die Bedingungen für die girocard (maestrocard)[2] und die Bedingungen für die Mastercard[3].

Die geänderten Bedingungen finden Sie auf unserer Homepage in unserem Downloadbereich
www.gabler-saliter-bank.de/services/downloads
unter dem Menüpunkt Neuregelungen PSD2 Richtlinien und in den Filialen zur Einsicht- und Mitnahme. Gerne stellen wir Ihnen eine Fassung der neuen Bedingungen auch postalisch zur Verfügung. Erläuterungen zu den wesentlichen Änderungen können Sie dieser Kundeninformation entnehmen.

Die Entgelte, die Annahme- und Ausführungsfristen für Zahlungsaufträge und die Geschäftstage der Bank entnehmen Sie bitte – wie gewohnt – dem „Preisaushang“ und dem „Preis- und Leistungsverzeichnis“.

Bitte haben Sie dafür Verständnis, dass die folgenden Ausführungen auch Erläuterungen zu Bedingungstexten für Produkte enthalten können, deren Nutzung Sie aktuell nicht mit uns vereinbart haben. In diesem Fall sind die entsprechenden Ausführungen sowie die dazugehörigen Kundenbedingungen für Sie gegenstandslos. Die Bedingungen entfalten erst im Zusammenwirken mit den jeweiligen Produktverträgen (zum Beispiel einer Zahlungskaren-Vereinbarung oder Online-Banking Vereinbarung) ihre Wirkung.

1 nur relevant, wenn mit Kunden Online-Banking vereinbart ist.
2 nur relevant, wenn Kunde girocard (maestrocard) der Bank nutzt.
3 nur relevant, wenn Kunde Kreditkarte der Bank nutzt.

GABLER-SALITER-BANK
Privatbankiers seit 1828

Sicherheit durch „starke“ Kundenauthentifizierung

Lösen Sie als Kunde eine Zahlung per Online Banking oder per Zahlungskarte aus, nutzen Sie die mit uns als Bank vereinbarten Authentifizierungselemente. Dies sind beispielsweise die Online Banking-PIN und -TAN oder die Zahlungskarte und Zahlungskarten-PIN. Damit können wir als Bank feststellen, dass tatsächlich Sie als Kunde diese Vorgänge veranlassen. Die Zweite EU-Zahlungsdiensterichtlinie erkennt diese Authentifizierungsverfahren an und regelt diese nunmehr gesetzlich:

- Grundsätzlich soll eine „starke“ Kundenauthentifizierung erfolgen. Das heißt, Sie müssen sich gegenüber uns als Bank mit zwei Authentifizierungselementen ausweisen. Dies können Wissenselemente (z.B. PIN, Passwort), Besitzelemente (z.B. Karte oder Mobiltelefon zum TAN-Empfang) und Seinselemente (z.B. Fingerabdruck) sein. Bei Erteilung von Zahlungsaufträgen im Online Banking und bei Kartenzahlungen verwenden Sie deshalb – wie bisher – zwei Elemente (z.B. Online Banking-PIN und-TAN, Zahlungskarte und Zahlungkarten-PIN). Neu ist allerdings Folgendes: Beim Zugriff auf Kontoinformationen im Online Banking müssen Sie ebenfalls zwei Authentifizierungselemente – beispielsweise Online Banking-PIN und –TAN - einsetzen, wie Sie es bereits von der Erteilung von Zahlungsaufträgen im Online Banking gewohnt sind.

- Allerdings erlauben die gesetzlichen Vorschriften in bestimmten Fällen, von Ihnen als Kunden nur ein einziges Authentifizierungselement anzufordern. So kann es z.B. im Online Banking beim wiederholten Abruf von Kontoinformationen innerhalb einer bestimmten Zeitspanne ausreichen, nur ein Authentifizierungselement einzusetzen (z.B. Online Banking-PIN). Bei Kartenzahlungen ist es beispielsweise weiterhin möglich, zur Zahlung von geringen Beträgen die Zahlungskarte ohne gesonderte PIN-Eingabe zu nutzen. Wird nur ein Authentifizierungselement abgefragt, ist der Kunde haftungsrechtlich besonders geschützt.

Was bedeutet das für Sie konkret? Wie gewohnt setzen Sie entsprechend der jeweiligen Anforderung der Bank im Online Banking oder bei Kartenzahlungen die mit Ihnen vereinbarten Authentifizierungselemente ein. Das gilt auch, wenn Sie im Online Banking Drittdienste, wie Zahlungsauslösedienste oder Kontoinformationsdienste, nutzen.

[4

Änderungen in den „Bedingungen für das Online Banking“

Allgemein

Die Bedingungen sind in etlichen Passagen überarbeitet worden, um die gesetzlichen Neuerungen inklusive der Änderung von Begriffen und die verfahrenstechnischen Entwicklungen zu berücksichtigen.

4 nur relevant, wenn Kunde Online-Banking vereinbart ist.

Nutzung von Drittdiensten

Wie schon zum 13. Januar 2018 in den Bedingungstext eingefügt, sind Sie als Kunde berechtigt, durch die Zweite EU-Zahlungsdiensterichtlinie regulierte Zahlungsauslösedienste und Konto-informationsdienste zu nutzen. Diese unterliegen der in dem jeweiligen EU-Mitgliedstaat zuständigen Bankaufsicht, in Deutschland ist dies die Bundesanstalt für Finanzdienstleistungsaufsicht. Ab dem 14. September 2019 treten weitere Regelungen zur Gewährleistung der Online Banking-Sicherheit in Kraft, die sich nicht an Sie als Kunden, sondern an Zahlungsauslösedienste, Kontoinformationsdienste und Banken richten.

Zur Klarstellung wird nunmehr ergänzt, dass Sie auch sonstige von Ihnen ausgewählte Drittdienste nutzen können, die nicht von der EU-Zahlungsdiensterichtlinie erfasst sind. Wichtig hierbei: Sonstige Drittdienste unterliegen nicht unbedingt der Bankenaufsicht und sollten deshalb von Ihnen sorgfältig auswählt werden, um in Ihrem Interesse die Sicherheit des Online Banking zu schützen (vgl. dazu auch Nummer 7.1. Absatz 5).

Neuer Begriff „Authentifizierungselement“

Um im Online Banking Informationen abzurufen oder Aufträge zu erteilen, müssen Sie sich mit den mit uns gesondert vereinbarten Authentifizierungselementen, beispielsweise Online-PIN und –TAN, ausweisen (vgl. auch Nummer 3 und 4). Damit können wir als Bank die Berechtigung des Online Banking-Zugriffs prüfen (Authentifizierung). Um einerseits den neuen gesetzlichen Vorgaben zu entsprechen und anderseits den Bedingungstext technikneutral zu halten, werden die bisherigen Begriffe „Authentifizierungsinstrument“ und „personalisiertes Sicherheitsmerkmal“ durch den neuen Sammelbegriff „Authentifizierungselement“ ersetzt. Sodann werden entsprechend dem Gesetz die Unterarten, nämlich Wissens-, Besitz- und Seinselemente, beschrieben.

Mit dem neuen Sammelbegriff „Authentifizierungselement“ ändern sich auch weitere Regelungen. So sind die „Authentifizierungselemente“ nunmehr der Bezugspunkt für die Regelungen über den Zugang zum Online Banking (Nummer 3), die Auftragserteilung (Nummer 4), die Sorgfaltspflichten (Nummer 7.1), die Sperranzeigepflicht (Nummer 8.1), die Nutzungssperre (Nummer 9) und die Haftung (Nummer 10).

Sorgfaltspflichten

Ihre Sorgfaltspflichten im Online Banking werden wegen der Einführung des neuen Sammelbegriffs „Authentifizierungselemente“ und der technischen Entwicklungen aktualisiert (Nummer 7.1).

Allgemein gilt weiterhin: Zum Schutz Ihrer Authentifizierungselemente vor unbefugtem Zugriff müssen Sie - wie bisher - alle zumutbaren Vorkehrungen treffen. Anderenfalls besteht die Gefahr, dass das Online Banking von Unbefugten missbräuchlich genutzt werden könnte.

In Nummer 7.1 Absatz 2 werden die Schutzpflichten wie bisher an Hand von Regelbeispielen beschrieben, die nach den Kategorien Wissen, Besitz und Sein untergliedert sind. Die einzelnen Verhaltenspflichten sind an aktuelle Entwicklungen angepasst worden. Indem Sie diese Sorgfaltspflichten beachten, schützen Sie das Online Banking und reduzieren Betrugsrisiken. Bei vorsätzlicher oder grob fahrlässiger Verletzung dieser Sorgfaltspflichten könnten Sie für den hieraus entstandenen Schaden haften (vgl. Nummer 10.2.1 Absatz 3).

Sie können das Online Banking auch mittels Kontoinformationsdiensten, Zahlungsauslösediensten und von Ihnen ausgewählten sonstigen Drittdiensten nutzen (vgl. Nummer 1 Absatz 1) und hierbei Ihre Authentifizierungselemente verwenden (Nummer 7.1 Absatz 5 Satz 1). Sofern Sie „sonstige Drittdienste“ nutzen, die nicht vom Zahlungsdienstaufsichtsgesetz und damit der Bankenaufsicht erfasst werden, müssen Sie diese sorgfältig auswählen (Nummer 7.1 Absatz 5 Satz 2), um die Sicherheit des Online Banking auch in Ihrem Interesse zu schützen.

[5

Änderungen in den „Bedingungen für die girocard“

Haftung bei fehlender starker Kundenauthentifizierung

In Umsetzung der gesetzlichen Vorgaben wird für den Fall einer fehlenden „starken“ Kundenauthentifizierung bei der Kartenzahlung mit dem neuen Absatz 6 in Nummer A.II.15.1 eine besondere Haftungsregelung zugunsten des Kunden aufgenommen. Diese Haftungsbefreiung gilt aber nicht, wenn der Kunde in betrügerischer Absicht gehandelt hat.

[6

Änderungen in den „Bedingungen für die MasterCard“

Verwendungsmöglichkeiten

Aufgrund der technischen Weiterentwicklungen kann die Kreditkarte auch als digitale Karte zur Nutzung auf einem mobilen Endgerät (z.B. Smartphone) ausgegeben werden. Sollten Sie eine solche digitale Karte nutzen wollen, ist dies gesondert mit uns als Bank zu vereinbaren. Neben den Kreditkartenbedingungen gelten dann gesonderte Nutzungsbedingungen (vgl. Nummer 1.1 am Ende).

Autorisierung von Kartenzahlungen durch den Karteninhaber

Die Nutzungsmöglichkeiten der Kreditkarte und die hierbei einzusetzenden Authentifizierungselemente sind aufgrund der gesetzlichen Vorgaben und der technischen Weiterentwicklungen aktualisiert worden.

Beim Bezahlen mit der Kreditkarte bei Vertragsunternehmen vor Ort (beispielsweise an der Ladenkasse, an Parkautomaten) kann in bestimmten Fällen auf die Eingabe der Karten-PIN verzichtet werden (vgl. Nummer 3.1 Absatz 3).

5 nur relevant, wenn Kunde girocard (maestrocard) der Bank nutzt.
6 nur relevant, wenn Kunde Kreditkarte der Bank nutzt.

Bei Online-Bezahlvorgängen (beispielsweise Karteneinsatz im Online-Handel) erfolgt die Authentifizierung des Karteninhabers – vergleichbar zum Online Banking - mit den jeweils angeforderten Authentifizierungselementen aus den Kategorien Wissen, Besitz und/oder Sein (vgl. Nummer 3.1 Absatz 3). Welche Authentifizierungselemente hierfür konkret zur Verfügung stehen, richtet sich nach gesonderter Vereinbarung mit uns. Der statt dem bisherigen Begriff „personalisiertes Sicherheitsmerkmal“ eingeführte Sammelbegriff „Authentifizierungselement“ ist aus den neuen gesetzlichen Vorgaben abgeleitet. Er ist technikneutral, um die verschiedenen von den Kreditkartenorganisationen unterstützten Verfahren erfassen zu können. Der Sammelbegriff wird dann auch in den weiteren Regelungen mit Bezug zu Online-Bezahlvorgängen verwendet (vgl. u.a. Nummer 3.1 Absatz 2, Nummer 8.6, Nummer 13).

Schutz der Authentifizierungselemente für Online-Bezahlvorgänge

Die Sorgfaltspflichten des Karteninhabers in Bezug auf seine Authentifizierungselemente für Online-Bezahlvorgänge werden nach dem Vorbild der „Bedingungen für das Online Banking“ konkretisiert. Zum Schutz Ihrer Authentifizierungselemente vor unbefugtem Zugriff müssen Sie - wie bisher - alle zumutbaren Vorkehrungen treffen. Anderenfalls besteht die Gefahr, dass Ihre Kreditkarte für Online-Bezahlvorgänge von Unbefugten missbräuchlich genutzt werden könnte.

In Nummer 8.4 Absatz 2 werden die Schutzpflichten an Hand von Regelbeispielen beschrieben, die nach den Kategorien Wissen, Besitz und Sein untergliedert sind. Indem Sie diese Sorgfaltspflichten beachten, schützen Sie Online-Bezahlvorgänge mit Ihrer Kreditkarte und reduzieren Betrugsrisiken. Bei vorsätzlicher oder grob fahrlässiger Verletzung dieser Sorgfaltspflichten könnten Sie für den hieraus entstandenen Schaden haften (vgl. Nummer 13.1 Absatz 4).

Kontrollpflichten bei Online-Bezahlvorgängen

Wegen des Sachzusammenhangs schließt sich die Regelung zur Kontrollpflicht bei Online-Bezahlvorgängen an Nummer 8.4 an.

Haftung bei fehlender starker Kundenauthentifizierung

In Umsetzung der gesetzlichen Vorgaben wird für den Fall einer fehlenden „starken“ Kundenauthentifizierung bei der Kartenzahlung mit dem neu formulierten Absatz 7 in Nummer 13.1 eine besondere Haftungsregelung zugunsten des Kunden aufgenommen. Diese Haftungsbefreiung gilt aber nicht, wenn der Kunde in betrügerischer Absicht gehandelt hat.] [7]

7 nur relevant, wenn Kunde Kreditkarte der Bank nutzt.

GABLER-SALITER-BANK
Privatbankiers seit 1828

[8

Änderungen in den „Bedingungen für Datenfernübertragung“

Die wesentlichen Anpassungen sind Folgende:

Verhaltens- und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags

Die Anforderungen an den Umgang mit Legitimationsmedien für die Autorisierung von Aufträgen werden präzisiert (Nummer 4). Zusätzlich darf zum Zweck der Risikobegrenzung nunmehr das Legitimationsmedium nicht dupliziert werden (Nummer 4 Absatz 2, 3. Spiegelstrich).

Anlage 1a - EBICS-Anbindung

Die Anlage 1a, Nummer 3 des Bedingungswerks enthält neue besondere Sorgfalts-pflichten, die der Kunde beachten muss, wenn er Legitimations- und Sicherungsmedien selbst erzeugt. Dabei handelt es sich um folgende Punkte:

- In allen Phasen der Authentifizierung sind die Vertraulichkeit und Integrität des Legitimationsmediums zu gewährleisten.
- Private Teilnehmerschlüssel auf den Legitimations- und Sicherungsmedien dürfen nicht im Klartext abgespeichert werden.
- Spätestens nach fünfmaliger Fehleingabe des Passwortes hat eine Sperrung des Legitimationsmediums zu erfolgen.
- Die Generierung der privaten und öffentlichen Teilnehmerschlüssel muss in einer sicheren Umgebung erfolgen.
- Die Legitimations- und Sicherungsmedien sind ausschließlich und eindeutig dem Teilnehmer zuzuordnen und zu verwenden.

8 nur relevant, wenn mit dem Kunden DFÜ-Verfahren vereinbart ist.