OstseeSparkasse Rostock

Echt von hier.
Nah bei mir.
Meine OSPA.

OstseeSparkasse Rostock · Am Vögenteich 23 · 18057 Rostock

Kundeninformation zu den Änderungen der Bedingungen für das Online-Banking

Sehr geehrte Kundin,
sehr geehrter Kunde,

am 14. September 2019 treten neue gesetzliche Bestimmungen für die Erbringung von Zahlungsdiensten in Kraft. Diese beruhen auf den europäischen Vorgaben der Zweiten EU-Zahlungsdiensterichtlinie (PSD 2), die unter anderem der Gewährleistung der Sicherheit und des Vertrauens bei elektronischen Zahlungen dienen. Daher ändern wir mit Wirkung zum 14. September 2019 die Bedingungen für das Online-Banking.

Die geänderten Bedingungen für das Online-Banking finden Sie unter www.ospa.de/psd2. Die Änderungen sind jeweils rot gekennzeichnet. Die wesentlichen Änderungen können Sie dieser Kundeninformation entnehmen.

I. Sicherheit im Online-Banking durch Kundenauthentifizierung

Im Online-Banking nutzen Sie für den Zugang („Login“) oder die Erteilung von Aufträgen die mit uns vereinbarten Authentifizierungselemente, wie z.B. PIN und TAN. Hierdurch können wir feststellen, dass tatsächlich Sie als unser Kunde diese Vorgänge veranlassen.
Die neuen gesetzlichen Bestimmungen erkennen diese Authentifizierungsverfahren an und regeln diese nunmehr auch gesetzlich. So ist ab dem 14. September 2019 im Online-Banking grundsätzlich eine sogenannte starke Kundenauthentifizierung erforderlich. Das bedeutet, dass zwei voneinander unabhängige Authentifizierungselemente aus den Kategorien Wissen, Besitz und Sein (z.B. eine PIN als Wissenselement oder ein Mobiltelefon, an welches eine TAN übermittelt wird, als Besitzelement) einzusetzen sind. Den Einsatz von zwei Authentifizierungselementen (z.B. Eingabe PIN und TAN) kennen Sie bereits im Zusammenhang mit der Erteilung von Zahlungsaufträgen (wie z.B. Überweisungen). Zukünftig kann dies auch in anderen Fällen, z.B. beim Zugriff auf Kontoinformationen (Kontostand, Umsätze) erforderlich sein.

Nach den gesetzlichen Bestimmungen sind auch Ausnahmen möglich. So können wir als Sparkasse in bestimmten Fällen auf den Einsatz eines zweiten Authentifizierungselements verzichten. So kann z.B. nicht bei jedem Login, sondern nur in regelmäßigen Abständen zusätzlich der Einsatz eines zweiten Authentifizierungselements (z.B. Eingabe einer TAN) erforderlich sein.

II. Änderungen der Bedingungen für das Online-Banking

1. Beschreibung des Verfahrens zur Kundenauthentifizierung

In Nummer 2 wird der neue Begriff „**Authentifizierung**“ eingeführt. Dabei handelt es sich um das Verfahren, mit dessen Hilfe wir Sie identifizieren oder die berechtigte Verwendung eines Zahlungsinstrumentes überprüfen können (Nummer 2 Absatz 2). Ihre Authentifizierung ist die Voraussetzung für die Nutzung des Online-Banking (Nummer 2 Absatz 1). Sie erfolgt anhand der zwischen Ihnen und uns vereinbarten Authentifizierungselemente (Nummer 2 Absätze 2 und 4).

In Nummer 2 Absatz 3 wird der neue Begriff „**Authentifizierungselement**“ eingeführt. Authentifizierungselemente sind

- Wissenselemente, also etwas, das nur Sie wissen (z.B. Ihre PIN),
- Besitzelemente, also etwas, das nur Sie besitzen (z.B. Ihre SparkassenCard mit TANGenerator oder ein Mobiltelefon, an welches eine TAN übermittelt wird), oder
- Seinselemente, also etwas, das nur Sie sind (z.B. Ihr Fingerabdruck als biometrisches Merkmal).

Mit Ihren Authentifizierungselementen können Sie sich im Online-Banking als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (z.B. Kontostände und Umsätze) sowie Aufträge (z.B. Überweisungen) erteilen (Nummer 2 Absatz 2). Welche Authentifizierungselemente Sie im Online-Banking einsetzen müssen, richtet sich nach der mit Ihnen getroffenen Vereinbarung.
Für Ihre Authentifizierungselemente gelten besondere Sorgfaltspflichten (Nummer 7.1), die Pflicht zur Sperranzeige (Nummer 8.1), die Regelungen zur Nutzungssperre (Nummer 9) sowie die Regelungen zur Haftung (Nummer 10).

Zudem wird der bereits oben erläuterte Begriff der „**starken Kundenauthentifizierung**“ eingeführt (Nummer 10.2.1 Absatz 4).

2. Ihre Sorgfaltspflichten zur Sicherheit des Online-Banking

Aufgrund der neuen gesetzlichen Bestimmungen und der damit einhergehenden technischen Anpassungen an die neuen Sicherheitsanforderungen haben sich auch ihre Sorgfaltspflichten als Teilnehmer im Online-Banking geändert (Nummer 7.1).

Zum Schutz Ihrer Authentifizierungselemente vor unbefugtem Zugriff müssen Sie alle zumutbaren Vorkehrungen treffen. Anderenfalls besteht die Gefahr, dass das Online-Banking missbräuchlich genutzt wird. Um dies zu verhindern müssen Sie nach Nummer 7.1 Absatz 2 insbesondere

- Ihre Wissenselemente (z.B. Ihre PIN) geheim halten,
- Ihre Besitzelemente (z.B. Ihre SparkassenCard mit TAN-Generator oder Ihr Mobiltelefon, an welches eine TAN übermittelt wird) vor Missbrauch schützen und
- bei der Verwendung von Seinselementen (z.B. Ihr Fingerabdruck als biometrisches Merkmal) beachten, dass auf Ihrem mobilen Endgerät (z.B. Mobiltelefon mit Fingerabdrucksensor) keine anderen Seinselemente anderer Personen gespeichert sind.

Wir bitten Sie, die Sorgfaltspflichten sorgfältig zu lesen. Indem Sie die Sorgfaltspflichten beachten, schützen Sie das Online-Banking und reduzieren Betrugsrisiken. Bei vorsätzlicher oder grob fahrlässiger Verletzung der Sorgfaltspflichten können Sie zudem für den hieraus entstandenen Schaden haften.

3. Nutzung des Online-Bankings mittels Kontoinformationsdiensten, Zahlungsauslösediensten und sonstigen Drittdiensten

Sie können das Online-Banking auch mittels Kontoinformationsdiensten, Zahlungsauslösediensten und von Ihnen ausgewählten sonstigen Drittdiensten nutzen (Nummer 1 Absatz 1). Ihre Authentifizierungselemente dürfen Sie auch gegenüber einem von ihnen ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden. Sofern Sie sonstige Drittdienste nutzen, müssen Sie diese sorgfältig auswählen (Nummer 7.1 Absatz 5).

Den gesetzlichen Regelungen entsprechend, können wir nach Nummer 9.5 Kontoinformations- und Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformations- oder des Zahlungsauslösedienstleisters zum Zahlungskonto es rechtfertigen. Über die Sperre sowie ggf. über die Aufhebung der Sperre wird der Kontoinhaber informiert.