Stadtsparkasse Cuxhaven

Kundeninformation zu den Änderungen der Bedingungen für das Online-Banking

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 TAN-Generator 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).

Stadtsparkasse Cuxhaven

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.

Bedingungen für das Online-Banking

(gültig ab 14. September 2019)

Fassung ~~13. Januar 2018~~ 14. September 2019

1 Leistungsangebot

(1) Der Konto-/Depotinhaber und dessen Bevollmächtigte können Bankgeschäfte mittels Online-Banking in dem von der Sparkasse angebotenen Umfang abwickeln. Zudem können sie Informationen der Sparkasse mittels Online-Banking abrufen. ~~Der Inhaber eines Zahlungskontos und dessen Bevollmächtigte~~ Des Weiteren sind ~~zusätzlich~~ sie gemäß § 675f Absatz 3 BGB berechtigt, ~~für die Auslösung eines Zahlungsauftrages einen Zahlungsauslösedienst~~ Zahlungsauslösedienste gemäß § 1 Absatz 33 Zahlungsdiensteaufsichtsgesetz ~~zu nutzen~~ (ZAG) und ~~für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienst~~ Kontoinformationsdienste gemäß § 1 Absatz 34 ~~Zahlungsdiensteaufsichtsgesetz~~ ZAG zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.

(2) Konto-/Depotinhaber und Bevollmächtigte werden ~~im Folgenden~~ einheitlich als „Teilnehmer“ ~~bezeichnet.~~ , Konto und Depot ~~werden im Folgenden~~ einheitlich als „Konto“ bezeichnet, es sei denn, dies ist ~~im Folgenden~~ ausdrücklich anders bestimmt.

(3) Zur Nutzung des Online-Banking gelten die mit der Sparkasse gesondert vereinbarten Verfügungslimite. Eine Änderung dieser Limite kann der Konto-/Depotinhaber mit seiner Sparkasse gesondert vereinbaren. Bevollmächtigte können nur eine Herabsetzung vereinbaren.

2 Voraussetzungen zur Nutzung des Online-Banking

(1) Der Teilnehmer ~~benötigt für die Nutzung des~~ kann das Online-Banking nutzen, wenn die Sparkasse ihn authentifiziert hat.

(2) Authentifizierung ist das mit der Sparkasse gesondert vereinbarte Verfahren, mit dessen Hilfe die Sparkasse die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten ~~Personalisierten Sicherheitsmerkmale und Zahlungsinstrumente, um~~ Zahlungsinstruments überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Sparkasse als berechtigter Teilnehmer ~~auszuweisen~~ ausweisen, auf Informationen zugreifen (siehe Nummer 3) ~~und~~ sowie Aufträge ~~zu autorisieren~~ erteilen (siehe Nummer 4).

(3) Authentifizierungselemente sind

- Wissenselemente, also etwas, das nur der ~~Authentifizierung bzw. Autorisierung vereinbart werden.~~
  ~~**2.1 Personalisierte Sicherheitsmerkmale**~~
  ~~Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die die Sparkasse dem~~ Teilnehmer ~~zum Zwecke der Authentifizierung bzw. Autorisierung bereitstellt.~~
  ~~Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind beispielsweise: – die~~ weiß (z. B. persönliche Identifikationsnummer ~~(PIN)~~ [PIN]),
- ~~einmal verwendbare Transaktionsnummern (TAN),~~ Besitzelemente, also etwas, das nur der ~~Nutzungscode für die elektronische Signatur.~~
  ~~**2.2 Zahlungsinstrumente**~~
  ~~Zahlungsinstrumente sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Sparkasse und dem Kontoinhaber vereinbart wurden und die vom~~ Teilnehmer ~~zur Erteilung eines Online-Banking-Auftrags verwendet werden. Insbesondere mittels folgender Zahlungsinstrumente kann das Personalisierte Sicherheitsmerkmal~~ besitzt (z. B. ~~TAN) dem Teilnehmer~~ Gerät zur ~~Verfügung gestellt werden: – PIN-Brief, – TAN-Generator, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur~~ Erzeugung ~~von TAN ist (chipTAN), –Online-Banking-App auf einem mobilen Endgerät (z. B. Mobiltelefon) zum Empfang~~ oder ~~zur Erzeugung von TAN, mobiles Endgerät (z. B. Mobiltelefon)~~ zum Empfang von ~~TAN per SMS (smsTAN), – Chipkarte~~ einmal verwendbaren Transaktionsnummern [TAN], die den Besitz des Teilnehmers nachweisen, wie die Sparkassen-Card mit ~~Signaturfunktion~~ TAN-Generator oder das mobile Endgerät), oder
- ~~sonstiges Zahlungsinstrument, auf dem sich Signaturschlüssel befinden.~~ Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

(4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Sparkasse das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Sparkasse übermittelt.

3 Zugang zum Online-Banking

(1) Der Teilnehmer erhält Zugang zum Online-Banking der Sparkasse, wenn

- ~~der Teilnehmer die Kontonummer oder~~ er seine individuelle Teilnehmerkennung (z. B. Kontonummer, Anmeldename) angibt und ~~seine PIN~~
- er sich unter Verwendung des oder ~~elektronische Signatur übermittelt oder sein biometrisches Merkmal eingesetzt hat, – die Prüfung dieser Daten bei~~ der von der Sparkasse ~~eine Zugangsberechtigung des Teilnehmers ergeben hat~~ angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.

Nach Gewährung des Zugangs zum Online-Banking kann ~~der Teilnehmer~~ auf Informationen ~~abrufen~~ zugegriffen oder können nach Nummer 4 Aufträge ~~erteilen.~~ erteilt werden.

~~Die Sätze 1 und 2 gelten auch, wenn Zahlungsaufträge über einen~~

(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z. B. zum Zweck der Änderung der Anschrift des Konto-/Depotinhabers) fordert die Sparkasse den Teilnehmer 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 Kontonummer sind für den vom Teilnehmer genutzten Zahlungsauslösedienst ~~ausgelöst~~ und ~~Zahlungskontoinformationen über einen~~ Kontoinformationsdienst ~~angefordert werden (siehe Nummer~~ keine sensiblen Zahlungsdaten (§ 1 Absatz ~~1~~ 26 Satz ~~3~~ 2 ZAG).

4 ~~Online-Banking~~-Aufträge

4.1 Auftragserteilung ~~und Autorisierung~~

Der Teilnehmer muss ~~Online-Banking-Aufträge~~ einem Auftrag (z. B. ~~Überweisungen~~ Überweisung) zu ~~deren~~ dessen Wirksamkeit ~~mit dem von der Sparkasse bereit gestellten Personalisierten Sicherheitsmerkmal~~ zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z. B. Eingabe einer TAN ~~oder elektronische Signatur) oder mit dem vereinbarten biometrischen Sicherheitsmerkmal autorisieren und der Sparkasse mittels Online-Banking übermitteln, sofern mit der Sparkasse nichts anderes vereinbart wurde.~~ als Nachweis des Besitzelements) zu verwenden.

Die Sparkasse bestätigt mittels Online-Banking den Eingang des Auftrags.

~~Die Sätze 1 und 2 gelten auch, wenn der Inhaber eines Zahlungskontos und dessen Bevollmächtigte Zahlungsaufträge über einen Zahlungsauslösedienst (siehe Nummer 1 Absatz 1 Satz 3) auslösen und übermitteln.~~

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines ~~Online-Banking~~-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Bedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen, es sei denn, die Sparkasse sieht eine Widerrufsmöglichkeit im Online-Banking ausdrücklich vor.

5 Bearbeitung von ~~Online-Banking-Aufträgen~~ Aufträge durch die Sparkasse

(1) Die Bearbeitung der ~~Online-Banking~~-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Online-Banking-Seite der Sparkasse oder im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen ~~Arbeitslaufes~~ Arbeitsablaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Sparkasse ~~angegebenen~~ oder im „Preis- und Leistungsverzeichnis“ ~~bestimmten~~ angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Online-Banking-Seite der Sparkasse oder „Preis- und Leistungsverzeichnis“ der Sparkasse, so gilt der Auftrag als am ~~darauffolgenden~~ darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem ~~Tag~~ Geschäftstag.

(2) Die Sparkasse wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1).
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten (vgl. Nummer 1 Absatz 3).
- Die weiteren ~~Ausführungsvoraussetzungen~~ Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Bedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Sparkasse die ~~Online-Banking~~-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Bedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

~~182 410.000~~ 182 410.050 D1 (Fassung ~~Jan. 2018~~ 14/09/2019) - v2.2 1.0 ~~e~~

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Sparkasse den ~~Online-Banking-~~Auftrag nicht ausführen. Sie wird ~~dem~~ den Teilnehmer hierüber mittels Online-Banking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6 Information des Kontoinhabers über Online-Banking-Verfügungen

Die Sparkasse unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7 Sorgfaltspflichten des Teilnehmers

7.1 ~~Technische Verbindung zum Online-Banking~~ Schutz der Authentifizierungselemente

(1) Der Teilnehmer ~~ist verpflichtet,~~ hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die ~~technische Verbindung zum Online-Banking über~~ Gefahr, dass das Online-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vgl. Nummer 3 und 4).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

(a) Wissenselemente, wie z. B. die ~~von der Sparkasse gesondert mitgeteilten Online-Banking-Zugangskanäle~~ PIN, sind geheim zu halten; sie dürfen insbesondere
- nicht mündlich (z. B. ~~Internetadresse) herzustellen. Der Inhaber eines Zahlungskontos und dessen Bevollmächtigte können zur Auslösung von Zahlungsaufträgen und zur Anforderung von Zahlungskontoinformationen auch über einen von ihnen ausgewählten Zahlungsauslösedienst~~ telefonisch oder ~~Kontoinformationsdienst (siehe Nummer 1 Absatz 1 Satz 3) die technische Verbindung zum~~ persönlich) mitgeteilt werden,
- nicht außerhalb des Online-Banking ~~herstellen.~~ in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden,
- nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. Sparkassen-Card mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Online-Banking und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z. B. die Sparkassen-Card mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
- sind die Sparkassen-Card mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können,
- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für das Online-Banking (z. B. Online-Banking-App, Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für das Online-Banking (z. B. Online-Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons),
- dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online-Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben werden und
- muss der Teilnehmer, der von der Sparkasse einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das Online-Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online-Banking des Teilnehmers aktivieren.

(c) Seinselemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online-Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online-Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Online-Banking das von der Sparkasse ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Beim smsTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (z. B. Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.

(4) Die für das smsTAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Online-Banking nicht mehr nutzt.

(5) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 4 darf der Teilnehmer seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden (siehe Nummer 1 Absatz 1 Sätze 3 und 4). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

~~7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Zahlungsinstrumente~~

~~(1) Der Teilnehmer hat~~
- ~~seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten sowie~~
- ~~sein Zahlungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.~~

~~Denn jede andere Person, die im Besitz des Zahlungsinstruments ist, kann in Verbindung mit der Kenntnis des dazugehörigen Personalisierten Sicherheitsmerkmals das Online-Banking-Verfahren missbräuchlich nutzen.~~

~~Die Geheimhaltungspflicht bezüglich der Personalisierten Sicherheitsmerkmale nach Satz 1 gilt nicht für den Inhaber eines Zahlungskontos und dessen Bevollmächtigte gegenüber Zahlungsauslösediensten und Kontoinformationsdiensten (siehe Nummer 1 Absatz 1 Satz 3), wenn diese Zahlungsaufträge über einen Zahlungsauslösedienst auslösen oder Zahlungskontoinformationen über einen Kontoinformationsdienst anfordern.~~

~~(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Zahlungsinstruments zu beachten:~~

~~a) Das Personalisierte Sicherheitsmerkmal darf nicht ungesichert elektronisch gespeichert werden.~~

~~b) Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.~~

~~c) Das Personalisierte Sicherheitsmerkmal darf nicht per E-Mail oder anderen Telekommunikationsmitteln weitergegeben werden.~~

~~d) Das Personalisierte Sicherheitsmerkmal (z. B. PIN) darf nicht zusammen mit dem Zahlungsinstrument verwahrt werden.~~

~~e) Der Teilnehmer darf zur Autorisierung z. B. eines Auftrags oder der Aufhebung einer Sperre nicht mehr als eine TAN verwenden.~~

~~f) Beim smsTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht für das Online-Banking genutzt werden.~~

7.~~3~~ 2 Sicherheitshinweise der Sparkasse

Der Teilnehmer muss die Sicherheitshinweise auf der Online-Banking-Seite der Sparkasse ~~zum Online-Banking~~, insbesondere die Maßnahmen zum Schutz der von ihm eingesetzten Hard- und Software ~~(Kundensystem)~~, beachten.

7.~~4~~ 3 ~~Kontrolle~~ Prüfung der Auftragsdaten mit von der Sparkasse angezeigten Daten

~~Soweit die~~ Die Sparkasse zeigt dem Teilnehmer ~~Daten aus seinem Online-Banking-Auftrag~~ die von ihr empfangenen Auftragsdaten (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) ~~im Kundensystem oder~~ über ~~ein anderes~~ das gesondert vereinbarte Gerät des Teilnehmers an (z. B. mittels mobilem Endgerät, Chipkartenlesegerät mit Display). ~~Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der~~ Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für ~~die Transaktion~~ den Auftrag vorgesehenen Daten zu prüfen. ~~Bei Feststellung von Abweichungen ist die Transaktion abzubrechen.~~

8 Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl ~~des Zahlungsinstruments,~~ eines Besitzelements zur Authentifizierung (z. B. Sparkassen-Card mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung ~~seines Zahlungsinstruments oder~~ eines ~~seiner Personalisierten Sicherheitsmerkmale~~ Authentifizierungselements

fest, muss der Teilnehmer die Sparkasse hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann ~~der Sparkasse~~ eine solche Sperranzeige jederzeit auch über ~~eine~~ die gesondert ~~mitgeteilte Telefonnummer aufgeben.~~ mitgeteilten Kommunikationskanäle abgeben.

(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.

(3) Hat der Teilnehmer den Verdacht~~, dass eine andere Person unberechtigt~~
- ~~den Besitz an seinem Zahlungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder~~

~~182 410 000~~ 182 410.050 D1 (Fassung ~~Jan. 2018~~ 14/09/2019) - v2.2 1.0 -e

– das Zahlungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet,
einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Konto-/Depotinhaber hat die Sparkasse unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9 Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Sparkasse sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1,
– den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
– ~~sein Zahlungsinstrument.~~ seine Authentifizierungselemente zur Nutzung des Online-Banking.

9.2 Sperre auf Veranlassung der Sparkasse

(1) Die Sparkasse darf den Online-Banking-Zugang für einen Teilnehmer sperren, wenn
– sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
– sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des ~~Zahlungsinstruments oder des Personalisierten Sicherheitsmerkmals~~ Teilnehmers dies rechtfertigen oder
– der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung ~~des Zahlungsinstruments~~ eines Authentifizierungselements besteht.

(2) Die Sparkasse wird den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Sparkasse hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

9.3 Aufhebung der Sperre

Die Sparkasse wird eine Sperre aufheben oder ~~das Personalisierte Sicherheitsmerkmal bzw. das Zahlungsinstrument~~ die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber unverzüglich.

9.4 Automatische Sperre eines chip-basierten ~~Zahlungsinstruments~~ Besitzelements

(1) ~~Die~~ Eine Chipkarte mit Signaturfunktion sperrt sich selbst, wenn ~~dreimal in Folge~~ der Nutzungscode für die elektronische Signatur ~~dreimal in Folge~~ falsch eingegeben wird.

(2) Ein TAN-Generator als Bestandteil einer Chipkarte (z. B. Sparkassen-Card), der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.

(3) Die in ~~den~~ Absätzen 1 und 2 genannten ~~Zahlungsinstrumente~~ Besitzelemente können dann nicht mehr für das Online-Banking genutzt werden. Der Teilnehmer kann sich mit der Sparkasse in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

9.5 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

Die Sparkasse kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Kontoinhabers verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Sparkasse wird den Kontoinhaber über eine solche Zugangsverweigerung auf dem vereinbarten Weg unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die Sparkasse hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Sparkasse die Zugangssperre auf. Hierüber unterrichtet sie den Kontoinhaber unverzüglich.

10 Haftung

10.1 Haftung der Sparkasse bei ~~einer~~ Ausführung eines nicht autorisierten ~~Online-Banking-Verfügung~~ Auftrags und ~~einer~~ eines nicht, fehlerhaft oder verspätet ausgeführten ~~Online-Banking-Verfügung~~ Auftrags

Die Haftung der Sparkasse bei ~~einer~~ einem nicht autorisierten ~~Online-Banking-Verfügung~~ Auftrag und ~~einer~~ einem nicht, fehlerhaft oder verspätet ausgeführten ~~Online-Banking-Verfügung~~ Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Bedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung ~~eines Personalisierten Sicherheitsmerkmals oder eines Zahlungsinstruments~~ der Authentifizierungselemente

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

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

(2) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn
– es ~~ihm~~ dem Teilnehmer nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des ~~Zahlungsinstruments~~ Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
– der Verlust des ~~Zahlungsinstruments~~ Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung~~/Zweigstelle~~ eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine ~~Anzeige-~~ Sorgfalts- und ~~Sorgfaltspflichten~~ Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere ~~dann~~ vorliegen, wenn er eine seiner Sorgfaltspflichten nach
~~a) den Verlust oder Diebstahl des Zahlungsinstruments oder die missbräuchliche Nutzung des Zahlungsinstruments oder des Personalisierten Sicherheitsmerkmals der Sparkasse nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1 Absatz 1),~~
~~b) das Personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe Nummer 7.2 Absatz 2 a),~~
~~c) das Personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1),~~
~~d) das Personalisierte Sicherheitsmerkmal per E-Mail oder anderen Telekommunikationsmitteln weitergegeben hat (siehe Nummer 7.2 Absatz 2 c),~~
~~e) das Personalisierte Sicherheitsmerkmal auf dem Zahlungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 d),~~
~~f) mehr als eine TAN zur Autorisierung eines Auftrags verwendet (siehe Nummer 7.2 Absatz 2 e),~~
~~g) beim smsTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Online-Banking nutzt (siehe Nummer 7.2 Absatz 2 f).~~
– Nummer 7.1 Absatz 2,
– Nummer 7.1 Absatz 4,
– Nummer 7.3 oder
– Nummer 8.1 Absatz 1

verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Sparkasse vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 ~~Zahlungsdiensteaufsichtsgesetz~~ ZAG nicht verlangt hat~~, obwohl die Sparkasse zur starken Kundenauthentifizierung nach § 68 Absatz 4 Zahlungsdiensteaufsichtsgesetz verpflichtet war~~. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen ~~Elementen~~ Authentifizierungselementen aus den Kategorien Wissen ~~(etwas, das der Teilnehmer weiß, z. B. PIN)~~, Besitz ~~(etwas, das der Teilnehmer besitzt, z. B. TAN-Generator)~~ oder ~~Inhärenz (etwas, das der Teilnehmer ist, z. B. Fingerabdruck)~~ Sein (siehe Nummer 2Absatz 3).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den ~~der Verfügungsrahmen~~ das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf ~~den vereinbarten Verfügungsrahmen~~ das vereinbarte Verfügungslimit.

(6) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach ~~den Absätzen~~ Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Sparkasse nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(8) Ist der Kontoinhaber kein Verbraucher, gilt ergänzend Folgendes:
– Der Kontoinhaber haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach ~~den~~

~~182 410 000~~ 182 410.050 D1 (Fassung ~~Jan. 2018~~ 14/09/2019) - v2.2 1.0 ~~e~~

~~Absätzen~~ Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
– Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

10.2.2 Haftung des Konto-/Depotinhabers bei nicht autorisierten ~~Wertpapiertransaktionen~~ Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige
Beruhen nicht autorisierte ~~Wertpapiertransaktionen~~ Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige auf der Nutzung eines ~~verloren gegangenen~~ verlorengegangenen oder gestohlenen ~~Zahlungsinstruments~~ Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des ~~Personalisierten Sicherheitsmerkmals oder des Zahlungsinstruments~~ Authentifizierungselements und ist der Sparkasse hierdurch ein Schaden entstanden, haften der Konto-/Depotinhaber und die Sparkasse nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung ~~der Sparkasse~~ ab der Sperranzeige
Sobald die Sparkasse eine Sperranzeige ~~des~~ eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-Banking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.2.4 Haftungsausschluss
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.

11 Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit
Für die Beilegung von Streitigkeiten mit der Sparkasse kann sich der Konto-/Depotinhaber an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.

~~182 410.000~~ 182 410.050 D1 (Fassung ~~Jan. 2018~~ 14/09/2019) - ~~v2.2~~ 1.0 ~~e~~