Hinweise für mehr Sicherheit im Internet

Fassung Oktober 2015

Berliner Sparkasse
Alexanderplatz 2, 10178 Berlin

Bevor Sie Online-Banking nutzen oder Ihre Kreditkarte im Internet einsetzen, nehmen Sie sich bitte einige Minuten Zeit für die nachfolgenden wichtigen Informationen.

Fit für das Internet

Wer die wichtigsten Grundregeln beachtet, kann sich gegen Angriffe aus dem Internet weitestgehend schützen. Erläuterungen, wie Sie Betrugsversuche erkennen, Ihren Computer und den Zugang zum Internet absichern sowie wichtige Hinweise zu aktuellen Betrugsversuchen erhalten Sie auf: www.berliner-sparkasse.de/sicherheit

- Aktualisieren Sie regelmäßig Ihr Betriebssystem und Ihre eingesetzten Programme.
- Arbeiten Sie nicht mit Administrator-rechten auf Ihrem Computer.
- Halten Sie Firewall und Virenscanner immer aktuell.
- Löschen Sie nach Geschäften über das Internet immer Browserverlauf und Cache.
- Erledigen Sie Bankgeschäfte oder online-Einkäufe nie über ein fremdes WLAN.
- Hinterlegen Sie keine persönlichen Zugangsdaten auf fremden Portalen, geben diese auch nicht an Dritte weiter.
- Achten Sie darauf, dass Sie Online-Geschäfte nur über eine verschlüsselte Verbindung tätigen.
- Für Online-Banking oder einen Einkauf im Internet geben Sie die Internet-Adresse immer von Hand ein.
- Öffnen Sie keine Dateianhänge in E-Mails von unbekannten Absendern.
- Folgen Sie nie Aufforderungen, die Sie per E-Mail oder Telefon erhalten, Zahlungsaufträge zu bestätigen.

Sicheres Online-Banking und Bezahlen im Internet. Diese Regeln sollten Sie unbedingt beachten:

Besser: vorsichtig sein

Mit der Eingabe der TAN wird im Regelfall eine Abbuchung von Ihrem Konto bestätigt. Denken Sie daran, wenn Sie nach Ihren Bankdaten oder einer TAN gefragt werden, ohne dass Sie eine Transaktion in Auftrag geben wollen.

Misstrauisch sein

Wenn Ihnen etwas seltsam vorkommt, brechen Sie im Zweifel lieber die Aktion ab. Ihre Sparkasse wird Sie z. B. niemals auffordern, eine TAN für Gewinn-spiele, Sicherheits-Updates oder vermeintliche Rücküberweisungen einzugeben.

Sorgfältig: Daten kontrollieren

Auf dem Display Ihres TAN-Generators oder Ihres Mobiltelefons werden Ihnen die wichtigsten Auftragsdaten angezeigt. Falls die Anzeigedaten nicht mit Ihrem Auftrag übereinstimmen, brechen Sie die Aktion ab.

Geschlossen: sichere Eingabe

Wenn Sie Ihre Anmeldedaten zum Online-Banking eingeben: Schauen Sie immer, ob das Schloss-symbol im Browser vorhanden ist.

Immer: aufmerksam bleiben

Kontrollieren Sie regelmäßig die Umsätze auf Ihrem Konto. Das geht im Online-Banking und mit Ihren Kontoauszügen. Nur so erkennen Sie unberechtigte Abbuchungen rechtzeitig und fristgerecht.

Eingrenzen: Tageslimit

Legen Sie ein Tageslimit für Ihre Transaktionen im Online-Banking fest. Mit Ihrem persönlichen Verfügungsrahmen schränken Sie die Möglichkeiten unberechtigter Zugriffe ein.

Im Zweifel: Zugang sperren

Falls Sie den Verdacht haben, dass mit der Banking-Anwendung irgendetwas nicht stimmt: Sperren Sie Ihren Zugang. Wenden Sie sich dazu direkt an uns: 030 869 869 57.

200.717 11/2015

Hinweise für mehr Sicherheit im Internet

Fassung Oktober 2015

Berliner Sparkasse
Alexanderplatz 2, 10178 Berlin

So einfach führen Sie eine Überweisung im Online-Banking durch:

Melden Sie sich mit Ihrem Anmeldenamen bzw. Ihrer Legitimations-ID sowie Ihrer 5-stelligen Online-Banking-PIN im Online-Banking an.

Erstellen Sie Ihren Auftrag und senden Sie diesen ab.

Der nächste Schritt unterscheidet sich je nachdem, welches Sicherungsverfahren Sie nutzen:

chipTAN:

Auf dem Bildschirm erscheint nun eine sogenannte animierte Grafik. Führen Sie Ihre SparkassenCard in den TAN-Generator ein und drücken Sie die Taste „F“.

Halten Sie den TAN-Generator an den Bildschirm auf die animierte Grafik. Die Daten werden nun über die lichtempfindlichen Kontakte auf der Rückseite übertragen.

Auf dem Display des TAN-Generators werden nun die wichtigsten Daten Ihres Auftrages angezeigt.

smsTAN:

Nach wenigen Sekunden erhalten Sie eine SMS mit den wichtigsten Daten Ihres Auftrages und einer speziell für diese eine Transaktion generierten TAN auf Ihr registriertes Handy.

pushTAN:

Wechseln Sie zur S-pushTAN-App und melden Sie sich dort mit dem von Ihnen vergebenen Zugangspasswort an. Anschließend werden in der App die wichtigsten Daten des Auftrags angezeigt.

Für alle drei Verfahren gilt:

Wichtig: Prüfen Sie die Daten auf ihre Richtigkeit (bei einer Überweisung z. B. die letzten 10 Stellen der IBAN und den Betrag).

Bei chipTAN: Bestätigen Sie mit der Taste „OK“. Anschließend wird Ihnen die für diesen Auftrag errechnete TAN angezeigt.

Stimmen die Daten überein, können Sie den Auftrag am PC mit der übermittelten TAN freigeben. Fertig!

Wenn es um Geld geht, muss auch die Kommunikation besonders sicher sein.

Nutzen Sie für die Kommunikation keine unverschlüsselte E-Mail. Diese Nachrichten können im Internet von Dritten mitgelesen werden. Für eine sichere Kommunikation mit uns oder sonstigen Dienstleistern stehen in der Internet-Präsenz Kontaktformulare zur Verfügung, über die eine Nachricht verschlüsselt übertragen wird.

Wichtige Informationen zu Veränderungen rund um Ihr Online-Banking und die verwendeten Sicherungsverfahren erhalten Sie von uns ausschließlich postalisch, als Nachricht über Ihr Elektronisches Postfach im Online-Banking oder als Information auf: www.berliner-sparkasse.de/sicherheit bereitgestellt.

In solchen Fällen werden wir Sie nie über eine E-Mail informieren. Bitte reagieren Sie daher niemals auf Aufträge und Anfragen per E-Mail, in denen der Eindruck vermittelt wird, dass diese von uns zugestellt worden sind. Solchen Mails beigefügte Anhänge öffnen Sie bitte niemals.

Sie haben weitere Fragen? Wir sind für Sie da!

Online-Banking-Hotline (Mo-Fr 08:00 - 19:00 Uhr, Sa 09:00 - 14:00 Uhr)	030 869 869 57
Kreditkarten-Service	030 245 524 00

Es fallen die mit Ihrem Anbieter vereinbarten Festnetz- bzw. Mobilfunkpreise an.

200.717 11/2015

Berliner Sparkasse

Bedingungen für das Online-Banking (Stand 31.10.2009)

Hinweis: Diese Bedingungen gelten für die Geschäftsverbindung des Kunden mit der Landesbank Berlin AG einschließlich ihrer Niederlassung "Berliner Sparkasse" - nachstehend einheitlich mit "Landesbank" bezeichnet.

1. Leistungsangebot
(1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels Online-Banking in dem von der Landesbank angebotenen Umfang abwickeln. Zudem kann er Informationen der Landesbank mittels Online-Banking abrufen.
(2) Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer" bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto" bezeichnet.
(3) Zur Nutzung des Online-Banking gelten die mit der Landesbank gesondert vereinbarten Verfügungslimite. Eine Änderung dieser Limite kann der Konto/Depotinhaber mit der Landesbank gesondert vereinbaren. Bevollmächtigte können nur eine Herabsetzung vereinbaren.

2. Voraussetzungen zur Nutzung des Online-Banking
Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels Online-Banking die mit der Landesbank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Landesbank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4).

2.1 Personalisierte Sicherheitsmerkmale
Personalisierte Sicherheitsmerkmale sind:
- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN),
- der Nutzungscode für die elektronische Signatur.

2.2 Authentifizierungsinstrumente
Die TAN beziehungsweise die elektronische Signatur können dem Teilnehmer auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:
- auf einer Liste mit einmal verwendbaren TAN,
- mittels eines TAN-Generators, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist (chipTAN),
- mittels eines mobilen Endgerätes (z. B. Mobiltelefon) zum Empfang von TAN per SMS (smsTAN),
- auf einer Chipkarte mit Signaturfunktion oder
- auf einem sonstigen Authentifzierungsinstrument, auf dem sich Signaturschlüssel befinden.

Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

3. Zugang zum Online-Banking
Der Teilnehmer erhält Zugang zum Online-Banking, wenn
- der Teilnehmer die Kontonummer oder seine individuelle Kundenkennung und seine PIN oder elektronische Signatur übermittelt hat,
- die Prüfung dieser Daten bei der Landesbank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummer 8.1 und 9) vorliegt.

Nach Gewährung des Zugangs zum Online-Banking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

4. Online-Banking-Aufträge
4.1 Auftragserteilung und Autorisierung
Der Teilnehmer muss Online-Banking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (TAN oder elektronische Signatur) autorisieren und der Landesbank mittels Online-Banking übermitteln. Die Landesbank bestätigt mittels Online-Banking den Eingang des Auftrags.
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-Bankings erfolgen, es sei denn, die Landesbank sieht eine Widerrufmöglichkeit im Online-Banking ausdrücklich vor.

5. Bearbeitung von Online-Banking-Aufträgen durch die Landesbank
(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 Landesbank oder im „Preis- und Leistungsverzeichnis" bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Landesbank angegebenen oder im „Preis- und Leistungsverzeichnis" bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis" der Landesbank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.
(2) Die Landesbank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- Der Teilnehmer hat sich mit seinem Personalisierten Sicherheitsmerkmal autorisiert.
- 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.
- Die Ausführungsvoraussetzungen 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 Landesbank 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.
(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Landesbank dem Online-Banking-Auftrag nicht ausführen und den Teilnehmer eine Information über die Nichtausführung und -soweit möglich- über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Online-Banking zur Verfügung stellen.

6. Information des Kontoinhabers über Online-Banking-Verfügungen
Die Landesbank 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
Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online-Banking nur über die von der Landesbank gesondert mitgeteilten Online-Banking-Zugangskanäle (z. B. Internetadresse) herzustellen.
7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente
(1) Der Teilnehmer hat
- seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der Landesbank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen Personalisierten Sicherheitsmerkmal das Online-Banking-Verfahren missbräuchlich nutzen.
(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:
a) Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (z. B. beim Kundensystem).
b) Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
c) Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf Online-Händlerseiten).
d) Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
e) Die PIN und der Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
f) Der Teilnehmer darf zur Autorisierung z. B. eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung einer neuen TAN-Liste nicht mehr als eine TAN verwenden.
g) Beim smsTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht für das Online-Banking genutzt werden.

7.3 Sicherheit des Kundensystems
Der Teilnehmer muss die Sicherheitshinweise der Landesbank zum Online-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.
(1) Das für das Online-Banking vom Teilnehmer genutzte System ist durch technische Maßnahmen gegen das Ausspähen der Sicherheitsmerkmale zu sichern.
(2) Es ist ein Betriebssystem einzusetzen, das dessen Hersteller für den Zugang zum Internet vorgesehen hat und für das er bei Bedarf Programmänderungen (z.B. Sicherheitspatches) zur Verfügung stellt, die erkannte Sicherheitsrisiken beheben. Die Systemeinstellungen sind entsprechend den Herstellerempfehlungen vorzunehmen. Bietet der Hersteller mehrere Sicherheitsstufen an, ist eine hohe Sicherheitsstufe ein zustellen. Zusätzlich ist - soweit technisch verfügbar - das System durch ein Antivirenprogramm zu schützen sowie der Datenverkehr durch ein Firewallprogramm zu kontrollieren.
(3) Betriebssystem, Programme, die den Zugang zum Internet vermitteln (z.B. Browser) sowie die installierten Schutzprogramme sind nach den Empfehlungen des jeweiligen Herstellers aktuell sicher zu halten.
(4) Weiterführende Hinweise zum Schutz des Teilnehmersystems sind den Sicherheitshinweisen der Landesbank zu entnehmen, die auf den Internetseiten für das Online-Banking veröffentlicht und aktualisiert werden.
(5) Bei Nutzung der Chipkarte als Authentifizierungsinstrument hat der Teilnehmer nur den von der Landesbank gesondert mitgeteilten Lesegerät-Typ zu verwenden.
7.4 Kontrolle der Auftragsdaten mit von der Landesbank angezeigten Daten
Soweit die Landesbank dem Teilnehmer Daten aus seinem Online-Banking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z. B. Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

SPK182410000

8. Anzeige- und Unterrichtspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines Persönlichen Sicherheitsmerkmals fest, muss der Teilnehmer die Landesbank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Landesbank eine Sperranzeige jederzeit auch über eine gesondert mitgeteilte Telefonnummer aufgeben.

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

(3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt

- den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder
- das Authentifizierungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet,

muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Kontoinhaber hat die Landesbank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Landesbank 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 Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Landesbank

(1) Die Landesbank 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 des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.

(2) Die Landesbank wird den/die Konto-/Depotinhaber bzw. den/die Teilnehmer unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

9.3 Aufhebung der Sperre

Die Landesbank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den/die Konto-Depotinhaber bzw. den/die Teilnehmer unverzüglich.

9.4 Automatische Sperre eines chipbasierten Authentifizierungsinstruments

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

(2) Ein TAN-Generator, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.

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

10. Haftung

10.1 Haftung der Landesbank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung

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

10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

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 verlorengegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Landesbank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigem Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Kontoinhaber für den der Landesbank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 Euro nach Absatz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen gehandelt hat.

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Landesbank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(5) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere dann vorliegen, wenn er

a) den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals der Landesbank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1 Absatz 1),
b) das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2 Absatz 2 a),
c) das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1 Satz 1),
d) das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2 c),
e) das Personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2 d),
f) das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 e),
g) mehr als eine TAN zur Autorisierung eines Auftrags verwendet (siehe Nummer 7.2 Absatz 2 f),
h) 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 g).

(6) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

10.2.2. Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Landesbank hierdurch ein Schaden entstanden, haften der Kontoinhaber und die Landesbank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3. Haftung der Landesbank ab der Sperranzeige

Sobald die Landesbank eine Sperranzeige des 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 Beschwerdemöglichkeiten

Für die Beilegung von Streitigkeiten mit der Landesbank kann sich der Teilnehmer an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.

12. Brokerage

Sofern sich die Rahmenvereinbarung auf ein Depotkonto erstreckt, können Wertpapierorder zu den nachfolgenden Bedingungen erteilt werden:

(1) Die Landesbank ist berechtigt, die Ausführung von Aufträgen abzulehnen, die nicht den bisherigen Wertpapierproduktgruppen (=Risikoklassen) des Teilnehmers entsprechen.

(2) Der Teilnehmer ist verpflichtet, eindeutige und vollständige Aufträge zu erteilen. Bei Kauf- oder Verkaufsaufträgen ist in Zweifelsfällen die ISIN-(International Securities Identification Number) bzw. Wertpapierkenn-Nummer entscheidend. Bei unvollständigen und nicht eindeutigen Aufträgen ist die Landesbank nicht verpflichtet, den Auftrag auszuführen.

(3) Die Buchung der Gegenwerte von Kauf oder Verkauf von Wertpapieren erfolgt ausschließlich auf dem bei dem Depotkonto hinterlegten Erträgnis- bzw. Verrechnungskonto.

(4) Auf Anfrage werden dem Teilnehmer Verkaufsunterlagen über Investmentfonds von Kapitalanlagegesellschaften vor Ordererteilung zugesandt bzw. mitgeteilt, wo und auf welche Weise diese Unterlagen kostenlos erhältlich sind.

Hinweis: Brokerage kann erst nach einer Aufklärung nach dem Wertpapierhandelsgesetz genutzt werden.

Bedingungen für das Online-Banking

(gültig ab 13. Januar 2018)

Fassung 13.01.2018

Berliner Sparkasse
Alexanderplatz 2, 10178 Berlin

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 sind zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrages einen Zahlungsauslösedienst gemäß § 1 Absatz 33 Zahlungsdiensteaufsichtsgesetz zu nutzen und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienst gemäß § 1 Absatz 34 Zahlungsdiensteaufsichtsgesetz zu 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
Der Teilnehmer benötigt für die Nutzung des Online-Banking die mit der Sparkasse vereinbarten Personalisierten Sicherheitsmerkmale und Zahlungsinstrumente, um sich gegenüber der Sparkasse als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4). Statt eines Personalisierten Sicherheitsmerkmals kann auch ein biometrisches Merkmal des Teilnehmers zum Zwecke 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 persönliche Identifikationsnummer (PIN),
– einmal verwendbare Transaktionsnummern (TAN),
– 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 (z. B. TAN) dem Teilnehmer 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 mit Signaturfunktion oder
– sonstiges Zahlungsinstrument, auf dem sich Signaturschlüssel befinden.

3 Zugang zum Online-Banking
Der Teilnehmer erhält Zugang zum Online-Banking, wenn
– der Teilnehmer die Kontonummer oder seine individuelle Teilnehmerkennung und seine PIN oder elektronische Signatur übermittelt oder sein biometrisches Merkmal eingesetzt hat,
– die Prüfung dieser Daten bei der Sparkasse eine Zugangsberechtigung des Teilnehmers ergeben hat und
– keine Sperre des Zugangs (siehe Nummer 8.1 und 9) vorliegt.
Nach Gewährung des Zugangs zum Online-Banking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.
Die Sätze 1 und 2 gelten auch, wenn Zahlungsaufträge über einen Zahlungsauslösedienst ausgelöst und Zahlungskontoinformationen über einen Kontoinformationsdienst angefordert werden (siehe Nummer 1 Absatz 1 Satz 3).

4 Online-Banking-Aufträge
4.1 Auftragserteilung und Autorisierung
Der Teilnehmer muss Online-Banking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem von der Sparkasse bereit gestellten Personalisierten Sicherheitsmerkmal (z. B. 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. 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 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. Geht der Auftrag nach dem auf der Online-Banking-Seite der Sparkasse angegebenen oder im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Sparkasse, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.
(2) Die Sparkasse wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
– Der Teilnehmer hat den Auftrag autorisiert.
– 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.
– Die weiteren Ausführungsvoraussetzungen 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.
(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Sparkasse den Online-Banking-Auftrag nicht ausführen. Sie wird dem 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
Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online-Banking über die von der Sparkasse gesondert mitgeteilten Online-Banking-Zugangskanäle (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 oder Kontoinformationsdienst (siehe Nummer 1 Absatz 1 Satz 3) die technische Verbindung zum Online-Banking herstellen.

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.

manuell
182 410.500 D1 (Fassung Jan. 2018) - v1.1 - o

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

7.4 Kontrolle der Auftragsdaten mit von der Sparkasse angezeigten Daten
Soweit die Sparkasse dem Teilnehmer Daten aus seinem Online-Banking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z. B. Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion 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, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Zahlungsinstruments oder eines seiner Personalisierten Sicherheitsmerkmale fest, muss der Teilnehmer die Sparkasse hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Sparkasse eine Sperranzeige jederzeit auch über eine gesondert mitgeteilte Telefonnummer aufgeben.
(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch 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
– das Zahlungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet,
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.

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 des Zahlungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
– der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Zahlungsinstruments besteht.
(2) Die Sparkasse wird den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

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

9.4 Automatische Sperre eines chip-basierten Zahlungsinstruments
(1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn der Nutzungscode für die elektronische Signatur dreimal in Folge falsch eingegeben wird.
(2) Ein TAN-Generator als Bestandteil einer Chipkarte, 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 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.

10 Haftung

10.1 Haftung der Sparkasse bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Online-Banking-Verfügung
Die Haftung der Sparkasse bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Online-Banking-Verfügung 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
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, gestohlenen oder sonst abhanden gekommenen Zahlungsinstruments oder auf der sonstigen missbräuchlichen Verwendung eines Zahlungsinstruments, 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 nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Zahlungsinstruments vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
– der Verlust des Zahlungsinstruments 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- und Sorgfaltspflichten 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
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).
(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 nicht verlangt hat, obwohl die Sparkasse zur starken Kundenauthentifizierung nach § 68 Absatz 4 Zahlungsdiensteaufsichtsgesetz verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbeson-

manuell
182 410.500 D1 (Fassung Jan. 2018) - v1.1 - o

dere die Verwendung von zwei voneinander unabhängigen Elementen 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).
(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.
(6) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 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 Absätzen 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 Depotinhabers bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige
Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verloren gegangenen oder gestohlenen Zahlungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Zahlungsinstruments und ist der Sparkasse hierdurch ein Schaden entstanden, haften der 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 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.

manuell

182 410.500 D1 (Fassung Jan. 2018) - v1.1 - o