

Sonderbedingungen für das Sparda-Online-Banking

Fassung: Oktober 2009

1. Leistungsangebot

(1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels Sparda-Online-Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Sparda-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 Sparda-Online-Banking gelten die mit der Bank gesondert vereinbarten Verfügungslimits. Eine Änderung dieser Limits kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

2. Voraussetzungen zur Nutzung des Sparda-Online-Banking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels Sparda-Online-Banking die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (vgl. Nummer 3) und Aufträge zu autorisieren (vgl. Nummer 4).

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind:

- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN).

2.2 Authentifizierungsinstrumente

Die TAN kann dem Teilnehmer auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:

- auf einer Liste mit einmal verwendbaren TAN,
- mittels eines mobilen Endgerätes (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobile TAN).

3. Zugang zum Sparda-Online-Banking

Der Teilnehmer erhält Zugang zum Sparda-Online-Banking, wenn

- der Teilnehmer die Kundennummer und seine PIN übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (vgl. Nummer 8.1 und 9) vorliegt.

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

4. Sparda-Online-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Sparda-Online-Banking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten personalisierten Sicherheitsmerkmal (TAN) autorisieren und der Bank mittels Sparda-Online-Banking übermitteln. Die Bank bestätigt mittels Sparda-Online-Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

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

5. Bearbeitung von Sparda-Online-Banking-Aufträgen durch die Bank

(1) Die Bearbeitung der Sparda-Online-Banking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Sparda-Online-Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der Sparda-Online-Banking-Seite der Bank 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 Bank, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen.

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

- Der Teilnehmer hat sich mit dem personalisierten Sicherheitsmerkmal autorisiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das Sparda-Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Sparda-Online-Banking-Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Sonderbedingungen für den Überweisungsverkehr) liegen vor.

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

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Sparda-Online-Banking-Auftrag nicht ausführen und dem 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 Sparda-Online-Banking zur Verfügung stellen.

6. Information des Kontoinhabers über Sparda-Online-Banking-Verfügungen

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

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum Sparda-Online-Banking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum Sparda-Online-Banking nur über die von der Bank gesondert mitgeteilten Sparda-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 (vgl. Nummer 2.1) geheim zu halten und nur im Rahmen einer Auftragserteilung über die von der Bank gesondert mitgeteilten Sparda-Online-Banking-Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument (vgl. 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 Sparda-Online-Banking-Verfahren missbräuchlich nutzen.

(2) Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

- Das personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (z. B. im Kundensystem).
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf Online-Händlerseiten).
- Das personalisierte Sicherheitsmerkmal darf nicht außerhalb des Sparda-Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Das personalisierte Sicherheitsmerkmal darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- 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.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht für das Sparda-Online-Banking genutzt werden.

7.3 Sicherheit des Kundensystems

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

7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem Sparda-Online-Banking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z. B. Mobiltelefon) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten

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 Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank 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 Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1,

- den Sparda-Online-Banking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Sparda-Online-Banking-Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den Sparda-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 Bank 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 Bank wird eine Sperre aufheben oder das personalisierte Sicherheitsmerkmal bzw. das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden.

10. Haftung

10.1 Haftung der Bank bei nicht autorisierten und nicht oder fehlerhaft ausgeführten Sparda-Online-Banking-Verfügungen

Die Haftung der Bank bei nicht autorisierten und nicht oder fehlerhaft ausgeführten Sparda-Online-Banking-Verfügungen richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr, Sonderbedingungen für das Wertpapiergeschäft).

10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstrumentes

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruht ein nicht autorisierter Zahlungsvorgang vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstrumentes, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob dem Teilnehmer an dem Verlust oder Diebstahl oder sonstigem Abhandenkommen des Authentifizierungsinstrumentes ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu einem nicht autorisierten Zahlungsvorgang aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstrumentes, ohne dass dieses verlorengegangen oder gestohlen oder sonst abhanden gekommen ist, haftet der Kontoinhaber für den der Bank 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 Zahlungen 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 Bank 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

- den Verlust oder Diebstahl des Authentifizierungsinstrumentes oder die missbräuchliche Nutzung des Authentifizierungsinstrumentes oder des personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (vgl. Nummer 8.1 Absatz 1),
- das personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (vgl. Nummer 7.2 Absatz 2, 1. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde (vgl. Nummer 7.2 Absatz 1, 2. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (vgl. Nummer 7.2 Absatz 2, 3. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal außerhalb des Sparda-Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (vgl. Nummer 7.2 Absatz 2, 4. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (vgl. Nummer 7.2 Absatz 2, 5. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet (vgl. Nummer 7.2 Absatz 2, 6. Spiegelstrich),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Sparda-Online-Banking nutzt (vgl. Nummer 7.2 Absatz 2, 7. Spiegelstrich).

(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

Beruht eine nicht autorisierte Wertpapiertransaktion vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstrumentes oder auf der sonstigen missbräuchlichen Nutzung des personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstrumentes und ist der Bank hierdurch ein Schaden entstanden, haften der Kontoinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige des Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Sparda-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 Bank kann sich der Teilnehmer an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.