Bedingungen für die Online Services

1. Leistungsangebot
(1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels der Online Services in dem von der Hamburger Sparkasse AG – im Folgenden „Haspa“ genannt - angebotenen Umfang abwickeln. Zudem kann er Informationen der Haspa mittels der Online Services 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 der Online Services gelten die mit der Haspa gesondert vereinbarten Verfügungslimite.

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

2.1 Personalisierte Sicherheitsmerkmale
Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- Die persönliche Identifikationsnummer (PIN).
- Einmal verwendbare Transaktionsnummern (TAN).
- Der Nutzungscode für die elektronische Signatur.

2.2 Authentifizierungsinstrumente
Die TAN bzw. 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.
- Mittels eines mobilen Endgerätes (z. B. Mobiltelefon) zum Empfang von TAN per SMS (smsTAN).
- Auf einer Chipkarte mit Signaturfunktion.
- Auf einem sonstigen Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden.

Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

3. Zugang zu den Online Services
Der Teilnehmer erhält Zugang zu den Online Services, wenn

- dieser die Kontonummer oder seine individuelle Kundenkennung und seine PIN oder elektronische Signatur übermittelt hat,
- die Prüfung dieser Daten bei der Haspa eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9.) vorliegt.

Nach Gewährung des Zugangs zu den Online Services kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

4. Online Services-Aufträge

4.1 Auftragserteilung und Autorisierung
Der Teilnehmer muss Online Services-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (TAN oder elektronische Signatur) autorisieren und der Haspa mittels der Online Services übermitteln. Die Haspa bestätigt mittels der Online Services den Eingang des Auftrags.

4.2 Widerruf von Aufträgen
Die Widerrufbarkeit eines Online Services-Auftrages richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb der Online Services erfolgen, es sei denn, die Haspa sieht eine Widerrufmöglichkeit in den Online Services ausdrücklich vor.

5. Bearbeitung von Online Services-Aufträgen durch die Haspa
(1) Die Bearbeitung der Online Services-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Online Services-Seite der Haspa oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der Online Services-Seite der Haspa 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 Haspa, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.
(2) Die Haspa wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat sich mit seinem Personalisierten Sicherheitsmerkmal legitimiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das Online Services-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online Services-Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Überweisungsbedingungen) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Haspa die Online Services-Aufträge nach Maßgabe der Bestimmungen der für den jeweiligen Geschäftsvorfall geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.
(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Haspa den Online Services-Auftrag nicht ausführen und den Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels der Online Services eine Information zur Verfügung stellen.

6. Information des Kontoinhabers über Online Service-Verfügungen
Die Haspa unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels der Online Services getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zu den Online Services
Der Teilnehmer ist verpflichtet, die technische Verbindung zu den Online Services nur über die von der Haspa gesondert mitgeteilten Online Services-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 Haspa gesondert mitgeteilten Online Services-Zugangskanäle an die Haspa 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 Services-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 diese 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 Online Services-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die PIN und der Nutzungscode für die elektronische Signatur dürfen 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 smsTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht gleichzeitig für die Online Services genutzt werden.

7.3 Sicherheit des Kundensystems
Der Teilnehmer muss die Sicherheitshinweise auf der Internetseite der Haspa zu den Online Services, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.4 Kontrolle der Auftragsdaten mit von der Haspa angezeigten Daten
Soweit die Haspa dem Teilnehmer Daten aus seinem Online Services-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.

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 Personalisierten Sicherheitsmerkmals fest, muss der Teilnehmer die Haspa hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Haspa eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben (während der Geschäftszeiten unter der Nummer 040 3579-7426, außerhalb der Geschäftszeiten unter der Nummer 040 3579-0).

(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 Haspa unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers
Die Haspa sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Verdachts- und Sperranzeige nach Nummer 8.1,
- den Online Services-Zugang für ihn oder alle Teilnehmer oder sein Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Haspa
(1) Die Haspa darf den Online Services-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, den Online Services-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 Haspa 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 Haspa 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 Konto-/Depotinhaber unverzüglich.

9.4 Automatische Sperre eines chip-basierten Authentifizierungsinstruments
(1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur 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 die Online Services genutzt werden. Der Teilnehmer kann sich mit der Haspa in Verbindung setzen, um die Nutzungsmöglichkeiten der Online Services wiederherzustellen.

10. Haftung

10.1 Haftung der Haspa bei nicht autorisierten und nicht oder fehlerhaft ausgeführten Online Services-Verfügungen
Die Haftung der Haspa bei nicht autorisierten und nicht oder fehlerhaft ausgeführten Online Services-Verfügungen richtet sich nach den für den jeweiligen Geschäftsvorfall 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 Verdachts- oder Sperranzeige
(1) Beruht ein nicht autorisierter Zahlungsvorgang vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Haspa hierdurch entstehenden Schaden bis zu einem Betrag von 150,00 Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust oder Diebstahl des Authentifizierungsinstruments ein Verschulden trifft.
(2) Kommt es vor der Sperranzeige zu einem nicht autorisierten Zahlungsvorgang aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen oder gestohlen worden ist, haftet der Kontoinhaber für den der Haspa hierdurch entstehenden Schaden bis zu einem Betrag von 150,00 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der Personalisierten Sicherheitsmerkmale verletzt hat.
(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungen über die Haftungsgrenze von 150,00 Euro nach Absatz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen 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 und 8.2 nicht abgeben konnte, weil die Haspa nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.
(5) Kommt es vor der Sperranzeige zu einer nicht autorisierten Verfügung 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 Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals der Haspa nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1 Absatz 2),
- das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2 Absatz 2, 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1, Satz 1),
- das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2, 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal außerhalb des Online Services-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2, 4. Spiegelstrich).
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2, 5. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet (siehe Nummer 7.2 Absatz 2, 6. Spiegelstrich).
- beim smsTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für die Online Services nutzt (siehe 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 Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Haspa hierdurch ein Schaden entstanden, haften der Kontoinhaber und die Haspa nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung der Haspa ab der Sperranzeige
Sobald die Haspa eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online Services-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
Für die Beilegung von Streitigkeiten mit der Haspa kann sich der Kunde an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.

12. Verfügungslimite
Es besteht die Möglichkeit, Verfügungslimite zu vereinbaren, z. B. formlos per elektronisch unterschriebener Mitteilung. Bei den Verfügungslimiten handelt es sich um Zahlungsverkehr-Limite pro Konto, pro Kalendertag. Das Limit hat folgende Wirkung: Bei der Haspa eingehende Einzel- und Sammelüberweisungen sowie EU-/SEPA-Überweisungen werden in der Reihenfolge ihres Eingangs nur entgegengenommen, wenn dadurch das Limit des Einreichungstages nicht überschritten wird. Bei Daueraufträgen, Terminüberweisungen und Wertpapier-Order wird das Limit nicht berücksichtigt. Brokerage-Verfügungen werden durch das am Ausführungstag vorhandene Guthaben sowie eine für das Verrechnungskonto vereinbarte Kreditlinie begrenzt.

13. Aufzeichnung von Telefongesprächen
Der Kunde erklärt sich mit der Aufzeichnung der Telefongespräche im Rahmen der Online Services-Hotline einverstanden. Die aufgezeichneten Gespräche dienen ausschließlich als Grundlage zur Sicherung der Servicequalität. Die Aufzeichnungen werden mindestens 6 Monate aufbewahrt.

September 2009 **Hamburger Sparkasse AG**