Bank für Sozialwirtschaft

Bedingungen zur elektronischen Kontoführung

1 Leistungsangebot

(1) Der Kontoinhaber und dessen Bevollmächtigte bzw. ein vom Kontoinhaber beauftragter Dritter (z. B. ein Dienstleister) können Bankgeschäfte mittels Online-Banking oder per Datenfernübertragung in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online-Banking abrufen.
Der Inhaber eines Zahlungskontos und dessen Bevollmächtigte sind zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrags 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) Der Kontoinhaber bzw. der von ihm beauftragte Dritte werden im Folgenden als „Kunde“ bezeichnet. Die durch den Kunden bevollmächtigten, natürlichen Personen werden im Folgenden als „Teilnehmer“ bezeichnet. Die Einreichung und der Abruf von Dateien (insbesondere Übermittlung von Aufträgen und Informationsabruf) per Datenfernübertragung werden im Folgenden als „DFÜ“ bezeichnet.
(3) Im Rahmen der elektronischen Kontoführung per Online-Banking oder DFÜ ist die Bank berechtigt,

- dem Kunden, den Teilnehmern bzw. u. U. den dafür speziell benannten Personen (z. B. Administratoren) Informationen, Daten und Mitteilungen direkt per Post, per Fax, per E-Mail oder über einen separat vereinbarten/abgesprochenen Kommunikationsweg zukommen zu lassen,
- im Supportfall, zur Wartung oder zur Problembehebung für das vom Kunden eingesetzte eb-Produkt der Bank auf dem Kundensystem während der veröffentlichten Servicezeiten Fernwartungsarbeiten gem. den Bedingungen zur Fernwartung (siehe Nummer 15) durchzuführen. Dabei sollte Folgendes vorab vom Teilnehmer beachtet werden:
  - Nutzungshinweise und Regelungen des Kunden zum Datenschutz
  - Prüfung, ob Fernwartung laut den Datenschutzbestimmungen des Kunden zulässig ist
  - Ist eine Datensicherung vor Beginn der Fernwartungssitzung erfolgt bzw. notwendig?
  - Sind alle Anwendungen geschlossen, die die Bank nicht sehen soll.

(4) Im Rahmen des Online-Bankings können Teilnehmer und Bank ein Limit vereinbaren und zur weiteren Risikobegrenzung bestimmte Funktionen ausschließen.
(5) Im Rahmen der DFÜ gibt die Bank dem Kunden die Dienstleistungsarten bekannt, die er nutzen kann. Der Satz- und Dateiaufbau für die Übermittlung von Aufträgen und den Informationsabruf wird in der Spezifikation der Datenformate (siehe Nummer 15) beschrieben.

2 Voraussetzungen zur elektronischen Kontoführung

2.1 Allgemeine Voraussetzungen
Für jeden Kunden wird durch die Bank mindestens eine Kunden-ID angelegt. Über die Kunden-ID werden die elektronischen Kontoinformationen der mit der Kunden-ID verknüpften Konten bankarbeitstäglich zur Verfügung gestellt. Weiterhin werden an der Kunden-ID die jeweiligen Teilnehmer hinterlegt. Jeder Teilnehmer erhält dazu eine Teilnehmer-ID. Zu jeder Teilnehmer-ID werden die Berechtigungen des Teilnehmers gespeichert. Aufträge nach Nummer 5 können nur Teilnehmer erteilen, die im Rahmen der getroffenen Regelung mit dem Kunden eine Vollmacht erhalten haben und über freigeschaltete Legitimationsmedien der Bank verfügen.

2.2 Weitere Voraussetzungen für Online-Banking
Der Teilnehmer benötigt für die Nutzung des Online-Bankings die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale und Zahlungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 5.1).

- Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die die Bank dem Teilnehmer zum Zwecke der Authentifizierung bzw. Autorisierung bereitstellt. Dies sind beispielsweise:
  - die persönliche Identifikationsnummer (PIN) oder der Nutzungscode für die elektronische Signatur und
  - einmal verwendbare Transaktionsnummern (TAN).
- Zahlungsinstrumente sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurden und die vom Teilnehmer zur Erteilung eines Online-Banking-Auftrags verwendet werden. Insbesondere mittels folgender Zahlungsinstrumente kann die TAN dem Teilnehmer zur Verfügung gestellt werden:
  - mittels eines TAN-Generators, der Bestandteil eines anderen elektronischen Geräts zur Erzeugung von TAN ist.

3 Zugang zum Online-Banking

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

a) der Teilnehmer seine individuelle Benutzerkennung und seine personalisierten Sicherheitsmerkmale (PIN/TAN) übermittelt. Hierbei wird unter PIN die persönliche Identifikationsnummer und unter TAN eine Transaktionsnummer verstanden,
b) die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
c) keine Sperre des Zugangs (siehe Nummer 12) vorliegt.

(2) Nach Gewährung des Zugangs zum Online-Banking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen. Die Punkte a) und b) gelten auch, wenn Zahlungsaufträge über einen Zahlungsauslösedienst ausgelöst und Zahlungskontoinformationen über einen Kontoinformationsdienst angefordert werden (siehe Nummer 1 Absatz 1 Satz 3).

4 Datenaustausch per DFÜ

(1) Der Austausch von Auftragsdaten und Informationen erfolgt gemäß der Spezifikation der Datenformate (siehe Nummer 15).
(2) Zur Unterscheidung von Auftragsdaten werden verschiedene Auftragsarten genutzt, denen die Datenformate zugeordnet sind.
(3) Die Belegung der Datenfelder richtet sich nach den Belegungs- und Kontrollrichtlinien des jeweils genutzten Datenformates (siehe Nummer 15).
(4) Für das zwischen Kunde und Bank vereinbarte DFÜ-Verfahren gelten die in der Spezifikation für die EBICS-Anbindung sowie die in der DFÜ-Verfahrensbeschreibung und die in der Spezifikation der Datenformate (siehe Nummer 15) beschriebenen Anforderungen.
(5) Der Kunde bzw. der Teilnehmer hat die Kundenkennung des Zahlungsempfängers beziehungsweise des Zahlers gemäß den maßgeblichen Sonderbedingungen zutreffend anzugeben. Die in die Abwicklung des Zahlungsauftrags eingeschalteten Zahlungsdienstleister sind berechtigt, die Bearbeitung ausschließlich anhand der Kundenkennung vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Auftrags zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zulasten des jeweiligen Kunden.
(6) Soweit die Bank dem Kunden Daten über Zahlungsvorgänge zur Verfügung stellt, die noch nicht endgültig bearbeitet sind, stellen diese lediglich eine unverbindliche Information dar. Die Daten sind jeweils besonders gekennzeichnet.

5 Auftragserteilung und Autorisierung

5.1 im Online-Banking
(1) Der Teilnehmer muss Online-Banking-Aufträge (z. B. Überweisungen) vor der Autorisierung auf ihre Richtigkeit überprüfen.
(2) Der Teilnehmer muss Online-Banking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem von der Bank bereitgestellten personalisierten Sicherheitsmerkmal (z. B. TAN) autorisieren und der Bank mittels Online-Banking übermitteln, sofern mit der Bank nichts anderes vereinbart wurde.
(3) Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags.
(4) Reicht ein Service-Rechenzentrum die Auftragsdaten per DFÜ ein, erfolgt die Autorisierung durch den Kunden bzw. dessen Teilnehmer mit personalisiertem Sicherheitsmerkmal (PIN/TAN) und Zahlungsinstrument (BFS-Token mit Token-PIN).
Die Absätze 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.

5.2 per DFÜ
(1) Zur Autorisierung von per DFÜ übermittelten Auftragsdaten benötigt jeder Teilnehmer jeweils individuelle, von der Bank freigeschaltete Legitimationsmedien. Die Anforderungen an die Legitimationsmedien sind in der Spezifikation für die EBICS-Anbindung sowie in der DFÜ-Verfahrensbeschreibung definiert.
(2) Für die Absicherung des Datenaustauschs benötigt jeder Teilnehmer jeweils individuelle, von der Bank freigeschaltete Sicherungsmedien. Die Anforderungen an die Sicherungsmedien sind in der Spezifikation für die EBICS-Anbindung sowie in der DFÜ-Verfahrensbeschreibung beschrieben.
(3) Vor der Einlieferung von Auftragsdaten bzw. vor deren Autorisierung muss der Teilnehmer die Auftragsdaten auf ihre Richtigkeit überprüfen und stellt somit sicher, dass genau diese Daten elektronisch unterschrieben werden.

5.3 gemäß individueller Vereinbarung zwischen Kunde und Bank
In Ausnahmefällen können bzgl. der Autorisierung von eingereichten Zahlungsaufträgen individuelle Verfahren (abweichend von den Nummern 5.1 und 5.2) vereinbart werden. Dabei gilt jedoch grundsätzlich, dass die Autorisierung nur anhand einer bei der Bank vorliegenden Kontobevollmächtigung erfolgen kann. Die Einreichung der Auftragsdatei erfolgt durch einen entsprechend berechtigten Teilnehmer.

6 Zugang von Aufträgen

(1) Bei Aufträgen ist der Zugangszeitpunkt der Tag, an dem die Autorisierung (gemäß Nummer 5.1, 5.2 bzw. 5.3) bis zum Ende des im Preis- und Leistungsverzeichnis bestimmten Zeitpunkts (Annahmefrist) abgeschlossen und ein etwaiges im Auftrag angegebenes Ausführungsdatum erreicht ist. Fällt dieser Tag nicht auf einen Geschäftstag gemäß dem Preis- und Leistungsverzeichnis der Bank, gilt der darauf folgende Geschäftstag als Zugangszeitpunkt.
(2) Für Überweisungsaufträge gelten ergänzende Regelungen zum Zeitpunkt des Zugangs und dem Beginn der Ausführungsfristen gemäß den Sonderbedingungen für den Überweisungsverkehr.

7 Auftragsbearbeitung durch die Bank

(1) Die Bank wird den Auftrag im Rahmen des ordnungsgemäßen Arbeitsablaufes ausführen, wenn

- dieser gemäß Nummer 5.1, 5.2 bzw. 5.3 autorisiert wurde,
- die Berechtigung des Teilnehmers/der Teilnehmer für die notwendige Autorisierung (z. B. gemeinsame Verfügungsberechtigung) vorliegt,
- alle erforderlichen Teilnehmerfreigaben innerhalb der in den jeweils gültigen Verfahrensbeschreibungen (siehe Nummer 15) genannten Fristen eingegangen sind,
- das Datenformat gemäß der Spezifikation der Datenformate (siehe Nummer 15) eingehalten ist,
- die Ausführungsvoraussetzungen nach den maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Überweisungsbedingungen) vorliegen und
- das mit dem Teilnehmer vereinbarte Limit (siehe Nummer 1 Absatz 4) nicht überschritten wird.

Dabei werden die unter www.sozialbank.de veröffentlichten Cut-Off-Zeiten berücksichtigt.

(2) Liegen die Ausführungsbedingungen nach Absatz 1 vor, führt die Bank den Auftrag nach Maßgabe der geltenden Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 1 nicht vor, wird die Bank den Auftrag nicht ausführen und den Teilnehmer über die Nichtausführung informieren (z. B. im DFÜ-Protokoll). Wenn möglich, werden die Ablehnungsgründe sowie Korrekturmöglichkeiten genannt. Die Bank ist berechtigt, nicht vollständig autorisierte Auftragsdaten nach Ablauf des von der Bank in den jeweils gültigen Verfahrensbeschreibungen mitgeteilten Zeitlimits zu löschen.

(4) Im Rahmen der DFÜ ist die Bank verpflichtet, die Abläufe (gemäß der Spezifikation für die EBICS-Anbindung – siehe Nummer 15) und die Weiterleitung der Aufträge zur Bearbeitung im Kundenprotokoll zu dokumentieren. Der Kunde ist seinerseits verpflichtet, das Kundenprotokoll zeitnah abzurufen und sich über den Status der Auftragsbearbeitung zu informieren. Bei Unstimmigkeiten soll er sich mit der Bank in Verbindung setzen.

8 Widerruf von Aufträgen

(1) Vor der Autorisierung der Auftragsdaten kann der Kunde die Datei zurückrufen. Änderungen einzelner Auftragsdaten sind nur durch Rückruf der gesamten Datei und erneute Einlieferung möglich. Die Bank kann einen Rückruf nur beachten, wenn ihr dieser so rechtzeitig zugeht, dass seine Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufs möglich ist.

(2) Die Widerrufbarkeit eines Auftrags richtet sich nach den dafür geltenden Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb der elektronischen Kontoführung erfolgen. Hierzu hat der Kunde der Bank die Einzelangaben des Originalauftrags mitzuteilen.

9 Informationen über ausgeführte Aufträge

(1) Die Bank unterrichtet den Teilnehmer täglich über die ausgeführten Zahlungsaufträge auf dem für Kontoinformationen vereinbarten elektronischen Kommunikationsweg.

(2) Soweit die Bank dem Teilnehmer Daten über Zahlungsvorgänge zur Verfügung stellt, die noch nicht endgültig bearbeitet sind, stellen diese lediglich eine unverbindliche Information dar. Diese Daten sind jeweils besonders gekennzeichnet.

(3) Handelt es sich beim Kunden um einen Verbraucher gemäß § 13 BGB (Bürgerliches Gesetzbuch) und die elektronische Bereitstellung von Kontoinformationen ist nicht vereinbart, so unterrichtet die Bank den Kunden mindestens einmal monatlich durch die Zusendung eines Papier-Kontoauszugs.

10 Sorgfaltspflichten

(1) Kunde und Teilnehmer sind verpflichtet, sich regelmäßig über die unter www.sozialbank.de veröffentlichten Sicherheitshinweise, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem) zu informieren und diese zu beachten. Die Sicherheitshinweise sind unter www.sozialbank.de veröffentlicht und werden regelmäßig durch die Bank aktualisiert.

(2) Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer diese Bedingungen nebst Anlagen kennen und beachten.

10.1 Technische Verbindung

(1) Der Teilnehmer ist verpflichtet, die technische Verbindung, die mit dem vereinbarten Kommunikationsweg gekoppelt ist, nur über die von der Bank gesondert mitgeteilten 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.

(2) Der Kunde hat für einen ausreichenden Schutz der von ihm bzw. von seinen Teilnehmern eingesetzten Systeme Sorge zu tragen.

(3) Die Bank empfiehlt dringend, dass auf dem vom Kunden bzw. dessen Teilnehmern genutzten EDV-System

- eine Firewall eingesetzt wird; eine Firewall ist eine Einrichtung, die den gesamten ein- und ausgehenden Nachrichtenverkehr überwacht und nur bekannte oder autorisierte Verbindungen zulässt,

- ein Virenscanner installiert und aktiviert ist, der regelmäßig mit den neuesten Virendefinitionsdateien versorgt wird,
- sicherheitsrelevante Updates für das jeweils eingesetzte und vom Hersteller gewartete Betriebssystem sowie weitere installierte sicherheitsrelevante Software-Programme eingespielt werden, sofern diese vorliegen.

(4) Im Rahmen der DFÜ mittels des EBICS-Verfahrens sind darüber hinaus folgende Sicherheitsmaßnahmen durch den Kunden zu berücksichtigen:

- Die vom Kunden für das EBICS-Verfahren eingesetzte Software muss die in der DFÜ-Verfahrensbeschreibung (siehe Nummer 15) beschriebenen Anforderungen erfüllen.
- Das EBICS-EDV-System des Kunden ist so einzurichten, dass sich der Teilnehmer zuvor anmelden muss. Die Anmeldung hat als normaler Benutzer und nicht als Administrator, der z. B. berechtigt ist, die Installation von Programmen vorzunehmen, zu erfolgen.
- Die internen IT-Kommunikationswege für unverschlüsselte bankfachliche Daten oder für unverschlüsselte EBICS-Nachrichten sind gegen Abhören und Manipulationen zu schützen.

Die Umsetzung dieser Anforderungen liegt ausschließlich in der Verantwortung des Kunden.

10.2 Geheimhaltung und sichere Aufbewahrung

(1) Jeder Teilnehmer hat

- seine personalisierten Sicherheitsmerkmale geheim zu halten sowie
- sein Zahlungsinstrument bzw. sein von der Bank freigeschaltetes Legitimationsmedium vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Zahlungsinstruments bzw. des von der Bank freigeschalteten Legitimationsmediums ist, kann in Verbindung mit der Kenntnis des dazugehörigen personalisierten Sicherheitsmerkmals diese 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, 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 bzw. des von der Bank freigeschaltetes Legitimationsmediums zu beachten:

- Das personalisierte Sicherheitsmerkmal darf nicht ungesichert elektronisch gespeichert werden.
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das personalisierte Sicherheitsmerkmal darf nicht per E-Mail oder andere Telekommunikationsmittel weitergegeben werden.
- Das personalisierte Sicherheitsmerkmal (z. B. PIN) darf nicht zusammen mit dem Zahlungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung (z. B. eines Auftrags) im Online-Banking nicht mehr als eine TAN verwenden.

(3) Soweit die Bank dem Teilnehmer Daten aus seinem Online-Banking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z. B. Zahlungsinstrument 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.

10.3 Sicherung

(1) Im Rahmen der DFÜ-Verfahren gem. der DFÜ-Verfahrensbeschreibung (siehe Nummer 15) hat der Kunde vor der Übertragung von Datensätzen an die Bank eine Kopie oder Aufzeichnung der zu übertragenden Datensätze mit dem vollständigen Inhalt sowie der zur Prüfung der Legitimation übermittelten Daten zu erstellen. Diese ist vom Kunden für einen Zeitraum von 30 Kalendertagen ab dem in der Datei angegebenen Ausführungstermin (für Überweisungen) bzw. Fälligkeitstermin (Lastschriften) o0der bei mehreren Terminen dem spätesten Termin in der Form nachweisbar zu halten, dass die Datei auf Anforderung der Bank kurzfristig erneut zur Verfügung gestellt werden kann, sofern nichts Abweichendes vereinbart wird.

(2) Außerdem hat der Kunde für jede Einreichung und jeden Abruf von Dateien ein maschinelles Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Spezifikation für die EBICS-Anbindung entspricht, zu erstellen, zu seinen Unterlagen zu nehmen und auf Anforderung der Bank zur Verfügung zu stellen.

10.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers) im vereinbarten Kommunikationsweg zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

11 Anzeige- und Unterrichtungspflichten

11.1 Sperranzeige

(1) Stellt der Teilnehmer den Verlust oder den Diebstahl seiner Legitimations- und Sicherungsmedien bzw. seines Zahlungsinstruments, die missbräuchli-

che Verwendung oder die sonstige nicht autorisierte Nutzung seiner Legitimations- und Sicherungsmedien bzw. seines personalisierten Sicherheitsmerkmals und Zahlungsinstruments fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über gesondert mitgeteilte Kontaktdaten abgeben.
(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 seinen Legitimations- und Sicherungsmedien bzw. an seinem Zahlungsinstrument oder die Kenntnis seines personalisierten Sicherheitsmerkmals erlangt hat oder
- seine Legitimations- und Sicherungsmedien bzw. sein personalisiertes Sicherheitsmerkmal und sein Zahlungsinstrument verwendet,

muss er ebenfalls eine Sperranzeige abgeben.

11.2 Unterrichtungspflicht über nicht autorisierte oder fehlerhaft ausgeführte Aufträge
Der Kunde hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Zahlungsauftrags hierüber zu unterrichten.

12 Nutzungssperre

12.1 Sperre auf Veranlassung des Teilnehmers
Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 11.1,

- seinen Teilnehmer-Zugang bzw. den Zugang für alle Teilnehmer oder
- seine Legitimations- und Sicherungsmedien bzw. sein Zahlungsinstrument.

12.2 Automatisierte Sperre eines Teilnehmers
Der Teilnehmer kann seinen Zugang selber sperren. Näheres ist in den jeweiligen Verfahrensbeschreibungen enthalten.

12.3 Sperre auf Veranlassung des Kunden
Der Kunde kann außerhalb des vereinbarten Kommunikationsweges die Verwendung der Legitimations- und Sicherungsmedien bzw. der personalisierten Sicherheitsmerkmale und Zahlungsinstrumente eines Teilnehmers oder den gesamten elektronischen Zugriff aller Teilnehmer per Sperranzeige über gesondert mitgeteilte Kontaktdaten abgeben.

12.4 Sperre auf Veranlassung der Bank
(1) Die Bank darf den Zugang für einen Teilnehmer oder den gesamten elektronischen Zugriff aller Teilnehmer sperren, wenn

- sie berechtigt ist, den für die elektronische Kontoführung zugrunde liegenden Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Legitimations- und Sicherungsmedien bzw. des personalisierten Sicherheitsmerkmals und des Zahlungsinstruments dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der Legitimations- und Sicherungsmedien bzw. des personalisierten Sicherheitsmerkmals und des Zahlungsinstruments besteht.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.
(3) Wird ein Teilnehmerzugang ein Jahr lang nicht aktiv genutzt (Teilnehmerinaktivität), so wird dieser Zugang aus Sicherheitsgründen durch die Bank gesperrt.

12.5 Aufhebung der Sperre
Erfolgte die Sperrung gemäß

- Nummer 12.1 bzw. 12.2 durch den Teilnehmer, so muss sich dieser zur Sperraufhebung mit der Bank in Verbindung setzen,
- Nummer 12.3 durch den Kunden, so muss sich dieser zur Sperraufhebung mit der Bank in Verbindung setzen,
- Nummer 12.4, wird die Bank die Sperre aufheben, die Legitimations- und Sicherungsmedien bzw. das personalisierte Sicherheitsmerkmal und das Zahlungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden/Teilnehmer. Sofern die Sperre aufgrund einer Teilnehmerinaktivität erfolgt ist, so muss sich dieser zur Sperraufhebung mit der Bank in Verbindung setzen.

13 Haftung

13.1 Haftung der Bank bei einem nicht autorisierten bzw. bei einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag
(1) Die Haftung der Bank bei einer nicht autorisierten bzw. einer nicht, fehlerhaft oder verspätet ausgeführten Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Bedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr).
(2) Entsteht ein Schaden durch einen nicht autorisierten bzw. einen nicht, fehlerhaft oder verspätet ausgeführten Auftrag durch ein vom Kunden berechtigtes Service-Rechenzentrum bzw. durch einen berechtigten Dritten, so kann die Bank von diesem einen Ersatz des Schadens verlangen.

13.2 Haftung des Kunden bei missbräuchlicher Nutzung eines Legitimations- und Sicherungsmediums bzw. personalisierten Sicherheitsmerkmals und Zahlungsinstruments vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhandengekommenen Legitimations- und Sicherungsmediums bzw. personalisierten Sicherheitsmerkmals und Zahlungsinstruments, haftet der Kunde für den der Bank hierdurch entstandenen Schaden bis zu einem Betrag von 50,00 EUR, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust oder Diebstahl ein Verschulden trifft.

(2) Der Kunde 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 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 Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fährlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er

- den Verlust oder Diebstahl oder die missbräuchliche Nutzung des Legitimations- und Sicherungsmediums bzw. personalisierten Sicherheitsmerkmals und Zahlungsinstruments der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 11.1 Satz 1),
- die Legitimations- und Sicherungsmedien bzw. das personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe Nummer 10.2 Satz 2),
- das personalisierte Sicherheitsmerkmal per E-Mail oder anderen Telekommunikationsmitteln weitergegeben hat (siehe Nummer 10.2 Satz 2),
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 10.2),
- das personalisierte Sicherheitsmerkmal auf dem Zahlungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 10.2),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet (siehe Nummer 10.2).

(4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt hat, obwohl die Bank zur starken Kundenauthentifizierung nach § 68 Absatz 4 Zahlungsdiensteaufsichtsgesetz verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere 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 das Verfügungslimit (siehe Nummer 1 Absatz 4) gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

(6) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 11.1 nicht abgeben konnte, weil die Bank 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 Kunde kein Verbraucher, gilt ergänzend Folgendes:

- Der Kunde haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50,00 Euro nach 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 Punkt findet keine Anwendung.

13.3 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige des Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

13.4 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, dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können oder von der Bank aufgrund einer gesetzlichen Verpflichtung herbeigeführt wurden.

14 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- oder Beschwerdestellen wenden.

15 Schlussbestimmungen

Die

- Spezifikation der Datenformate (Anlage 3 des DFÜ-Abkommens),
- Spezifikation für die EBICS-Anbindung (EBICS-Spezifikation –- Anlage 1 des DFÜ-Abkommens),
- Verfahrensbeschreibung BFS-Net.Banking
- DFÜ-Verfahrensbeschreibung und
- Bedingungen zur Fernwartung

in ihrer jeweils aktuellen Fassung sind Bestandteile der elektronischen Kontoführung und sind unter www.sozialbank.de veröffentlicht.

Stand: 13.01.2018