Bedingungen zur elektronischen Kontoführung

1 Leistungsangebot

(1) Der Kontoinhaber bzw. ein von ihm beauftragter Dritter (z. B. ein Dienstleister) können Bankgeschäfte (Übermittlung von Aufträgen, Auftragserteilung und Informationsabruf) auf elektronischem Wege mit der Bank für Sozialwirtschaft AG abwickeln.
(2) Der Kontoinhaber bzw. der von ihm beauftragte Dritte werden im Folgenden als „Kunde“ bezeichnet. Die durch den Kunden benannten berechtigten, natürlichen Personen werden im Folgenden als „Teilnehmer“ bezeichnet. Die Bank für Sozialwirtschaft AG wird im Folgenden als „Bank“ bezeichnet. Die Übermittlung von Aufträgen, die Auftragserteilung und der Informationsabruf auf elektronischem Wege werden im Folgenden als „DFÜ“ bezeichnet.
(3) Im Rahmen der elektronischen Kontoführung 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.

(4) Im Rahmen der elektronischen Kontoführung können Kunde und Bank ein Limit, im Folgenden Limit genannt, vereinbaren.

2 Voraussetzungen zur elektronischen Kontoführung

Anhand der Regelung auf dem Unterschriftenblatt des Kunden bzw. vertraglicher Regelung und unter Berücksichtigung des eingesetzten eb-Produktes wird für jeden Kunden mindestens eine Kunden-ID und für jeden Teilnehmer mindestens eine Teilnehmer-ID angelegt. Über die Kunden-ID werden die elektronischen Kontoinformationen der mit der Kunden-ID verknüpften Konten zur Verfügung gestellt. Weiterhin werden an der Kunden-ID die jeweiligen Teilnehmer hinterlegt, die über die Kunden-ID die Übermittlung von Aufträgen, die Auftragserteilung und den Informationsabruf auf elektronischem Wege durchführen sollen. 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 von der Bank freigeschaltete Legitimationsmedien verfügen.

3 Datenaustausch

(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. Zudem gibt es weitere Auftragsarten, die mit dem jeweiligen Kommunikationsweg gekoppelt sind.
(3) Die Belegung der Datenfelder richtet sich nach den Belegungs- und Kontrollrichtlinien des jeweils genutzten Datenformates (siehe Nummer 15).
(4) Der Kunde bzw. der Teilnehmer hat den Kontoidentifikationscode (IBAN) des Zahlungsempfängers beziehungsweise des Zahlers und - soweit diese Angabe erforderlich ist - den Zahlungsdienstleisteridentifikationscode (BIC) des Zahlungsdienstleisters des Zahlungsempfängers beziehungsweise des Zahlungsdienstleisters des Zahlers (Zahlstelle) zutreffend anzugeben.
Die in die Abwicklung des Zahlungsauftrags eingeschalteten Zahlungsdienstleister sind berechtigt, die Bearbeitung ausschließlich anhand des Kontoidentifikationscodes und - soweit diese Angabe vorhanden ist - des Zahlungsdienstleisteridentifikationscodes vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Auftrags zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zulasten des jeweiligen Kontoinhabers.
(5) Der Kunde ist verpflichtet, Überweisungsaufträge und Lastschrifteinzugsaufträge für Zahlungen in Euro innerhalb des Europäischen Wirtschaftsraums nur noch im Format ISO 20022 gemäß Kapitel 2 der Spezifikation der Datenformate (siehe Nummer 15) einzureichen. Lastschrifteinzugsaufträge für Zahlungen, die an einer Verkaufsstelle mithilfe einer Zahlungskarte generiert wurden und zu einer Lastschrift von einem inländischen Zahlungskonto führen (§ 7c Absatz 1 Zahlungsdiensteaufsichtsgesetz), sind erst ab dem 01. Februar 2016 verpflichtend im Format ISO 20022 einzureichen.
(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.

4 Einlieferung von Auftragsdaten

(1) Vor der Einlieferung von Auftragsdaten muss der Teilnehmer die Auftragsdaten auf ihre Richtigkeit

überprüfen und stellt somit sicher, dass genau diese Daten elektronisch unterschrieben werden.
(2) Unter Berücksichtigung der technischen Vorgaben (siehe Nummer 3) übermittelt der Teilnehmer die Auftragsdaten an die Bank.
(3) Im Rahmen des Lastschriftverkehrs ist die Bank verpflichtet sicherzustellen, dass der Lastschriftbetrag spätestens innerhalb von einem Geschäftstag beim Zahlungsdienstleister des Zahlungsempfängers eingeht. Daher sind bei der Einreichung von Lastschriften die verfahrensbedingt vorgeschriebenen Vorlauftage und die vereinbarten Einlieferungsfristen zu beachten.
Die Geschäftstage der Bank ergeben sich aus dem Preis- und Leistungsverzeichnis.
(4) Bei Aufnahme der Kommunikation werden seitens der Bank zuerst teilnehmerbezogene Berechtigungsprüfungen durchgeführt.
(5) Die Bank bestätigt den Eingang der Auftragsdaten sowie die Ergebnisse weiterer bankfachlicher Prüfungen (z. B. Kontoberechtigungsprüfungen) innerhalb des gewählten Kommunikationsweges (z. B. DFÜ-Protokoll im EBICS-Verfahren) und stellt dem Teilnehmer diese zur Verfügung.

5 Auftragsautorisierung

Eingelieferte Auftragsdaten werden gegenüber der Bank wirksam, wenn diese wie folgt autorisiert wurden:

5.1 mit elektronischer Unterschrift (EU) bzw. verteilter elektronischer Unterschrift (VEU), wenn

- alle erforderlichen elektronischen Unterschriften der bevollmächtigten Teilnehmer (ggf. in Verbindung mit der Funktionalität der Kunden-ID-übergreifenden verteilten elektronischen Unterschrift) innerhalb von 14 Kalendertagen eingegangen sind,
- die elektronischen Unterschriften geprüft und verarbeitet wurden,
- die elektronischen Unterschriften zur Autorisierung des Zahlungsauftrags ausreichten und
- der Auftrag dokumentiert zur Weiterverarbeitung weitergeleitet wurde.

Die Bank ist verpflichtet, die vorstehenden Abläufe im DFÜ-Protokoll zu dokumentieren. Der Teilnehmer ist seinerseits verpflichtet, das DFÜ-Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Spezifikation der EBICS-Anbindung (siehe Nummer 15) entspricht, zeitnah abzurufen, die vorstehenden dokumentierten Arbeitsabläufe zu prüfen, zu seinen Unterlagen zu nehmen und auf Anforderung der Bank zur Verfügung zu stellen.
Der Austausch von elektronischen Unterschriften und die Funktionalität der Kunden-ID-übergreifenden verteilten elektronischen Unterschrift sind spezifiziert in der DFÜ-Verfahrensbeschreibung (siehe Nummer 15). Die Erweiterung bzgl. der Funktionalität der Kunden-ID-übergreifenden verteilten elektronischen Unterschrift muss vereinbart werden.

5.2 mit personalisiertem Sicherheitsmerkmal (PIN/TAN) und Authentifizierungsinstrument (BFS-Token ggf. mit Token-PIN), wenn

- der Teilnehmer den Auftrag (z. B. Überweisungen) mit einer mittels seines BFS-Token erzeugten TAN (ggf. mit Token-PIN und unter Einbeziehung von Auftragsdaten) freigegeben hat,
- alle erforderlichen Teilnehmerfreigaben innerhalb von 14 Kalendertagen eingegangen sind,
- die Teilnehmerfreigaben geprüft und verarbeitet wurden,
- die Teilnehmerfreigaben zur Autorisierung des Zahlungsauftrags ausreichen und
- die Bank den Auftragseingang bestätigt und die Weiterleitung zur Weiterverarbeitung dokumentiert wurde.
- Bei der Bestätigung zeigt die Bank dem Teilnehmer Daten aus seinem Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers) an.

Reicht ein Service-Rechenzentrum die Auftragsdaten per EBICS ein, erfolgt die Autorisierung durch den Kunden bzw. dessen Teilnehmer mit personalisiertem Sicherheitsmerkmal (PIN/TAN) und Authentifizierungsinstrument (BFS-Token ggf. mit Token-PIN).

5.3 gemäß individueller Vereinbarung zwischen Kunde und Bank
In Ausnahmefällen können bzgl. der Autorisierung von eingereichten Zahlungsaufträgen individuelle Verfahren (abweichend von den Punkten 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. Die Bank bestätigt den Eingang der Auftragsdatei im DFÜ-Protokoll.

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 für die notwendige Autorisierung (z. B. gemeinsame Verfügungsberechtigung) vorliegt,
- 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 Kunden vereinbarte Limit (siehe Punkt 1 Unterpunkt 4) nicht überschritten wird.

(2) Liegen die Ausführungsbedingungen nach Satz 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 und – soweit möglich – über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, informieren (z. B. im DFÜ-Protokoll). Die Bank ist berechtigt, nicht vollständig autorisierte Auftragsdaten nach Ablauf des von der Bank mitgeteilten Zeitlimits zu löschen.

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 dieser einen Geschäftstag vor Ausführung bei der Bank eingegangen 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.

10 Sorgfaltspflichten

10.1 Verfahrensbestimmungen
(1) Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer diese Bedingungen nebst Anlagen beachten.

10.2 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 und nur über diese den Datenaustausch mit der Bank durchzuführen.
(2) Eine Nutzung außerhalb der durch die Bank gesondert mitgeteilten Zugangskanäle (z. B. auf Online-Händlerseiten) ist nicht erlaubt.
(3) Der Kunde hat für einen ausreichenden Schutz der von ihm bzw. von seinen Teilnehmern eingesetzten Systeme Sorge zu tragen und muss dabei die Sicherheitshinweise der Bank, insbesondere die empfohlenen Maßnahmen zum Schutz der eingesetzten Hard- und Software, beachten.

(4) 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.

(5) Im Rahmen 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.

(6) Wenn sicherheitsrelevante Updates für das jeweils eingesetzte Betriebssystem und weitere installierte sicherheitsrelevante Software-Programme vorliegen, muss das EDV-System des Kunden mit diesen aktualisiert werden.

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

10.3 Geheimhaltung und sichere Aufbewahrung
(1) Jeder Teilnehmer hat dafür Sorge zu tragen, dass keine andere Person in den Besitz seiner Legitimations- und Sicherungsmedien bzw. seines personalisierten Sicherheitsmerkmals und Authentifizierungsinstruments gelangt, von diesen Kenntnis erlangt (z. B. durch Ausspähen) oder diese nutzen kann.
(2) Die Legitimations- und Sicherungsmedien bzw. das personalisierte Sicherheitsmerkmal und Authentifizierungsinstrument dürfen nicht an Dritte (z. B. per E-Mail) weitergegeben werden.
(3) Bei Ablage der Legitimations- und Sicherungsmedien bzw. des personalisierten Sicherheitsmerkmals auf einem technischen EDV-System ist der Kunde dafür verantwortlich, dass dieses vor unautorisiertem Zugriff geschützt wird. Der Zugriffsschutz bezieht sich auch auf Duplikate der Medien.

Jede andere Person, die im Besitz der Legitimations- und Sicherungsmedien bzw. des personalisierten Sicherheitsmerkmals und Authentifizierungsinstruments ist, kann diese im Rahmen des vereinbarten Kommunikationsweges missbräuchlich nutzen.

10.4 Sicherung
Im Rahmen der DFÜ-Verfahren gem. der DFÜ-Verfahrensbeschreibung (siehe Nummer 15) hat der Kunde vor einer Übertragung von Datensätzen an die Bank eine Kopie oder Aufzeichnung der zu übertragenen 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 Ausführungstag in der Form nachweisbar zu halten, dass die Datensätze auf Anforderung der Bank kurzfristig erneut zur Verfügung gestellt werden können. Außerdem hat der Kunde für jeden Datenaustausch ein maschinelles Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Spezifikation für die EBICS-Anbindung (siehe Nummer 15) entspricht, zu erstellen, zu seinen Unterlagen zu nehmen und auf Anforderung der Bank zur Verfügung zu stellen.

10.5 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 (siehe Nummer 5.2), ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten prüfen.

11 Anzeige- und Unterrichtungspflichten

11.1 Sperranzeige
(1) Stellt der Teilnehmer den Verlust oder den Diebstahl seiner Legitimations- und Sicherungsmedien bzw. seines Authentifizierungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seiner Legitimations- und Sicherungsmedien bzw. seines persönlichen Sicherheitsmerkmals und Authentifizierungsinstruments fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über eine gesondert mitgeteilte Telefonnummer 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 Authentifizierungsinstrument oder die Kenntnis seines personalisierten Sicherheitsmerkmals erlangt hat oder
- seine Legitimations- und Sicherungsmedien bzw. sein personalisiertes Sicherheitsmerkmal und sein Authentifizierungsinstrument 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 Authentifizierungsinstrument.

12.2 Automatisierte Sperre eines Teilnehmers
Der Teilnehmer-Zugang sperrt sich selbst, wenn dreimal in Folge die Passwörter seiner Legitimations- und Sicherungsmedien bzw. sein personalisiertes Sicherheitsmerkmal und sein Authentifizierungsinstrument falsch eingegeben wurden.

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 Authentifizierungsinstrumente eines Teilnehmers oder den gesamten elektronischen Zugriff aller Teilnehmer per Sperranzeige über eine gesondert mitgeteilte Telefonnummer 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 Authentifizierungsinstruments dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der Legitimations- und Sicherungsmedien bzw. des personalisierten Sicherheitsmerkmals und des Authentifizierungsinstruments besteht.

(2) Die Bank wird den Kunden/Teilnehmer 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 Authentifizierungsinstrument 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 oder fehlerhaft ausgeführten Auftrag
(1) Die Haftung der Bank bei einer nicht autorisierten bzw. einer nicht oder fehlerhaft 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. nicht oder fehlerhaft ausgeführten Auftrag durch ein vom Kunden berechtigtes Service-Rechenzentrum, 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 Authentifizierungsinstruments 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 Authentifizierungsinstruments, haftet der Kunde für den der Bank hierdurch entstandenen Schaden bis zu einem Betrag von 150,00 EUR, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust oder Diebstahl ein Verschulden trifft.
(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Legitimations- und Sicherungsmediums bzw. personalisierten Sicherheitsmerkmals und Authentifizierungsinstruments, ohne dass dieses verloren gegangen oder gestohlen worden ist, haftet der Kunde für den der Bank hierdurch entstandenen Schaden bis zu einem Betrag von 150,00 EUR, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung seines Legitimations- und Sicherungsmediums bzw. personalisierten Sicherheitsmerkmals und Authentifizierungsinstruments schuldhaft verletzt hat.
(3) Der Kunde ist nicht zum Ersatz des Schadens nach den Sätzen 1 und 2 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 und dadurch der Schaden eingetreten ist.
(4) 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 Kunde den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fährlässigkeit des Teilnehmers kann insbesondere dann vorliegen, wenn er

- den Verlust oder Diebstahl oder die missbräuchliche Nutzung des Legitimations- und Sicherungsmediums bzw. personalisierten Sicherheitsmerkmals und Authentifizierungsinstruments 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 im Kundensystem bzw. im System des durch ihn beauftragten Dritten gespeichert hat, welches nicht ausreichend gegen unautorisierten Zugriff geschützt war (siehe Nummer 10.3 Satz 3),
- die Legitimations- und Sicherungsmedien bzw. das personalisierte Sicherheitsmerkmal und Authentifizierungsinstrument einer anderen Person (z. B. per E-Mail) mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 10.3 Satz 2),
- die Nutzung außerhalb der gesondert mitgeteilten Zugangskanäle (z. B. Internetseiten) eingegeben hat (siehe Nummer 10.1 Satz 2).

(5) Ist der Kunde kein Verbraucher gemäß § 13 BGB (Bürgerliches Gesetzbuch), haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150,00 EUR nach Satz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

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,
- Spezifikation für die EBICS-Anbindung,
- DFÜ-Verfahrensbeschreibung und
- Bedingungen zur Fernwartung

sind Bestandteile der elektronischen Kontoführung und sind unter www.sozialbank.de veröffentlicht.

Stand: 01.01.2016