



## Bedingungen zur elektronischen Kontoführung

---

### 1. Leistungsangebot

(1) Der Kunde bzw. der durch ihn beauftragte Dritte (z. B. ein Service-Rechenzentrum, ein Dienstleister oder ein anderer Kunde der Bank für Sozialwirtschaft AG) können Bankgeschäfte auf elektronischen Wege in dem mit der Bank für Sozialwirtschaft AG vereinbarten Umfang (Kommunikationsweg, Auftragsarten, angebundene Konten, berechnigte Personen, E-Banking-Vollmacht) abwickeln.

(2) Die durch den Kunden bzw. durch den von ihm beauftragten Dritten benannten berechtigten, natürlichen Personen werden im Folgenden als „Teilnehmer“ bezeichnet. Die Bank für Sozialwirtschaft AG wird im Folgenden als „Bank“ bezeichnet. Die Datenfernübertragung auf elektronischem Wege unter Einsatz elektronischer Unterschriften/Signaturen wird im Folgenden als „DFÜ“ bezeichnet.

(3) Im Rahmen der elektronischen Kontoführung ist die Bank berechnigt

- dem Kunden, dem von ihm beauftragten Dritten, den Teilnehmern bzw. u.U. den dafür speziell benannten Personen (z. B. Administratoren) Informationen, Daten und Mitteilungen direkt per Post, per Fax, per eMail oder über den vereinbarten Kommunikationsweg zukommen zu lassen.
- im Supportfall, zur Wartung oder zur Problembehebung für das vom Kunden eingesetzte E-Banking-Produkt der Bank auf dem EDV-System des Kunden während der veröffentlichten Servicezeiten Fernwartungsarbeiten gem. den Bedingungen zur Fernwartung (siehe Nummer 15) durchzuführen.

### 2. Voraussetzungen zur elektronischen Kontoführung

Anhand der vertraglichen Regelung wird für jeden Kunden bzw. für jeden von ihm beauftragten Dritten eine Kunden-ID und für jeden Teilnehmer eine Teilnehmer-ID angelegt. Zu jeder Teilnehmer-ID werden die Berechnigungen des Teilnehmers gespeichert (z. B. E-Banking-Vollmacht, Auftragsarten). Aufträge nach Nummer 5 können nur Teilnehmer erteilen, die im Rahmen der vertraglichen Regelung mit dem Kunden bzw. mit dessen beauftragten Dritten eine spezielle E-Banking-Vollmacht erhalten haben. Diese kann zu einer eventuell bereits bestehenden Kontovollmacht abweichend sein.

### 3. Datenaustausch

(1) Der Austausch von Auftragsdaten und Informationen erfolgt über den vereinbarten Kommunikationsweg 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 vereinbarten Kommunikationsweg gekoppelt sind.

### 4. Einlieferung von Auftragsdaten

Unter Berücksichtigung der vertraglichen und technischen Vorgaben (siehe Nummer 3) übermittelt der Teilnehmer die Auftragsdaten an die Bank. Die Bank bestätigt den Eingang der Auftragsdaten innerhalb des vereinbarten Kommunikationsweges (z. B. DFÜ-Protokoll im DFÜ-Verfahren).

### 5. Auftrags-Autorisierung

Eingelieferte Auftragsdaten werden gegenüber der Bank wirksam, wenn sie, wie mit dem Kunden oder mit dessen beauftragten Dritten vereinbart, wie folgt autorisiert wurden:

#### 5.1 mit Elektronischer Unterschrift (EU) bzw. Verteilter Elektronischer Unterschrift (VEU), wenn

- alle erforderlichen, Elektronischen Unterschriften/Signaturen der bevollmächtigten Teilnehmer über den vereinbarten Kommunikationsweg ggfs. in Verbindung mit der Funktionalität der Kunden-ID übergreifende Verteilten Elektronischen Unterschrift gemäß der DFÜ-Verfahrensbeschreibung (siehe Nummer 15) innerhalb von 14 Kalendertagen eingegangen sind,
- die Elektronischen Unterschriften/Signaturen geprüft und verarbeitet wurden,
- die Elektronischen Unterschriften zur Autorisierung des Zahlungsauftrages ausreichen und
- der Auftrag im DFÜ-Protokoll dokumentiert zu 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 bzw. von Kapitel 1.7 der Spezifikation der FTAM-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/Signaturen 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 vertraglich vereinbart werden.

#### **5.2 mit Personalisiertem Sicherheitsmerkmal (PIN/TAN) und Authentifizierungsinstrument (BFS-Token ggfs. mit Token-PIN), wenn**

- der Teilnehmer den Auftrag (z. B. Überweisungen) mit einer mittels seines BFS-Token erzeugten TAN (ggfs. mit Token-PIN) freigegeben hat,
- alle erforderlichen Teilnehmerfreigaben innerhalb von 14 Kalendertagen eingegangen sind,
- die Teilnehmerfreigaben geprüft und verarbeitet wurden,
- die Teilnehmerfreigaben zur Autorisierung des Zahlungsauftrages 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 oder Dienstleister die Auftragsdaten per EBICS ein, kann mit dem Kunden und mit dem Service-Rechenzentrum bzw. Dienstleister vereinbart werden, dass die Autorisierung durch den Kunden bzw. dessen Teilneh-

mer(n) mit Personalisiertem Sicherheitsmerkmal (PIN/TAN) und Authentifizierungsinstrument (BFS-Token ggfs. mit Token-PIN) erfolgt. Die Einreichung der Auftragsdatei erfolgt durch einen vom Service-Rechenzentrum bzw. Dienstleister berechtigten Teilnehmer. Die Bank bestätigt den Eingang der Auftragsdatei im DFÜ-Protokoll. Der Teilnehmer ist seinerseits verpflichtet das DFÜ-Protokoll zeitnah abzurufen und die vorstehenden dokumentierten Arbeitsabläufe in Augenschein zu nehmen.

#### **5.3 mit beleghaften Datenträgerbegleitzettel, wenn**

- der Datenträgerbegleitzettel innerhalb von 14 Kalendertagen eingeht und
- dieser alle erforderlichen Unterschriften entsprechend den bei der Bank hinterlegten Kontovollmachten enthält.

Bei der Auftragseinreichung kann vereinbart werden, dass die Autorisierung anhand beleghafter Datenträgerbegleitzettel erfolgen kann. Die Einreichung der Auftragsdatei erfolgt durch einen entsprechend berechtigten Teilnehmer. Die Bank bestätigt den Eingang der Auftragsdatei im DFÜ-Protokoll. Der Teilnehmer ist seinerseits verpflichtet das DFÜ-Protokoll, das inhaltlich den Bestimmungen bzw. von Kapitel 1.7 der Spezifikation der FTAM-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.

### **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 oder auf dem Datenträgerbegleitzettel 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 Überweisungsbedingungen.



## 7. Auftragsbearbeitung durch die Bank

(1) Die Bank wird den Auftrag ausführen, wenn zum Zugangszeitpunkt

- dieser gemäß der mit dem Kunden bzw. mit dessen beauftragten Dritten geschlossenen Vereinbarung nach Nummer 5.1, 5.2 bzw. 5.3 autorisiert wurde,
- die Berechtigung des Teilnehmers für die jeweilige Auftragsart beziehungsweise die notwendige Autorisierung (z. B. gemeinsame Verfügungsberechtigung) vorliegt,
- das Datenformat gemäß der Spezifikation der Datenformate (siehe Nummer 15) eingehalten ist und
- die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Überweisungsbedingungen) vorliegen.

(2) Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank den Auftrag nach Maßgabe der Bestimmungen für die jeweilige Auftragsart 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 über den vereinbarten Kommunikationsweg (z. B. im DFÜ-Protokoll) eine Information zur Verfügung stellen.

## 8. Widerruf von Aufträgen

(1) Nach Zugang des Auftrags bei der Bank (z. B. bei Überweisungen - siehe Nummer 1.4 Absätze 1 und 2 der Sonderbedingungen für den Überweisungsverkehr) kann der Kunde diesen nicht mehr widerrufen. Bis zu diesem Zeitpunkt ist ein Widerruf durch Erklärung gegenüber der Bank außerhalb des vereinbarten Kommunikationswegs möglich.

(2) Haben Bank und Kunde einen bestimmten Termin für die Ausführung des Auftrages vereinbart (z. B. bei Überweisungen - siehe Nummer 2.2.2 Absatz 2 der Sonderbedingungen für den

Überweisungsverkehr), kann der Kunde diesen bis zum Ende des vor dem vereinbarten Tag liegenden Geschäftstags der Bank widerrufen. Die Geschäftstage der Bank ergeben sich aus dem „Preis- und Leistungsverzeichnis“.

(3) Nach den in Absätzen 1 und 2 genannten Zeitpunkten kann der Auftrag nur widerrufen werden, wenn Kunde und Bank dies vereinbart haben. Die Vereinbarung wird wirksam, wenn es der Bank gelingt, die Ausführung zu verhindern oder den Auftragsbetrag zurückzuerlangen. Für die Bearbeitung eines solchen Widerrufs des Kunden berechnet die Bank das im „Preis- und Leistungsverzeichnis“ ausgewiesene Entgelt.

## 9. Informationen des Kunden 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 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 bzw. der von ihm beauftragte Dritte hat für einen ausreichenden Schutz der von ihm bzw. von seinen Teil-



nehmern eingesetzten Systeme zu tragen und muss dabei die Sicherheitshinweise der Bank, insbesondere die empfohlenen Maßnahmen zum Schutz der eingesetzten Hard- und Software, beachten.

(4) Im Rahmen des EBICS-Verfahrens sind darüber hinaus folgende Sicherheitsmaßnahmen durch den Kunden bzw. dessen beauftragten Dritten folgende Anforderungen zu berücksichtigen:

- Die vom Kunden bzw. dessen beauftragten Dritten für das EBICS-Verfahren eingesetzte Software muss die in der DFÜ-Verfahrensbeschreibung (siehe Nummer 15) beschriebenen Anforderungen erfüllen.
- Das EBICS-EDV-System des Kunden bzw. dessen beauftragten Dritten dürfen nicht ohne Firewall eingesetzt werden. Eine Firewall ist eine Einrichtung, die den gesamten ein- und ausgehenden Nachrichtenverkehr überwacht und nur bekannte oder autorisierte Verbindungen zulässt.
- Auf dem EBICS-EDV-System des Kunden bzw. dessen beauftragten Dritten ein Virenschanner installiert und aktiviert ist, der regelmäßig mit den neuesten Virendefinitionsdateien versorgt wird.
- Das EBICS-EDV-System des Kunden bzw. dessen beauftragten Dritten 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.
- Wenn sicherheitsrelevante Updates für das jeweils eingesetzte Betriebssystem und weiterer installierter sicherheitsrelevanter Software-Programme vorliegen, sollten die eingesetzten EBICS-EDV-System des Kunden bzw. dessen beauftragten Dritten mit diesen aktualisiert werden.

Die Umsetzung dieser Anforderungen liegt ausschließlich in der Verantwortung des Kunden bzw. dessen beauftragten Dritten.

## 10.2 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 eMail) weitergegeben werden.

(3) Bei Ablage der Legitimations- und Sicherungsmedien bzw. des Personalisierten Sicherheitsmerkmals auf einem technischen System ist der Kunde bzw. der von ihm beauftragte Dritte dafür verantwortlich, dass dieses vor unautorisiertem Zugriff geschützt wird. Der Zugriffsschutz bezieht sich auch auf Duplikate der Medien.

Denn jede andere Person, die im Besitz der Legitimations- und Sicherungsmedien bzw. des Personalisierten Sicherheitsmerkmals und Authentifizierungsinstruments ist, kann diese im Rahmen des vereinbarten Kommunikationswegs missbräuchlich nutzen.

## 10.3 Sicherung

Im Rahmen der DFÜ-Verfahren gem. der DFÜ-Verfahrensbeschreibung (siehe Nummer 15) hat der Kunde bzw. der von ihm beauftragte Dritte vor einer Übertragung von Datensätzen an die Bank eine Kopie oder Aufzeichnung der zu übertragenen Datensätze mit dem vollständigem Inhalt sowie der zur Prüfung der Legitimation übermittelten Daten zu erstellen. Diese ist vom Kunden bzw. von dessen beauftragten Dritten für einen Zeitraum von 14 Kalendertagen bei Inlandszahlungsaufträgen und 30 Kalendertagen bei Auslandzahlungsaufträgen 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 bzw. der von ihm beauftragte Dritte 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.



## 10.4 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 (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 den 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 oder der durch ihn beauftragte Dritte 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 liegende 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.

### 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.

## 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 ein nicht autorisierter bzw. nicht oder fehlerhaft ausgeführter Auftrag durch einen vom Kunden berechtigten Service-Rechenzentrum/Dienstleister, so kann die Bank von diesen 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 abhanden gekommenen 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 dem 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. Große Fahrlässigkeit 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 unautorisiertem Zugriff geschützt war (siehe Nummer 10.2 Satz 3),
- die Legitimations- und Sicherungsmedien bzw. das Personalisierte Sicherheitsmerkmal und Authentifizierungsinstrument einer anderen Person (z. B. per eMail) mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 10.2 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 der 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
- Spezifikation für die FTAM-Anbindung
- DFÜ-Verfahrensbeschreibung
- Bedingungen zur Fernwartung

sind Bestandteile der mit dem Kunden bzw. mit dem von ihm beauftragten Dritten geschlossenen Vereinbarung und sind unter [www.sozialbank.de](http://www.sozialbank.de) veröffentlicht.