

### **I. Leistungsumfang**

1. Das Kreditinstitut steht seinem Kunden (Kontoinhaber) für die Datenfernübertragung auf elektronischem Wege – nachfolgend „Datenfernübertragung“ oder „DFÜ“ genannt – zur Verfügung. Die Datenfernübertragung umfasst die Auftragserteilung sowie den Datenaustausch (Übermittlung von Aufträgen und Informationsabruf).
2. Das Kreditinstitut gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen der Datenfernübertragung nutzen kann. Zur Nutzung der Datenfernübertragung gelten die mit dem Kreditinstitut vereinbarten Verfügungsmitel.
3. Die Datenfernübertragung ist über zwei verschiedene Verfahren, die EBICS-Anbindung (Anlage 1a bis 1c) und die FTAM-Anbindung (Anlage 2a und 2b) möglich. Das maßgebliche Übertragungsverfahren wird zwischen Kunde und Kreditinstitut vereinbart.
4. Der Satz- und Dateiaufbau für die Übermittlung von Aufträgen und den Informationsabruf wird in der Spezifikation der Datenformate (Anlage 3) beschrieben.

### **II. Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien**

1. Aufträge können über die EBICS- oder FTAM-Anbindung nur vom Kunden oder seinen Kontobevollmächtigten erteilt werden. Kunde und Kontobevollmächtigte werden im Folgenden einheitlich als „Nutzer“ bezeichnet. Zur Autorisierung von per DFÜ übermittelten Auftragsdaten benötigt jeder Nutzer jeweils individuelle, vom Kreditinstitut freigeschaltete Legitimationsmedien. Die Anforderungen an die Legitimationsmedien sind in Anlage 1a bzw. 2a definiert. Wenn mit dem Kreditinstitut vereinbart, können per DFÜ übermittelte Auftragsdaten mit unterschriebenem Begleitzettel autorisiert werden.
2. Für den Datenaustausch über die EBICS-Anbindung kann der Kunde zusätzlich zu den Bevollmächtigten „Technische Teilnehmer“ benennen, die lediglich befugt sind, den Datenaustausch durchzuführen. Nutzer und Technische Teilnehmer werden im Folgenden unter dem Begriff „Teilnehmer“ zusammengefasst. Für die Absicherung des Datenaustauschs benötigt jeder Teilnehmer jeweils individuelle, vom Kreditinstitut freigeschaltete Sicherungsmedien. Die Anforderungen an die Sicherungsmedien sind in Anlage 1a beschrieben.
3. Für den Datenaustausch über die FTAM-Anbindung benötigt jeder Nutzer ein vom Kreditinstitut bereitgestelltes DFÜ-Passwort. Die Anforderungen an das DFÜ-Passwort sind in Anlage 2a beschrieben.
4. Legitimations- und Sicherungsmedien sind Authentifizierungsinstrumente im Sinne von § 1 Absatz 5 Zahlungsdienstleistungsgesetz.

### **III. Verfahrensbestimmungen**

1. Für das zwischen Kunde und Kreditinstitut vereinbarte Übertragungsverfahren gelten jeweils die in Anlage 1a beziehungsweise Anlage 2a sowie die in der Dokumentation der technischen Schnittstellen (Anlage 1b beziehungsweise Anlage 2b) und der Spezifikation der Datenformate (Anlage 3) beschriebenen Anforderungen.
2. Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer die mit dem Kreditinstitut vereinbarten Verfahren und Spezifikationen beachten.
3. Die Belegung der Datenfelder richtet sich nach den Belegungs- und Kontrollrichtlinien des jeweils genutzten Formates.
4. Für Zahlungsaufträge hat der Nutzer die Kundenkennung (Kontonummer und Bankleitzahl oder IBAN und BIC) des Zahlers und die Kundenkennung des Zahlungsempfängers (Kontonummer und Bankleitzahl oder IBAN und BIC oder andere Kennung des Zahlungsdienstleisters des Zahlungsempfängers) zutreffend anzugeben. Die in die Abwicklung des Zahlungsauftrages eingeschalteten Zahlungsdienstleister sind berechtigt, die Bearbeitung ausschließlich anhand der

Kundenkennungen vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Auftrags zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zu Lasten des Kunden.

5. Vor Übertragung von Auftragsdaten an das Kreditinstitut ist eine Aufzeichnung der zu übertragenden Dateien mit deren vollständigem Inhalt sowie der zur Prüfung der Legitimation übermittelten Daten zu erstellen. Diese ist von dem Kunden mindestens für einen Zeitraum von 14 Kalendertagen bei Inlandszahlungsaufträgen und 30 Kalendertagen bei Auslandszahlungsaufträgen ab dem Ausführungstag in der Form nachweisbar zu halten, dass die Datei auf Anforderung des Kreditinstitutes kurzfristig erneut zur Verfügung gestellt werden kann, sofern nichts Abweichendes vereinbart wird.

6. Außerdem hat der Kunde für jeden Datenaustausch ein maschinelles Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Spezifikation für die EBICS-Anbindung (Anlage 1b) bzw. Kapitel 1.7 der Spezifikation für die FTAM-Anbindung (Anlage 2b) entspricht, zu erstellen, zu seinen Unterlagen zu nehmen und auf Anforderung des Kreditinstitutes zur Verfügung zu stellen.

7. Soweit das Kreditinstitut dem Kunden Daten über die Zahlungsvorgänge zur Verfügung stellt, die noch nicht endgültig bearbeitet sind, stellen diese lediglich eine unverbindliche Information dar. Die Daten sind jeweils besonders gekennzeichnet.

8. Die per DFÜ eingelieferten Auftragsdaten sind wie mit dem Kreditinstitut vereinbart entweder mit Elektronischer Unterschrift oder dem unterschriebenen Begleitzettel zu autorisieren. Diese Auftragsdaten werden als Auftrag wirksam

a) bei Einreichung mit Elektronischer Unterschrift, wenn

- alle erforderlichen Elektronischen Unterschriften der Nutzer per Datenfernübertragung innerhalb des vereinbarten Zeitraumes eingegangen sind und
- die Elektronischen Unterschriften mit den vereinbarten Schlüsseln erfolgreich geprüft werden können

oder

b) bei Einreichung mit Begleitzettel, wenn

- der Begleitzettel im vereinbarten Zeitraum bei dem Kreditinstitut eingegangen ist und
- der Begleitzettel der Kontovollmacht entsprechend unterzeichnet worden ist.

### **IV. Verhaltens- und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags**

1. Der Kunde ist in Abhängigkeit von dem mit dem Kreditinstitut vereinbarten Übertragungsverfahren verpflichtet sicherzustellen, dass alle Nutzer die in Anlage 1a bzw. Anlage 2a beschriebenen Legitimationsverfahren einhalten.

2. Mit Hilfe der vom Kreditinstitut freigeschalteten Legitimationsmedien kann der Nutzer Aufträge erteilen. Der Kunde stellt sicher, dass jeder Nutzer dafür Sorge trägt, dass keine andere Person in den Besitz seines Legitimationsmediums kommt, sowie Kenntnis von dem zu dessen Schutz dienenden Passwortes erlangt. Denn jede andere Person, die im Besitz des Mediums oder eines entsprechenden Duplikates ist, kann in Verbindung mit dem dazugehörigen Passwort die vereinbarten Dienstleistungen missbräuchlich nutzen.

Insbesondere Folgendes ist zur Geheimhaltung der Legitimationsmedien zu beachten:

- Die dem Nutzer legitimierenden Daten dürfen nicht außerhalb des Legitimationsmediums, z.B. auf der Festplatte des Rechners, gespeichert werden;
- das Legitimationsmedium ist nach Beendigung der DFÜ-Nutzung aus dem Lesegerät zu entnehmen und sicher zu verwahren;

## **Bedingungen für die Datenfernübertragung (Stand: Oktober 2009)**

2/3

- das zum Schutz des Legitimationsmediums dienende Passwort darf nicht notiert oder elektronisch abgespeichert werden;
- bei Eingabe des Passwortes ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.

### **V. Verhaltens- und Sorgfaltspflichten im Umgang mit den Sicherungsmedien für den Datenaustausch**

1. Der Kunde ist im Rahmen der EBICS-Anbindung verpflichtet sicherzustellen, dass alle Teilnehmer die in Anlage 1a beschriebenen Sicherungsverfahren einhalten.

Mit Hilfe der vom Kreditinstitut freigeschalteten Sicherungsmedien sichert der Teilnehmer den Datenaustausch ab. Der Kunde ist dazu verpflichtet sicherzustellen, dass jeder Teilnehmer dafür Sorge trägt, dass keine andere Person in den Besitz seines Sicherungsmediums kommt oder dieses nutzen kann. Insbesondere im Falle der Ablage auf einem technischen System muss das Sicherungsmedium des Teilnehmers in einer technischen Umgebung gespeichert werden, die vor unautorisiertem Zugriff geschützt ist. Denn jede andere Person, die Zugriff auf das Sicherungsmedium oder ein entsprechendes Duplikat hat, kann den Datenaustausch missbräuchlich durchführen.

2. Der Kunde ist im Rahmen der FTAM-Anbindung verpflichtet sicherzustellen, dass alle Nutzer die in Anlage 2a beschriebenen Sicherungsverfahren einhalten. Der Kunde stellt sicher, dass jeder Nutzer dafür Sorge trägt, dass keine andere Person Kenntnis von seinem DFÜ-Passwort erlangt. Denn jede andere Person, die das DFÜ-Passwort kennt, kann den Datenaustausch mit dem Kreditinstitut durchführen.

### **VI. Sperre der Legitimations- und Sicherungsmedien**

1. Gehen die Legitimations- oder Sicherungsmedien verloren, werden sie anderen Personen bekannt oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so hat der Teilnehmer unverzüglich seinen DFÜ-Zugang beim Kreditinstitut zu sperren oder sperren zu lassen. Näheres regeln Anlage 1a und Anlage 2a. Der Teilnehmer kann dem Kreditinstitut eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

2. Wird dreimal hintereinander versucht, einen Auftrag mit einem falschen Legitimationsmedium an das Kreditinstitut zu übermitteln oder mit einem falschen Sicherungsmedium den Datenaustausch durchzuführen, so sperrt das Kreditinstitut den DFÜ-Zugang des betreffenden Teilnehmers. Diese Sperre kann mittels DFÜ nicht aufgehoben werden. Zur Aufhebung dieser Sperre muss sich der Kunde mit seinem Kreditinstitut in Verbindung setzen.

3. Der Kunde kann außerhalb des DFÜ-Verfahrens die Verwendung der Legitimations- und Sicherungsmedien eines Teilnehmers oder den gesamten DFÜ-Zugang über die vom Kreditinstitut bekannt gegebene Sperrfazität sperren lassen.

4. Das Kreditinstitut wird den gesamten DFÜ-Zugang sperren, wenn der Verdacht einer missbräuchlichen Nutzung des DFÜ-Zugangs besteht. Es wird den Kunden hierüber außerhalb des DFÜ-Verfahrens informieren. Diese Sperre kann mittels DFÜ nicht aufgehoben werden.

### **VII. Behandlung eingehender Auftragsdaten durch das Kreditinstitut**

1. Die dem Kreditinstitut im DFÜ-Verfahren übermittelten Auftragsdaten werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet.

Kann das Kreditinstitut eine vom Kunden im Format „SEPA-Überweisung“ beleglos erteilte Überweisung nicht in diesem Format ausführen, weil der vom Kunden angegebene Zahlungsdienstleister des Zahlungsempfängers dieses Format nicht unterstützt, und weist das Kreditinstitut die Überweisung nicht zurück, kann sie die Überweisung in einem von dem Zahlungsdienstleister des Zahlungsempfängers unterstütztem Format ausführen. Bei diesem Formatwechsel

können die in der Anlage 4 genannten Datenelemente – oder Teile davon – nicht übermittelt werden.

2. Das Kreditinstitut prüft anhand der von den Teilnehmern mittels der Sicherungsmedien erstellten Signaturen, ob der Absender berechtigt ist, den Datenaustausch durchzuführen. Ergibt die Prüfung Unstimmigkeiten, wird das Kreditinstitut den betreffenden Auftrag nicht verarbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen.

3. Das Kreditinstitut prüft die Legitimation des Nutzers bzw. der Nutzer und die Autorisierung der per DFÜ übermittelten Auftragsdaten anhand der von den Nutzern mittels der Legitimationsmedien erstellten Elektronischen Unterschriften oder des übermittelten Begleitzettels sowie die Übereinstimmung der Auftragsdatensätze mit den Bestimmungen gemäß Anlage 3. Ergibt die Prüfung Unstimmigkeiten, wird das Kreditinstitut die betreffenden Aufträge nicht bearbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen. Das Kreditinstitut ist berechtigt, nicht vollständig autorisierte Aufträge nach Ablauf des von dem Kreditinstitut gesondert mitgeteilten Zeitlimits zu löschen.

4. Ergeben sich bei den von dem Kreditinstitut durchgeführten Prüfungen der Dateien oder Datensätze nach Anlage 3 Fehler, so wird das Kreditinstitut die fehlerhaften Dateien oder Datensätze in geeigneter Form nachweisen und sie dem Nutzer unverzüglich mitteilen. Das Kreditinstitut ist berechtigt, die fehlerhaften Dateien oder Datensätze von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrages nicht sichergestellt werden kann.

5. Die Bank ist verpflichtet die Abläufe (siehe Anlage 1a und 2a) und die Weiterleitung der Aufträge zur Bearbeitung im Kundenprotokoll zu dokumentieren. Der Kunde ist seinerseits verpflichtet, das Kundenprotokollzeitnah abzurufen und sich über den Status der Auftragsbearbeitung zu informieren. Bei Unstimmigkeiten soll er sich mit der Bank in Verbindung setzen.

### **VIII. Rückruf**

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. Das Kreditinstitut kann einen Rückruf allerdings nur beachten, wenn ihm diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufes möglich ist. Änderungen eines Dateiinhaltes sind nur durch Rückruf der Datei und erneute Auftragserteilung möglich.

2. Die Widerrufbarkeit eines Auftrags richtet sich nach den dafür geltenden Sonderbindungen (z.B. Bedingungen für den Überweisungsverkehr). Hierzu hat der Kunde dem Kreditinstitut die Einzelangaben des Originalauftrages mitzuteilen.

### **IX. Ausführung der Aufträge**

1. Das Kreditinstitut wird die Aufträge ausführen, wenn alle nachfolgenden Ausführungsbedingungen vorliegen:

- Die per DFÜ eingelieferten Auftragsdaten wurden gemäß Nummer 3 Absatz 8 autorisiert.
- Das festgelegte Datenformat ist eingehalten.
- Das Verfügungslimit, sofern vereinbart, ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Bedingungen (z.B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

2. Liegen die Ausführungsbedingungen nach Absatz 1 nicht vor, wird das Kreditinstitut den Auftrag nicht ausführen und den Kunden über die Nichtausführung unverzüglich auf dem vereinbarten Weg unterrichten. Soweit möglich, nennt das Kreditinstitut dem Kunden die Gründe und Fehler, die zur Nichtausführung geführt haben, und Möglichkeiten, wie diese Fehler berichtigt werden können.

#### X. Sicherheit des Kundensystems

Der Kunde hat für einen ausreichenden Schutz der von ihm für die Datenfernübertragung eingesetzten Systeme Sorge zu tragen. Die für das EBICS-Verfahren geltenden Sicherheitsanforderungen sind in Anlage 1c beschrieben.

#### XI. Haftung

##### 11.1 Haftung des Kreditinstituts bei einer nicht autorisierten DFÜ-Verfügung und einer nicht oder fehlerhaft ausgeführten DFÜ-Verfügung

Die Haftung des Kreditinstituts bei einer nicht autorisierten DFÜ-Verfügung und einer nicht oder fehlerhaft ausgeführten DFÜ-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Bedingungen (z.B. Bedingungen für den Überweisungsverkehr).

##### 11.2 Haftung des Kunden bei missbräuchlicher Nutzung der Legitimations- oder Sicherungsmedien

###### 11.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Legitimations- oder Sicherungsmediums, haftet der Kunde für den dem Kreditinstitut hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigem Abhandenkommen des Legitimations- oder Sicherungsmediums ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Legitimations- oder Sicherungsmediums, ohne dass dieses verlorengegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Kontoinhaber für den dem Kreditinstitut hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung des Legitimations- oder Sicherungsmediums schuldhaft verletzt hat.

(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 Euro nach Absatz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen gehandelt hat.

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 6 Absatz 1 nicht abgeben konnte, weil das Kreditinstitut nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

###### 11.2.2 Haftung des Kunden bei sonstigen nicht autorisierten Vorgängen vor der Sperranzeige

Beruhen nicht autorisierte Vorgänge, die keine Zahlungsvorgänge sind, vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Legitimations- oder Sicherungsmediums oder auf der sonstigen missbräuchlichen Nutzung des Legitimations- oder Sicherungsmediums und ist dem Kreditinstitut hierdurch ein Schaden entstanden, haften der Kunde und das Kreditinstitut nach den gesetzlichen Grundsätzen des Mitverschuldens.

###### 11.2.3 Haftung der Kreditinstitute ab der Sperranzeige

Sobald das Kreditinstitut eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt es alle danach durch nicht autorisierte DFÜ-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn ein Teilnehmer in betrügerischer Absicht gehandelt hat.

#### 11.3 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.

#### XII. Schlussbestimmungen

Die in diesen Bedingungen erwähnten Anlagen sind Bestandteil der mit dem Kunden geschlossenen Vereinbarung.

**Alle genannten Anlagen sind nicht abgedruckt, können aber jederzeit eingesehen werden.**

Anlage 1a: EBICS-Anbindung

Anlage 1b: Spezifikation der EBICS-Anbindung

Anlage 1c: Sicherheitsanforderungen an das EBICS-Kundensystem

Anlage 2a: FTAM-Anbindung

Anlage 2b: Spezifikation der FTAM-Anbindung

Anlage 3: Spezifikation der Datenformate

Anlage 4: Weiterleitung von Daten bei Formatwechsel