DRUCKEN

Name und Anschrift des Konto-/Depotinhabers

Kundennr:

HOTLINE:

Tel.: 07161/6714-20 oder -35
07161/6714-51 ausserhalb u. Geschäftszeiten
FAX: 07161/969316

E-Mail: tzeqaj@martinbank.de
bschrod@martinbank.de

Auftrag zur Nutzung von ONLINE-Banking mit

☐ i-TAN und/oder ☐ m-TAN auf Handy-Nr.

☐ Postbox-Verfahren ☐ täglich ☐ wöchentlich

Der/Die genannten Konto-/Depotinhaber der unter 1. aufgeführten Konten/Depots vereinbaren mit der Bank für die elektronische Datenübermittlung folgendes:

1. Vertragsgegenstand

Der/Die Konto-/Depotinhaber ist/sind zur Inanspruchnahme von ONLINE-Banking/ Postbox-Verfahren in dem von der Bank angebotenen Umfang berechtigt. Folgende Konten/Depots sollen im ONLINE-Banking/ Postbox-Verfahren freigeschaltet werden (zutreffendes bitte ankreuzen bzw. vervollständigen):

☐ alle bestehenden und zukünftigen Konten/Depots/Darlehen (nur wenn Teilnehmer zugleich Konto/ Depotinhaber)

☐ oder folgende Konto-/Depot-/Darlehen-Nr.:

2. Sperrnachricht

Die Sperrnachricht gem. den beigefügten Bedingungen kann der Nutzer unter der Hotline mitteilen. Die Bearbeitung Ihrer Sperrnachricht erfolgt zu unseren üblichen Geschäftszeiten.

3. Hinweis nach Teledienstedatenschutz

Die im Rahmen des ONLINE-Banking und Postbox-Verfahren anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank verarbeitet und genutzt.

4. Einbeziehung der Bedingungen für ONLINE-Banking und Postbox-Verfahren

Für die Teilnahme am ONLINE-Banking/Postbox-Verfahren gelten die beigefügten Bedingungen für die Nutzung des ONLINE-Banking sowie Postbox-Verfahren .

5. Verfügungshöchstbetrag

Verfügungen (nur Kontokorrent- u.Cashkonten) über ONLINE-Banking sind begrenzt auf EUR je Kalendertag.
(Wenn nichts notiert wurde, werden wir Privatkunden automatisch ein Limit von EUR 2.500,00 je Kalendertag und Geschäftskunden ein Limit von EUR 100.000,00 je Kalendertag einräumen.)

Ort, Datum Unterschrift des/der Konto-/Depotinhabers(s) oder Bevollmächtigten bzw. gesetzl. Vertreter

Meine / unsere Email-Adresse lautet:

Bankhaus Gebr. Martin AG
Schlossplatz 7, 73033 Göppingen
Tel.Nr. 07161/6714-0; Fax Nr.07161/979710
Email: info@martinbank.de
www.martinbank.de

Nähere Angaben zur Bank sind im „Preis- und Leistungsverzeichnis“ enthalten.

Bedingungen für das Online-Banking

1. Leistungsangebot

(1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels Online-Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Online-Banking abrufen.

(2) Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.

(3) Zur Nutzung des Online-Banking gelten die mit der Bank gesondert vereinbarten Verfügungslimite.

2. Voraussetzungen zur Nutzung des Online-Banking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels Online-Banking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifzierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4).

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- die persönliche Identifkationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN),
- der Nutzungscode für die elektronische Signatur.

2.2 Authentifzierungsinstrumente

Die TAN beziehungsweise die elektronische Signatur können dem Teilnehmer auf folgenden Authentifzierungsinstrumenten zur Verfügung gestellt werden:

- auf einer Liste mit einmal verwendbaren TAN,
- mittels eines TAN-Generators, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist,
- mittels eines mobilen Endgerätes (zum Beispiel Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
- auf einer Chipkarte mit Signaturfunktion oder
- auf einem sonstigen Authentifzierungsinstrument, auf dem sich Signaturschlüssel befnden.

Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

3. Zugang zum Online-Banking

Der Teilnehmer erhält Zugang zum Online-Banking, wenn

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

Nach Gewährung des Zugangs zum Online-Banking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

4. Online-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Online-Banking-Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (TAN oder elektronische Signatur) autorisieren und der Bank mittels Online-Banking übermitteln. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Online-Banking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Online-Banking ausdrücklich vor.

5. Bearbeitung von Online-Banking-Aufträgen durch die Bank

(1) Die Bearbeitung der Online-Banking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung) auf der Online-Banking-Seite der Bank oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank angegebenen oder im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- der Teilnehmer hat sich mit seinem Personalisierten Sicherheitsmerkmal legitimiert;
- die Berechtigung des Teilnehmers für die jeweilige Auftragsart (zum Beispiel Wertpapierorder) liegt vor;
- das Online-Banking-Datenformat ist eingehalten;
- das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten;
- die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Online-Banking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen und dem Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Online-Banking eine Information zur Verfügung stellen.

6. Information des Kontoinhabers über Online-Banking-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspfichten des Teilnehmers

7.1 Technische Verbindung zum Online-Banking

Der Teilnehmer ist verpfichtet, die technische Verbindung zum Online-Banking nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle (zum Beispiel Internetadresse) herzustellen.

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifzierungsinstrumente

(1) Der Teilnehmer hat

- seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln sowie
- sein Authentifzierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifzierungsinstruments ist, kann in Verbindung mit dem dazugehörigen Personalisierten Sicherheitsmerkmal das Online-Banking-Verfahren missbräuchlich nutzen.

(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifzierungsinstruments zu beachten:

- Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (zum Beispiel im Kundensystem).
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (zum Beispiel nicht auf Online-Händlerseiten).
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die PIN und der Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifzierungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung zum Beispiel eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung einer neuen TAN-Liste nicht mehr als eine TAN verwenden.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (zum Beispiel Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.

Bank-Verlag Medien GmbH 47.000 (11/09)

7.3 Sicherheit des Kundensystems

Der Teilnehmer muss die Sicherheitshinweise auf der Internetseite der Bank zum Online-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem Online-Banking-Auftrag (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapier-Kennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (zum Beispiel Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspfichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl des Authentifzierungsinstruments, die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifzierungsinstruments oder seines Persönlichen Sicherheitsmerkmals

fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten 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 seinem Authentifzierungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder
- das Authentifzierungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet,

muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Konto-/Depotinhaber hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1
- den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifzierungsinstrument.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Online-Banking-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifzierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifzierungsinstruments besteht.

(2) Die Bank wird den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal beziehungsweise das Authentifzierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber unverzüglich.

9.4 Automatische Sperre eines chip-basierten Authentifzierungsinstruments

(1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur falsch eingegeben wird.

(2) Ein TAN-Generator, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.

(3) Die in Absätzen 1 und 2 genannten Authentifzierungsinstrumente können dann nicht mehr für das Online-Banking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

10. Haftung

10.1 Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung

Die Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung seines Authentifzierungsinstruments

10.2.1 Haftung des Kontoinhabers 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 Authentifzierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,– Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigen Abhandenkommen des Authentifzierungsinstruments ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifzierungsinstruments, ohne dass dieses verlorengegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,– Euro, wenn der Teilnehmer seine Pficht zur sicheren Aufbewahrung der Personalisierten Sicherheitsmerkmale 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 Sorgfaltspfichten nach diesen Bedingungen verstoßen hat.

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpfichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(5) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspfichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem UmfangGrobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er
- den Verlust oder Diebstahl des Authentifzierungsinstruments oder die missbräuchliche Nutzung des Authentifzierungsinstruments oder des Personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1 Absatz 1),
- das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2 Absatz 2 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1 2. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2 4. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifzierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 5. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2 6. Spiegelstrich),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Online-Banking nutzt (siehe Nummer 7.2 Absatz 2 7. Spiegelstrich).

(6) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

10.2.2 Haftung des Depotinhabers bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifzierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifzierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften der Depotinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung der Bank ab der Sperranzeige

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

10.2.4 Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

Bankhaus Gebr. Martin AG
Schlossplatz 7, 73033 Göppingen
Tel.Nr. 07161 / 6714-0; Fax Nr. 07161/979710
E-Mail: info@martinbank.de
www.martinbank.de

Nähere Angaben zur Bank sind im „Preis- und Leistungsverzeichnis“ enthalten.

Bedingungen für Datenfernübertragung

1 Leistungsumfang

(1)Die Bank steht ihrem Kunden (Kontoinhaber), der kein Verbraucher ist, 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)Die Bank gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen der Datenfernübertragung nutzen kann. Zur Nutzung der Datenfernübertragung gelten die mit der Bank vereinbarten Verfügungslimite.
(3)Die Datenfernübertragung ist über die OnlineBanking-Anbindung möglich.
(4)Der Satz- und Dateiaufbau für die Übermittlung von Aufträgen und den Informationsabruf wird in der Spezifikation der Datenformate beschrieben.

2 Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien

(1)Aufträge können über die OnlineBanking-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, von der Bank freigeschaltete Legitimationsmedien.
Per DFÜ übermittelte Auftragsdaten müssen mit Transaktionsnummern autorisiert werden.
(2)Legitimations- und Sicherungsmedien sind Authentifizierungsinstrumente im Sinne von §1 Absatz 5 Zahlungsdiensteaufsichtsgesetz.

3 Verfahrensbestimmungen

(1)Für das zwischen Kunde und Bank vereinbarte Übertragungsverfahren gelten die im OnlineBanking-Vertrag beschriebenen Anforderungen sowie die Bedingungen für das OnlineBanking. Der Kunde ist verpflichtet, ab dem 1. Februar 2014 Überweisungsaufträge und Lastschrifteinzugsaufträge für Zahlungen in Euro innerhalb des Europäischen Wirtschaftsraums nur noch im Format ISO 20022 gemäß einzureichen. Lastschrifteinzugsaufträge für Zahlungen, die an einer Verkaufsstelle mit Hilfe einer Zahlungskarte generiert wurden und zu einer Lastschrift von einem inländischen Zahlungskonto führen (§ 7c Absatz 1 Zahlungsdiensteaufsichtsgesetz), sind erst ab dem 1. Februar 2016 verpflichtend im Format ISO 20022 einzureichen.
(2)Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer das DFÜ-Verfahren und die Spezifikationen beachten.
(3)Die Belegung der Datenfelder richtet sich nach den Belegungs- und Kontrollrichtlinien des jeweils genutzten Formates.
(4) Der Nutzer hat den Kontoidentifikationscode (Kontonummer oder IBAN) des Zahlungsempfängers beziehungsweise des Zahlers und – soweit diese Angabe erforderlich ist – den Zahlungsdienstleister-Identifikationscode (Bankleitzahl oder BIC) des Zahlungsdienstleisters des Zahlungsempfängers beziehungsweise des Zahlungsdienstleisters des Zahlers (Zahlstelle) zutreffend anzugeben. Die in die Abwicklung des Zahlungsauftrages 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 zu Lasten des Kunden.
(5) Vor Übertragung von Auftragsdaten an die Bank 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 30 Kalendertagen ab dem Ausführungstag 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.
(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.
(7) Die per DFÜ eingelieferten Auftragsdaten sind wie mit der Bank vereinbart mit Elektronischer Unterschrift (TAN) 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

4 Verhaltens- und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags

(1) Der Kunde ist in Abhängigkeit von dem mit der Bank vereinbarten Übertragungsverfahren verpflichtet sicherzustellen, dass alle Nutzer die Legitimationsverfahren einhalten.
(2) Mit Hilfe der von der Bank 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 Passwort 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 den Nutzer legitimierenden Daten dürfen nicht außerhalb des Legitimationsmediums, z. B. auf der Festplatte des Rechners, gespeichert werden;

– 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.

5 Verhaltens- und Sorgfaltspflichten im Umgang mit den Sicherungsmedien für den Datenaustausch

Der Kunde ist im Rahmen der Online Banking-Anbindung verpflichtet sicherzustellen, dass alle Teilnehmer die Anlage beschriebenen Sicherungsverfahren einhalten. Mit Hilfe der von der Bank 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.

6 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 bei der Bank zu sperren oder sperren zu lassen.
Der Teilnehmer kann der Bank eine Sperranzeige Jederzeit auch über die gesondert mitgeteilten Kontaktdatenaufgeben.
(2) Der Kunde kann außerhalb des DFÜ-Verfahrens die Verwendung der Legitimations-
und Sicherungsmedien eines Teilnehmers oder den gesamten DFÜ-Zugang über die von der Bank bekannt gegebene Sperrfazilität sperren lassen.
(3) Die Bank wird den gesamten DFÜ-Zugang sperren, wenn der Verdacht einer missbräuchlichen Nutzung des DFÜ-Zugangs besteht. Die Bank wird den Kunden hierüber außerhalb des DFÜ-Verfahrens informieren. Diese Sperre kann mittels DFÜ nicht aufgehoben werden.

7 Behandlung eingehender Auftragsdaten durch die Bank

(1) Die der Bank per DFÜ-Verfahren übermittelten Auftragsdaten werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet.
(2) Die Bank prüft anhand der von den Teilnehmern mittels Der Sicherungsmedien erstellten Signaturen, ob der Absender berechtigt ist, den Datenaustausch durchzuführen. Ergibt die Prüfung Unstimmigkeiten, wird die Bank die betreffenden Auftragsdaten nicht verarbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen.
(3) Die Bank prüft die Legitimation des Nutzers beziehungsweise der Nutzer und die Autorisierung der per DFÜ übermittelten Auftragsdaten anhand der von den Nutzern mittels der Legitimationsmedien erstellten elektronischen Unterschriften.
Die Bank ist berechtigt, nicht vollständig autorisierte Auftragsdaten nach Ablauf des von der Bank gesondert mitgeteilten Zeitlimits zu löschen.
(4) Ergeben sich bei den von der Bank durchgeführten Prüfungen der Dateien oder Datensätze Fehler, so wird die Bank die fehlerhaften Dateien oder Datensätze in geeigneter Form nachweisen und sie dem Nutzer unverzüglich mitteilen. Die Bank ist berechtigt, die fehlerhaften Dateien oder Datensätze von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrages nicht sichergestellt werden kann.

8 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. Die Bank kann einen Rückruf nur beachten, wenn ihr dieser so rechtzeitig zugeht, dass seine Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufes möglich ist.
(2) Die Widerrufbarkeit eines Auftrags richtet sich nach den dafür geltenden Sonderbedingungen
(z. B. Bedingungen für den Überweisungsverkehr).
Der Widerruf von Aufträgen kann nur außerhalb des DFÜ-Verfahrens erfolgen. Hierzu hat der Kunde der Bank die Einzelangaben des Originalauftrages mitzuteilen.

9 Ausführung der Aufträge

(1) Die Bank wird die Aufträge ausführen, wenn alle nachfolgenden Ausführungsbedingungen vorliegen:
– Die per DFÜ eingelieferten Auftragsdaten wurden gemäß Nummer 3 Absatz 7 autorisiert.
– Das festgelegte Datenformat ist eingehalten.
– Das Verfügungslimit ist nicht überschritten.
– Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.
(2) Liegen die Ausführungsbedingungen nach Absatz 1 nicht vor, wird die Bank den Auftrag nicht ausführen und den Kunden über die Nichtausführung unverzüglich auf dem vereinbarten Weg unterrichten.
Soweit möglich, nennt die Bank dem Kunden die Gründe und Fehler, die zur Nichtausführung geführt haben, und Möglichkeiten, wie diese Fehler berichtigt werden können.

10 Sicherheit des Kundensystems

Der Kunde hat für einen ausreichenden Schutz der von ihm für die Datenfernübertragung eingesetzten Systeme Sorge zu tragen. Die für das Online-Banking-Verfahren geltenden Sicherheitsanforderungen sind in den Bedingungen für das Online-Banking beschrieben.

11 Haftung

11.1 Haftung der Bank bei einer nicht autorisierten DFÜ-Verfügung und einer nicht oder fehlerhaft ausgeführten DFÜ-Verfügung

Die Haftung der Bank bei einer nicht autorisierten DFÜ-Verfügung und einer nicht oder fehlerhaft ausgeführten DFÜ-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen
(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 der Bank 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 t
(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 der Bank 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) Für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150,– Euro nach Absätzen 1 und 2 hinaus haftet der Kunde, abweichend von § 675v BGB, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine vertraglichen Verhaltens- und Sorgfaltspflichten verstoßen h
(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 die Bank 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 der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

11.2.3 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie 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.

12 Schlussbestimmungen

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