

# Vereinbarung über die Nutzung des Online-Banking – PIN/TAN-Verfahren; Telefon

Zur bankinternen Bearbeitung

Nr.

Konto-/Depotinhaber (Name, Anschrift, Telefon, E-Mail-Adresse)

Bank

Der/Die Konto-/Depotinhaber trifft/treffen als Inhaber der unter Nummer 1 genannten Konten mit der Bank für die elektronische Datenübermittlung im Wege des Online-Banking-Dialogs – mittels  PIN-/TAN-Verfahren  Telefon (nachfolgend „Online-Banking“) – folgende Teilnahmevereinbarung:

## 1 Vertragsgegenstand

Der/Die Konto-/Depotinhaber sowie etwaige unter Nummer 2 genannte Bevollmächtigte (im Folgenden einheitlich „Nutzer“ genannt) sind zur Inanspruchnahme des Online-Banking-Dialogs in dem von der Bank angebotenen Umfang berechtigt.

Der/Die Konto-/Depotinhaber nutzt/nutzen das Online-Banking-Angebot der Bank nicht selbst, ist/sind aber mit der Nutzung durch den/die unter Nummer 2 genannten Bevollmächtigten zu den gemäß Nummer 9 einbezogenen Bedingungen einverstanden.

Die Nutzung des Online-Banking bezieht sich auf folgende Konten/Depots:

Konto-Nummer/Depot-Nummer

## 2 Bevollmächtigte

Die nachstehend aufgeführten über die oben genannten Konten/Depots Bevollmächtigten

Name, Vorname des/der Bevollmächtigten

dürfen den Online-Banking-Dialog im folgenden Umfang nutzen:

uneingeschränkt alle von der Bank angebotenen Online-Banking-Leistungen

nur die Konto-/Depotabfrage<sup>1</sup>

<sup>2</sup>

Es gelten die vereinbarten Zeichnungsberechtigungen.

## 3 Höchstbeträge

Verfügungen über Online-Banking sind je Kalendertag begrenzt auf:

Geschäftsvorfall (z. B. Überweisung)	Konto-Nr.	EUR

Der Verfügungshöchstbetrag gilt nicht für Überweisungen und Lastschriften zugunsten und zulasten anderer Konten des Kontoinhabers bei der Bank.

Sonstige Aufträge dürfen den Höchstbetrag von EUR  je Auftrag (Transaktion) nicht überschreiten.

## 4 Sicherheitsmedien

Die Online-PIN, die für Online-Banking ausgehändigten Transaktionsnummern (TAN) und die Telefon-PIN sind zur Vermeidung von Missbrauch geheim zu halten. Der Nutzer ist aus Sicherheitsgründen verpflichtet, die ihm ausgehändigte persönliche Geheimzahl (Online-PIN) für den Online-Banking-Zugang sofort zu ändern. Einzelheiten zur Änderung der Online-PIN regelt die Verfahrensanleitung.

## 5 Schutz vor Missbrauch/Zugangskanäle

Verwendet der Nutzer ein Telefon mit Nummernspeicher und Wahlwiederholungsfunktion, ist er verpflichtet, nach Beendigung des Telefonats mit der Bank den Speicherinhalt zu überspielen (z. B. durch Eingabe einer beliebigen Nummer über die Tastatur). Dadurch wird verhindert, dass ein Dritter durch Nutzung der Wahlwiederholungsfunktion Kenntnis von der zuvor eingegebenen Kontonummer und PIN bzw. missbräuchlich Zugang zum Online-Banking erhält. Der Nutzer ist verpflichtet, die technische Verbindung zum VR-NetWorld-Angebot der Bank nur über folgende Zugangskanäle herzustellen:

Internet-Adresse

T-Online-Gateway-Seite

Telefon-Nr.

Eventuelle Änderungen gibt die Bank dem Nutzer bekannt.

## 6 Telefonaufzeichnung

Der Nutzer ist damit einverstanden, dass die Bank die mit ihm im Rahmen des Online-Banking-Dialogs geführten Telefonate sowie die von ihm über die Tastatur des Telefons eingegebenen Ziffern aufzeichnet und aufbewahrt. Dies ist zur ordnungsgemäßen Auftragsbearbeitung und aus Beweisgründen erforderlich.

## 7 Sperrnachricht

Die Sperrnachricht nach Nr. 12 „Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN“ kann der Nutzer unter (Telefonnummer)  mitteilen.

## 8 Hinweis nach § 4 Abs. 1 TDDSG (Teledienstdatenschutzgesetz)

Alle im Rahmen des Online-Banking anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und gegebenenfalls dem von ihr beauftragten Rechenzentrum innerhalb Deutschlands bzw. der Europäischen Union verarbeitet.

## 9 Einbeziehung der Online-Banking-Bedingungen

Ergänzend gelten die **Allgemeinen Geschäftsbedingungen** sowie für die Teilnahme am Online-Banking die „**Sonderbedingungen** für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN“. Der Wortlaut dieser Geschäftsbedingungen kann in den Geschäftsräumen der Bank eingesehen werden; auf Verlangen werden diese Geschäftsbedingungen ausgehändigt.

Ort, Datum	Ort, Datum	Ort, Datum
Konto-/Depotinhaber	Bevollmächtigte(r)	Bank

<sup>1</sup> Zum Beispiel Buchhalter, die nicht selbst verfügen sollen.

<sup>2</sup> Individuelle Auswahl einzelner Homebanking-Leistungen.

# Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN

Stand: Mai 2004

## 1 Leistungsangebot

Der Konto-/Depotinhaber kann Bankgeschäfte mittels Online-Banking in dem vom Kreditinstitut angebotenen Umfang abwickeln. Sofern das Kreditinstitut für Verfügungen mittels Online-Banking eine Betragsbegrenzung im System vorsieht, informiert es ihn hierüber.

## 2 Nutzungsberechtigte und Zugangsmedien

Zur Abwicklung von Bankgeschäften mittels Online-Banking unter Verwendung von PIN und TAN benötigt der Konto-/Depotinhaber und etwaige Bevollmächtigte jeweils eine persönliche Identifikationsnummer (PIN) sowie gegebenenfalls Transaktionsnummern (TAN) aus

- einer TAN-Liste oder
- einem TAN-Generator.

Ein TAN-Generator ist Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN. Aus der Chipkarte können jeweils einmal verwendbare TAN mithilfe eines Lesegeräts ausgelesen werden. Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden als Nutzer bezeichnet.

## 3 Verfahren

(1) Der Nutzer hat mittels Online-Banking Zugang zum Konto/Depot, wenn er zuvor die Konto-/Depotnummer/seine individuelle Kundenkennung<sup>1</sup> sowie seine PIN eingegeben hat.

(2) In den vom Kreditinstitut im Einzelnen angegebenen Fällen hat der Nutzer jeweils zusätzlich eine TAN einzugeben. Zur Erläuterung der Nutzungsmöglichkeiten stellt das Kreditinstitut eine Verfahrensanleitung zur Verfügung, die die Besonderheiten der vereinbarten Online-Anwendungen beschreibt.

(3) Der Nutzer ist verpflichtet, die technische Verbindung zum Online-Banking-Angebot des Kreditinstituts nur über die vom Kreditinstitut gesondert mitgeteilten Online-Banking-Zugangskanäle herzustellen.

## 4 Nachrichtenfregabe/Verwendung der TAN

Erklärungen jeder Art (z. B. Kontostandsabfragen oder Überweisungen) sind abgegeben, wenn sie abschließend zur Übermittlung an das Kreditinstitut freigegeben sind. Bei Vorgängen, die zusätzlich der Eingabe einer TAN bedürfen (z. B. Überweisungen), ist die Freigabe der TAN maßgebend.

Eine TAN kann nicht mehr verwendet werden, sobald sie zur Übermittlung an das Institut freigegeben worden ist.

## 5 Bearbeitung von Aufträgen im Online-Banking

Mittels Online-Banking erteilte Aufträge werden im Rahmen des ordnungsgemäßen Arbeitsablaufs bearbeitet.

## 6 Finanzielle Nutzungsgrenze

Der Nutzer darf Verfügungen nur im Rahmen des Kontoguthabens oder eines vorher für das Konto eingeräumten Kredits vornehmen. Auch wenn der Nutzer diese Nutzungsgrenze bei seinen Verfügungen nicht einhält, ist das Kreditinstitut berechtigt, den Ersatz der Aufwendungen zu verlangen, die aus der Nutzung des Online-Banking entstehen. Die Buchung solcher Verfügungen auf dem Konto führt lediglich zu einer geduldeten Kontoüberziehung; das Kreditinstitut ist berechtigt, in diesem Fall den höheren Zinssatz für geduldete Kontoüberziehungen zu verlangen.

## 7 Geheimhaltung der PIN und der TAN

Der Nutzer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN und den TAN erlangt. Jede Person, die die PIN und – falls erforderlich – eine TAN kennt, hat die Möglichkeit, das Online-Banking-Leistungsangebot zu nutzen. Sie kann z. B. Aufträge zulasten des Kontos/Depots erteilen. Insbesondere Folgendes ist zur Geheimhaltung der PIN und TAN zu beachten:

- PIN und TAN dürfen nicht elektronisch gespeichert oder in anderer Form notiert werden;
- die dem Nutzer zur Verfügung gestellte TAN-Liste bzw. der dem Nutzer zur Verfügung gestellte TAN-Generator ist sicher zu verwahren;
- bei Eingabe der PIN und TAN ist sicherzustellen, dass Dritte diese nicht ausspähen können.

## 8 Maßnahmen bei Bekanntwerden von PIN oder TAN aus einer TAN-Liste oder Verdacht ihrer missbräuchlichen Nutzung

Stellt der Nutzer fest, dass eine andere Person

- von seiner PIN oder
- von einer TAN aus seiner TAN-Liste

Kenntnis erhalten hat oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so ist der Nutzer verpflichtet, unverzüglich seine PIN zu ändern bzw. die noch nicht aus der TAN-Liste verbrauchten TAN zu sperren. Sofern ihm dies nicht möglich ist, hat er das Kreditinstitut unverzüglich zu unterrichten. In diesem Fall wird das Kreditinstitut den Online-Banking-Zugang zum Konto/Depot sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht des Nutzers für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

## 9 Maßnahmen bei Verlust des TAN-Generators

Stellt der Nutzer den Verlust seines TAN-Generators fest oder besteht der Verdacht seiner missbräuchlichen Nutzung, so ist der Nutzer zu Folgendem verpflichtet:

- Befindet sich der TAN-Generator auf einer Chipkarte mit Zahlungsfunktionen (z. B. VR-BankCard), hat er das Kreditinstitut, und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. Den Verlust der Karte kann der Karteninhaber auch gegenüber dem Zentralen Sperrannahmedienst (Telefon 01805/021 021) anzeigen. In diesem Fall ist eine Kartensperre nur möglich, wenn der Name des Kreditinstituts – möglichst mit Bankleitzahl – und die Kontonummer angegeben werden. Der Zentrale Sperrannahmedienst sperrt alle für die betreffenden Konten ausgegebenen Karten sowie gegebenenfalls den Zugriff auf zusätzlich definierte Konten, auf die der Karteninhaber Zugriff hat, für die weitere Nutzung an Geldautomaten, an automatisierten Kassen sowie den TAN-Generator. Zur Beschränkung der Sperre auf die abhandlungsgemachte Karte muss sich der Karteninhaber mit seinem Kreditinstitut, möglichst mit der kontoführenden Stelle, in Verbindung setzen. Wird die Karte gestohlen oder missbräuchlich verwendet, ist unverzüglich Anzeige bei der Polizei zu erstatten.

Sobald dem Kreditinstitut oder dem Zentralen Sperrannahmedienst der Verlust der Karte angezeigt worden ist, trägt das Kreditinstitut die danach durch missbräuchliche Nutzung des Online-Banking entstandenen Schäden.

- Befindet sich der TAN-Generator auf einer Chipkarte ohne Zahlungsfunktion oder auf einem anderen elektronischen Gerät, so ist der Nutzer verpflichtet, sein Kreditinstitut, und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. In diesem Fall wird das Kreditinstitut den TAN-Generator sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht des Nutzers für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

## 10 Änderung der PIN

Der Nutzer ist berechtigt, seine PIN unter Verwendung einer TAN jederzeit zu ändern. Bei Änderung der PIN wird seine bisherige PIN ungültig.

## 11 Sperre des Online-Banking-Angebotes durch das Kreditinstitut

(1) Wird dreimal hintereinander eine falsche PIN eingegeben, so sperrt das Kreditinstitut den Online-Banking-Zugang zum Konto/Depot. Der Nutzer kann diese Sperre aufheben, indem er neben der richtigen PIN eine gültige TAN eingibt.

(2) Werden dreimal hintereinander falsche TAN eingegeben, so werden alle noch nicht verbrauchten TAN bzw. der TAN-Generator für das betreffende Konto/Depot gesperrt. Im Falle der vollständigen Sperrung der unverbrauchten TAN in der TAN-Liste oder des TAN-Generators sollte sich der Nutzer mit dem Kreditinstitut in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

(3) Das Kreditinstitut wird den Online-Banking-Zugang zum Konto/Depot sperren, wenn der Verdacht einer missbräuchlichen Nutzung des Kontos/Depots über den Online-Banking-Zugang besteht. Es wird den Konto-inhaber hierüber außerhalb des Online-Banking informieren. Diese Sperre kann mittels Online-Banking nicht aufgehoben werden.

## 12 Sperre des Online-Banking-Angebotes auf Wunsch des Konto-inhabers

Das Kreditinstitut wird den Online-Banking-Zugang zum Konto/Depot auf Wunsch des Kontoinhabers sperren. Diese Sperre kann nicht mittels Online-Banking aufgehoben werden.

## 13 Einzug der Chipkarte mit Zahlungsfunktion und TAN-Generator

Das Kreditinstitut darf den Einzug der Chipkarte mit Zahlungsfunktion und TAN-Generator (z. B. am Geldausgabeautomaten) veranlassen, wenn es berechtigt ist, den Kartenvertrag aus wichtigem Grund zu kündigen. Das Kreditinstitut ist zur Einziehung der Karte auch berechtigt, wenn die Nutzungsberechtigung der Karte durch Gültigkeitsablauf oder durch ordentliche Kündigung endet. Der Einzug der Karte hat zur Folge, dass der Nutzer den TAN-Generator auf der Karte für das Online-Banking nicht mehr nutzen kann.

## 14 Rückruf oder Änderung von Aufträgen

Der Rückruf oder die Änderung von Aufträgen kann nur außerhalb des Online-Banking-Verfahrens erfolgen, es sei denn, das Kreditinstitut sieht eine solche Möglichkeit innerhalb des Verfahrens ausdrücklich vor. Das Kreditinstitut kann einen Rückruf oder eine Änderung allerdings nur beachten, wenn ihm diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufs möglich ist.

## 15 Anwendbares Recht

Auf die Geschäftsbeziehung zwischen dem Konto-/Depotinhaber und dem Kreditinstitut findet deutsches Recht Anwendung, es sei denn, dieses verweist auf eine ausländische Rechtsordnung.

# Vereinbarung über die Nutzung des Online-Banking – PIN/TAN-Verfahren; Telefon

Zur bankinternen Bearbeitung

Nr.

Konto-/Depotinhaber (Name, Anschrift, Telefon, E-Mail-Adresse)

Bank

Der/Die Konto-/Depotinhaber trifft/treffen als Inhaber der unter Nummer 1 genannten Konten mit der Bank für die elektronische Datenübermittlung im Wege des Online-Banking-Dialogs – mittels  PIN-/TAN-Verfahren  Telefon (nachfolgend „Online-Banking“) – folgende Teilnahmevereinbarung:

## 1 Vertragsgegenstand

Der/Die Konto-/Depotinhaber sowie etwaige unter Nummer 2 genannte Bevollmächtigte (im Folgenden einheitlich „Nutzer“ genannt) sind zur Inanspruchnahme des Online-Banking-Dialogs in dem von der Bank angebotenen Umfang berechtigt.

Der/Die Konto-/Depotinhaber nutzt/nutzen das Online-Banking-Angebot der Bank nicht selbst, ist/sind aber mit der Nutzung durch den/die unter Nummer 2 genannten Bevollmächtigten zu den gemäß Nummer 9 einbezogenen Bedingungen einverstanden.

Die Nutzung des Online-Banking bezieht sich auf folgende Konten/Depots:

Konto-Nummer/Depot-Nummer

## 2 Bevollmächtigte

Die nachstehend aufgeführten über die oben genannten Konten/Depots Bevollmächtigten

Name, Vorname des/der Bevollmächtigten

dürfen den Online-Banking-Dialog im folgenden Umfang nutzen:

uneingeschränkt alle von der Bank angebotenen Online-Banking-Leistungen

nur die Konto-/Depotabfrage<sup>1</sup>

<sup>2</sup>

Es gelten die vereinbarten Zeichnungsberechtigungen.

## 3 Höchstbeträge

Verfügungen über Online-Banking sind je Kalendertag begrenzt auf:

Geschäftsvorfall (z. B. Überweisung)	Konto-Nr.	EUR

Der Verfügungshöchstbetrag gilt nicht für Überweisungen und Lastschriften zugunsten und zulasten anderer Konten des Kontoinhabers bei der Bank.

Sonstige Aufträge dürfen den Höchstbetrag von EUR  je Auftrag (Transaktion) nicht überschreiten.

## 4 Sicherheitsmedien

Die Online-PIN, die für Online-Banking ausgehändigten Transaktionsnummern (TAN) und die Telefon-PIN sind zur Vermeidung von Missbrauch geheim zu halten. Der Nutzer ist aus Sicherheitsgründen verpflichtet, die ihm ausgehändigte persönliche Geheimzahl (Online-PIN) für den Online-Banking-Zugang sofort zu ändern. Einzelheiten zur Änderung der Online-PIN regelt die Verfahrensanleitung.

## 5 Schutz vor Missbrauch/Zugangskanäle

Verwendet der Nutzer ein Telefon mit Nummernspeicher und Wahlwiederholungsfunktion, ist er verpflichtet, nach Beendigung des Telefonats mit der Bank den Speicherinhalt zu überspielen (z. B. durch Eingabe einer beliebigen Nummer über die Tastatur). Dadurch wird verhindert, dass ein Dritter durch Nutzung der Wahlwiederholungsfunktion Kenntnis von der zuvor eingegebenen Kontonummer und PIN bzw. missbräuchlich Zugang zum Online-Banking erhält. Der Nutzer ist verpflichtet, die technische Verbindung zum VR-NetWorld-Angebot der Bank nur über folgende Zugangskanäle herzustellen:

Internet-Adresse

T-Online-Gateway-Seite

Telefon-Nr.

Eventuelle Änderungen gibt die Bank dem Nutzer bekannt.

## 6 Telefonaufzeichnung

Der Nutzer ist damit einverstanden, dass die Bank die mit ihm im Rahmen des Online-Banking-Dialogs geführten Telefonate sowie die von ihm über die Tastatur des Telefons eingegebenen Ziffern aufzeichnet und aufbewahrt. Dies ist zur ordnungsgemäßen Auftragsbearbeitung und aus Beweisgründen erforderlich.

## 7 Sperrnachricht

Die Sperrnachricht nach Nr. 12 „Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN“ kann der Nutzer unter (Telefonnummer)  mitteilen.

## 8 Hinweis nach § 4 Abs. 1 TDDSG (Teledienstdatenschutzgesetz)

Alle im Rahmen des Online-Banking anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und gegebenenfalls dem von ihr beauftragten Rechenzentrum innerhalb Deutschlands bzw. der Europäischen Union verarbeitet.

## 9 Einbeziehung der Online-Banking-Bedingungen

Ergänzend gelten die **Allgemeinen Geschäftsbedingungen** sowie für die Teilnahme am Online-Banking die „**Sonderbedingungen** für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN“. Der Wortlaut dieser Geschäftsbedingungen kann in den Geschäftsräumen der Bank eingesehen werden; auf Verlangen werden diese Geschäftsbedingungen ausgehändigt.

Ort, Datum	Ort, Datum	Ort, Datum
Konto-/Depotinhaber	Bevollmächtigte(r)	Bank

<sup>1</sup> Zum Beispiel Buchhalter, die nicht selbst verfügen sollen.

<sup>2</sup> Individuelle Auswahl einzelner Homebanking-Leistungen.

# Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN

Stand: Mai 2004

## 1 Leistungsangebot

Der Konto-/Depotinhaber kann Bankgeschäfte mittels Online-Banking in dem vom Kreditinstitut angebotenen Umfang abwickeln. Sofern das Kreditinstitut für Verfügungen mittels Online-Banking eine Betragsbegrenzung im System vorsieht, informiert es ihn hierüber.

## 2 Nutzungsberechtigte und Zugangsmedien

Zur Abwicklung von Bankgeschäften mittels Online-Banking unter Verwendung von PIN und TAN benötigt der Konto-/Depotinhaber und etwaige Bevollmächtigte jeweils eine persönliche Identifikationsnummer (PIN) sowie gegebenenfalls Transaktionsnummern (TAN) aus

- einer TAN-Liste oder
- einem TAN-Generator.

Ein TAN-Generator ist Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN. Aus der Chipkarte können jeweils einmal verwendbare TAN mithilfe eines Lesegeräts ausgelesen werden. Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden als Nutzer bezeichnet.

## 3 Verfahren

(1) Der Nutzer hat mittels Online-Banking Zugang zum Konto/Depot, wenn er zuvor die Konto-/Depotnummer/seine individuelle Kundenkennung<sup>1</sup> sowie seine PIN eingegeben hat.

(2) In den vom Kreditinstitut im Einzelnen angegebenen Fällen hat der Nutzer jeweils zusätzlich eine TAN einzugeben. Zur Erläuterung der Nutzungsmöglichkeiten stellt das Kreditinstitut eine Verfahrensanleitung zur Verfügung, die die Besonderheiten der vereinbarten Online-Anwendungen beschreibt.

(3) Der Nutzer ist verpflichtet, die technische Verbindung zum Online-Banking-Angebot des Kreditinstituts nur über die vom Kreditinstitut besonders mitgeteilten Online-Banking-Zugangskanäle herzustellen.

## 4 Nachrichtenfreigabe/Verwendung der TAN

Erklärungen jeder Art (z. B. Kontostandsabfragen oder Überweisungen) sind abgegeben, wenn sie abschließend zur Übermittlung an das Kreditinstitut freigegeben sind. Bei Vorgängen, die zusätzlich der Eingabe einer TAN bedürfen (z. B. Überweisungen), ist die Freigabe der TAN maßgebend.

Eine TAN kann nicht mehr verwendet werden, sobald sie zur Übermittlung an das Institut freigegeben worden ist.

## 5 Bearbeitung von Aufträgen im Online-Banking

Mittels Online-Banking erteilte Aufträge werden im Rahmen des ordnungsgemäßen Arbeitsablaufs bearbeitet.

## 6 Finanzielle Nutzungsgrenze

Der Nutzer darf Verfügungen nur im Rahmen des Kontoguthabens oder eines vorher für das Konto eingeräumten Kredits vornehmen. Auch wenn der Nutzer diese Nutzungsgrenze bei seinen Verfügungen nicht einhält, ist das Kreditinstitut berechtigt, den Ersatz der Aufwendungen zu verlangen, die aus der Nutzung des Online-Banking entstehen. Die Buchung solcher Verfügungen auf dem Konto führt lediglich zu einer geduldeten Kontoüberziehung; das Kreditinstitut ist berechtigt, in diesem Fall den höheren Zinssatz für geduldete Kontoüberziehungen zu verlangen.

## 7 Geheimhaltung der PIN und der TAN

Der Nutzer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN und den TAN erlangt. Jede Person, die die PIN und – falls erforderlich – eine TAN kennt, hat die Möglichkeit, das Online-Banking-Leistungsangebot zu nutzen. Sie kann z. B. Aufträge zulasten des Kontos/Depots erteilen. Insbesondere Folgendes ist zur Geheimhaltung der PIN und TAN zu beachten:

- PIN und TAN dürfen nicht elektronisch gespeichert oder in anderer Form notiert werden;
- die dem Nutzer zur Verfügung gestellte TAN-Liste bzw. der dem Nutzer zur Verfügung gestellte TAN-Generator ist sicher zu verwahren;
- bei Eingabe der PIN und TAN ist sicherzustellen, dass Dritte diese nicht ausspähen können.

## 8 Maßnahmen bei Bekanntwerden von PIN oder TAN aus einer TAN-Liste oder Verdacht ihrer missbräuchlichen Nutzung

Stellt der Nutzer fest, dass eine andere Person

- von seiner PIN oder
- von einer TAN aus seiner TAN-Liste

Kenntnis erhalten hat oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so ist der Nutzer verpflichtet, unverzüglich seine PIN zu ändern bzw. die noch nicht aus der TAN-Liste verbrauchten TAN zu sperren. Sofern ihm dies nicht möglich ist, hat er das Kreditinstitut unverzüglich zu unterrichten. In diesem Fall wird das Kreditinstitut den Online-Banking-Zugang zum Konto/Depot sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht des Nutzers für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

## 9 Maßnahmen bei Verlust des TAN-Generators

Stellt der Nutzer den Verlust seines TAN-Generators fest oder besteht der Verdacht seiner missbräuchlichen Nutzung, so ist der Nutzer zu Folgendem verpflichtet:

- Befindet sich der TAN-Generator auf einer Chipkarte mit Zahlungsfunktionen (z. B. VR-BankCard), hat er das Kreditinstitut, und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. Den Verlust der Karte kann der Karteninhaber auch gegenüber dem Zentralen Sperrannahmedienst (Telefon 01805/021 021) anzeigen. In diesem Fall ist eine Kartensperre nur möglich, wenn der Name des Kreditinstituts – möglichst mit Bankleitzahl – und die Kontonummer angegeben werden. Der Zentrale Sperrannahmedienst sperrt alle für die betreffenden Konten ausgegebenen Karten sowie gegebenenfalls den Zugriff auf zusätzlich definierte Konten, auf die der Karteninhaber Zugriff hat, für die weitere Nutzung an Geldautomaten, an automatisierten Kassen sowie den TAN-Generator. Zur Beschränkung der Sperre auf die abhandlungsgemene Karte muss sich der Karteninhaber mit seinem Kreditinstitut, möglichst mit der kontoführenden Stelle, in Verbindung setzen. Wird die Karte gestohlen oder missbräuchlich verwendet, ist unverzüglich Anzeige bei der Polizei zu erstatten.

Sobald dem Kreditinstitut oder dem Zentralen Sperrannahmedienst der Verlust der Karte angezeigt worden ist, trägt das Kreditinstitut die danach durch missbräuchliche Nutzung des Online-Banking entstandenen Schäden.

- Befindet sich der TAN-Generator auf einer Chipkarte ohne Zahlungsfunktion oder auf einem anderen elektronischen Gerät, so ist der Nutzer verpflichtet, sein Kreditinstitut, und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. In diesem Fall wird das Kreditinstitut den TAN-Generator sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht des Nutzers für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

## 10 Änderung der PIN

Der Nutzer ist berechtigt, seine PIN unter Verwendung einer TAN jederzeit zu ändern. Bei Änderung der PIN wird seine bisherige PIN ungültig.

## 11 Sperre des Online-Banking-Angebotes durch das Kreditinstitut

(1) Wird dreimal hintereinander eine falsche PIN eingegeben, so sperrt das Kreditinstitut den Online-Banking-Zugang zum Konto/Depot. Der Nutzer kann diese Sperre aufheben, indem er neben der richtigen PIN eine gültige TAN eingibt.

(2) Werden dreimal hintereinander falsche TAN eingegeben, so werden alle noch nicht verbrauchten TAN bzw. der TAN-Generator für das betreffende Konto/Depot gesperrt. Im Falle der vollständigen Sperrung der unverbrauchten TAN in der TAN-Liste oder des TAN-Generators sollte sich der Nutzer mit dem Kreditinstitut in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

(3) Das Kreditinstitut wird den Online-Banking-Zugang zum Konto/Depot sperren, wenn der Verdacht einer missbräuchlichen Nutzung des Kontos/Depots über den Online-Banking-Zugang besteht. Es wird den Konto-inhaber hierüber außerhalb des Online-Banking informieren. Diese Sperre kann mittels Online-Banking nicht aufgehoben werden.

## 12 Sperre des Online-Banking-Angebotes auf Wunsch des Konto-inhabers

Das Kreditinstitut wird den Online-Banking-Zugang zum Konto/Depot auf Wunsch des Kontoinhabers sperren. Diese Sperre kann nicht mittels Online-Banking aufgehoben werden.

## 13 Einzug der Chipkarte mit Zahlungsfunktion und TAN-Generator

Das Kreditinstitut darf den Einzug der Chipkarte mit Zahlungsfunktion und TAN-Generator (z. B. am Geldausgabeautomaten) veranlassen, wenn es berechtigt ist, den Kartenvertrag aus wichtigem Grund zu kündigen. Das Kreditinstitut ist zur Einziehung der Karte auch berechtigt, wenn die Nutzungsberechtigung der Karte durch Gültigkeitsablauf oder durch ordentliche Kündigung endet. Der Einzug der Karte hat zur Folge, dass der Nutzer den TAN-Generator auf der Karte für das Online-Banking nicht mehr nutzen kann.

## 14 Rückruf oder Änderung von Aufträgen

Der Rückruf oder die Änderung von Aufträgen kann nur außerhalb des Online-Banking-Verfahrens erfolgen, es sei denn, das Kreditinstitut sieht eine solche Möglichkeit innerhalb des Verfahrens ausdrücklich vor. Das Kreditinstitut kann einen Rückruf oder eine Änderung allerdings nur beachten, wenn ihm diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufs möglich ist.

## 15 Anwendbares Recht

Auf die Geschäftsbeziehung zwischen dem Konto-/Depotinhaber und dem Kreditinstitut findet deutsches Recht Anwendung, es sei denn, dieses verweist auf eine ausländische Rechtsordnung.

# Vereinbarung über die Nutzung des Online-Banking – PIN/TAN-Verfahren; Telefon

Zur bankinternen Bearbeitung

Nr.

Konto-/Depotinhaber (Name, Anschrift, Telefon, E-Mail-Adresse)

Bank

Der/Die Konto-/Depotinhaber trifft/treffen als Inhaber der unter Nummer 1 genannten Konten mit der Bank für die elektronische Datenübermittlung im Wege des Online-Banking-Dialogs – mittels  PIN-/TAN-Verfahren  Telefon (nachfolgend „Online-Banking“) – folgende Teilnahmevereinbarung:

## 1 Vertragsgegenstand

Der/Die Konto-/Depotinhaber sowie etwaige unter Nummer 2 genannte Bevollmächtigte (im Folgenden einheitlich „Nutzer“ genannt) sind zur Inanspruchnahme des Online-Banking-Dialogs in dem von der Bank angebotenen Umfang berechtigt.

Der/Die Konto-/Depotinhaber nutzt/nutzen das Online-Banking-Angebot der Bank nicht selbst, ist/sind aber mit der Nutzung durch den/die unter Nummer 2 genannten Bevollmächtigten zu den gemäß Nummer 9 einbezogenen Bedingungen einverstanden.

Die Nutzung des Online-Banking bezieht sich auf folgende Konten/Depots:

Konto-Nummer/Depot-Nummer

## 2 Bevollmächtigte

Die nachstehend aufgeführten über die oben genannten Konten/Depots Bevollmächtigten

Name, Vorname des/der Bevollmächtigten

dürfen den Online-Banking-Dialog im folgenden Umfang nutzen:

uneingeschränkt alle von der Bank angebotenen Online-Banking-Leistungen

nur die Konto-/Depotabfrage<sup>1</sup>

<sup>2</sup>

Es gelten die vereinbarten Zeichnungsberechtigungen.

## 3 Höchstbeträge

Verfügungen über Online-Banking sind je Kalendertag begrenzt auf:

Geschäftsvorfall (z. B. Überweisung)	Konto-Nr.	EUR

Der Verfügungshöchstbetrag gilt nicht für Überweisungen und Lastschriften zugunsten und zulasten anderer Konten des Kontoinhabers bei der Bank.

Sonstige Aufträge dürfen den Höchstbetrag von EUR  je Auftrag (Transaktion) nicht überschreiten.

## 4 Sicherheitsmedien

Die Online-PIN, die für Online-Banking ausgehändigten Transaktionsnummern (TAN) und die Telefon-PIN sind zur Vermeidung von Missbrauch geheim zu halten. Der Nutzer ist aus Sicherheitsgründen verpflichtet, die ihm ausgehändigte persönliche Geheimzahl (Online-PIN) für den Online-Banking-Zugang sofort zu ändern. Einzelheiten zur Änderung der Online-PIN regelt die Verfahrensanleitung.

## 5 Schutz vor Missbrauch/Zugangskanäle

Verwendet der Nutzer ein Telefon mit Nummernspeicher und Wahlwiederholungsfunktion, ist er verpflichtet, nach Beendigung des Telefonats mit der Bank den Speicherinhalt zu überspielen (z. B. durch Eingabe einer beliebigen Nummer über die Tastatur). Dadurch wird verhindert, dass ein Dritter durch Nutzung der Wahlwiederholungsfunktion Kenntnis von der zuvor eingegebenen Kontonummer und PIN bzw. missbräuchlich Zugang zum Online-Banking erhält. Der Nutzer ist verpflichtet, die technische Verbindung zum VR-NetWorld-Angebot der Bank nur über folgende Zugangskanäle herzustellen:

Internet-Adresse

T-Online-Gateway-Seite

Telefon-Nr.

Eventuelle Änderungen gibt die Bank dem Nutzer bekannt.

## 6 Telefonaufzeichnung

Der Nutzer ist damit einverstanden, dass die Bank die mit ihm im Rahmen des Online-Banking-Dialogs geführten Telefonate sowie die von ihm über die Tastatur des Telefons eingegebenen Ziffern aufzeichnet und aufbewahrt. Dies ist zur ordnungsgemäßen Auftragsbearbeitung und aus Beweisgründen erforderlich.

## 7 Sperrnachricht

Die Sperrnachricht nach Nr. 12 „Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN“ kann der Nutzer unter (Telefonnummer)  mitteilen.

## 8 Hinweis nach § 4 Abs. 1 TDDSG (Teledienstdatenschutzgesetz)

Alle im Rahmen des Online-Banking anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und gegebenenfalls dem von ihr beauftragten Rechenzentrum innerhalb Deutschlands bzw. der Europäischen Union verarbeitet.

## 9 Einbeziehung der Online-Banking-Bedingungen

Ergänzend gelten die **Allgemeinen Geschäftsbedingungen** sowie für die Teilnahme am Online-Banking die „**Sonderbedingungen** für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN“. Der Wortlaut dieser Geschäftsbedingungen kann in den Geschäftsräumen der Bank eingesehen werden; auf Verlangen werden diese Geschäftsbedingungen ausgehändigt.

Ort, Datum	Ort, Datum	Ort, Datum
Konto-/Depotinhaber	Bevollmächtigte(r)	Bank

<sup>1</sup> Zum Beispiel Buchhalter, die nicht selbst verfügen sollen.

<sup>2</sup> Individuelle Auswahl einzelner Homebanking-Leistungen.

# Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN

Stand: Mai 2004

## 1 Leistungsangebot

Der Konto-/Depotinhaber kann Bankgeschäfte mittels Online-Banking in dem vom Kreditinstitut angebotenen Umfang abwickeln. Sofern das Kreditinstitut für Verfügungen mittels Online-Banking eine Betragsbegrenzung im System vorsieht, informiert es ihn hierüber.

## 2 Nutzungsberechtigte und Zugangsmedien

Zur Abwicklung von Bankgeschäften mittels Online-Banking unter Verwendung von PIN und TAN benötigt der Konto-/Depotinhaber und etwaige Bevollmächtigte jeweils eine persönliche Identifikationsnummer (PIN) sowie gegebenenfalls Transaktionsnummern (TAN) aus

- einer TAN-Liste oder
- einem TAN-Generator.

Ein TAN-Generator ist Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN. Aus der Chipkarte können jeweils einmal verwendbare TAN mithilfe eines Lesegeräts ausgelesen werden. Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden als Nutzer bezeichnet.

## 3 Verfahren

(1) Der Nutzer hat mittels Online-Banking Zugang zum Konto/Depot, wenn er zuvor die Konto-/Depotnummer/seine individuelle Kundenkennung<sup>1</sup> sowie seine PIN eingegeben hat.

(2) In den vom Kreditinstitut im Einzelnen angegebenen Fällen hat der Nutzer jeweils zusätzlich eine TAN einzugeben. Zur Erläuterung der Nutzungsmöglichkeiten stellt das Kreditinstitut eine Verfahrensanleitung zur Verfügung, die die Besonderheiten der vereinbarten Online-Anwendungen beschreibt.

(3) Der Nutzer ist verpflichtet, die technische Verbindung zum Online-Banking-Angebot des Kreditinstituts nur über die vom Kreditinstitut besonders mitgeteilten Online-Banking-Zugangskanäle herzustellen.

## 4 Nachrichtenfregabe/Verwendung der TAN

Erklärungen jeder Art (z. B. Kontostandsabfragen oder Überweisungen) sind abgegeben, wenn sie abschließend zur Übermittlung an das Kreditinstitut freigegeben sind. Bei Vorgängen, die zusätzlich der Eingabe einer TAN bedürfen (z. B. Überweisungen), ist die Freigabe der TAN maßgebend.

Eine TAN kann nicht mehr verwendet werden, sobald sie zur Übermittlung an das Institut freigegeben worden ist.

## 5 Bearbeitung von Aufträgen im Online-Banking

Mittels Online-Banking erteilte Aufträge werden im Rahmen des ordnungsgemäßen Arbeitsablaufs bearbeitet.

## 6 Finanzielle Nutzungsgrenze

Der Nutzer darf Verfügungen nur im Rahmen des Kontoguthabens oder eines vorher für das Konto eingeräumten Kredits vornehmen. Auch wenn der Nutzer diese Nutzungsgrenze bei seinen Verfügungen nicht einhält, ist das Kreditinstitut berechtigt, den Ersatz der Aufwendungen zu verlangen, die aus der Nutzung des Online-Banking entstehen. Die Buchung solcher Verfügungen auf dem Konto führt lediglich zu einer geduldeten Kontoüberziehung; das Kreditinstitut ist berechtigt, in diesem Fall den höheren Zinssatz für geduldete Kontoüberziehungen zu verlangen.

## 7 Geheimhaltung der PIN und der TAN

Der Nutzer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN und den TAN erlangt. Jede Person, die die PIN und – falls erforderlich – eine TAN kennt, hat die Möglichkeit, das Online-Banking-Leistungsangebot zu nutzen. Sie kann z. B. Aufträge zulasten des Kontos/Depots erteilen. Insbesondere Folgendes ist zur Geheimhaltung der PIN und TAN zu beachten:

- PIN und TAN dürfen nicht elektronisch gespeichert oder in anderer Form notiert werden;
- die dem Nutzer zur Verfügung gestellte TAN-Liste bzw. der dem Nutzer zur Verfügung gestellte TAN-Generator ist sicher zu verwahren;
- bei Eingabe der PIN und TAN ist sicherzustellen, dass Dritte diese nicht ausspähen können.

## 8 Maßnahmen bei Bekanntwerden von PIN oder TAN aus einer TAN-Liste oder Verdacht ihrer missbräuchlichen Nutzung

Stellt der Nutzer fest, dass eine andere Person

- von seiner PIN oder
- von einer TAN aus seiner TAN-Liste

Kenntnis erhalten hat oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so ist der Nutzer verpflichtet, unverzüglich seine PIN zu ändern bzw. die noch nicht aus der TAN-Liste verbrauchten TAN zu sperren. Sofern ihm dies nicht möglich ist, hat er das Kreditinstitut unverzüglich zu unterrichten. In diesem Fall wird das Kreditinstitut den Online-Banking-Zugang zum Konto/Depot sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht des Nutzers für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

## 9 Maßnahmen bei Verlust des TAN-Generators

Stellt der Nutzer den Verlust seines TAN-Generators fest oder besteht der Verdacht seiner missbräuchlichen Nutzung, so ist der Nutzer zu Folgendem verpflichtet:

- Befindet sich der TAN-Generator auf einer Chipkarte mit Zahlungsfunktionen (z. B. VR-BankCard), hat er das Kreditinstitut, und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. Den Verlust der Karte kann der Karteninhaber auch gegenüber dem Zentralen Sperrannahmedienst (Telefon 01805/021 021) anzeigen. In diesem Fall ist eine Kartensperre nur möglich, wenn der Name des Kreditinstituts – möglichst mit Bankleitzahl – und die Kontonummer angegeben werden. Der Zentrale Sperrannahmedienst sperrt alle für die betreffenden Konten ausgegebenen Karten sowie gegebenenfalls den Zugriff auf zusätzlich definierte Konten, auf die der Karteninhaber Zugriff hat, für die weitere Nutzung an Geldautomaten, an automatisierten Kassen sowie den TAN-Generator. Zur Beschränkung der Sperre auf die abhandlungsgemene Karte muss sich der Karteninhaber mit seinem Kreditinstitut, möglichst mit der kontoführenden Stelle, in Verbindung setzen. Wird die Karte gestohlen oder missbräuchlich verwendet, ist unverzüglich Anzeige bei der Polizei zu erstatten.

Sobald dem Kreditinstitut oder dem Zentralen Sperrannahmedienst der Verlust der Karte angezeigt worden ist, trägt das Kreditinstitut die danach durch missbräuchliche Nutzung des Online-Banking entstandenen Schäden.

- Befindet sich der TAN-Generator auf einer Chipkarte ohne Zahlungsfunktion oder auf einem anderen elektronischen Gerät, so ist der Nutzer verpflichtet, sein Kreditinstitut, und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. In diesem Fall wird das Kreditinstitut den TAN-Generator sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht des Nutzers für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

## 10 Änderung der PIN

Der Nutzer ist berechtigt, seine PIN unter Verwendung einer TAN jederzeit zu ändern. Bei Änderung der PIN wird seine bisherige PIN ungültig.

## 11 Sperre des Online-Banking-Angebotes durch das Kreditinstitut

(1) Wird dreimal hintereinander eine falsche PIN eingegeben, so sperrt das Kreditinstitut den Online-Banking-Zugang zum Konto/Depot. Der Nutzer kann diese Sperre aufheben, indem er neben der richtigen PIN eine gültige TAN eingibt.

(2) Werden dreimal hintereinander falsche TAN eingegeben, so werden alle noch nicht verbrauchten TAN bzw. der TAN-Generator für das betreffende Konto/Depot gesperrt. Im Falle der vollständigen Sperrung der unbrauchten TAN in der TAN-Liste oder des TAN-Generators sollte sich der Nutzer mit dem Kreditinstitut in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

(3) Das Kreditinstitut wird den Online-Banking-Zugang zum Konto/Depot sperren, wenn der Verdacht einer missbräuchlichen Nutzung des Kontos/Depots über den Online-Banking-Zugang besteht. Es wird den Konto-inhaber hierüber außerhalb des Online-Banking informieren. Diese Sperre kann mittels Online-Banking nicht aufgehoben werden.

## 12 Sperre des Online-Banking-Angebotes auf Wunsch des Konto-inhabers

Das Kreditinstitut wird den Online-Banking-Zugang zum Konto/Depot auf Wunsch des Kontoinhabers sperren. Diese Sperre kann nicht mittels Online-Banking aufgehoben werden.

## 13 Einzug der Chipkarte mit Zahlungsfunktion und TAN-Generator

Das Kreditinstitut darf den Einzug der Chipkarte mit Zahlungsfunktion und TAN-Generator (z. B. am Geldausgabeautomaten) veranlassen, wenn es berechtigt ist, den Kartenvertrag aus wichtigem Grund zu kündigen. Das Kreditinstitut ist zur Einziehung der Karte auch berechtigt, wenn die Nutzungsberechtigung der Karte durch Gültigkeitsablauf oder durch ordentliche Kündigung endet. Der Einzug der Karte hat zur Folge, dass der Nutzer den TAN-Generator auf der Karte für das Online-Banking nicht mehr nutzen kann.

## 14 Rückruf oder Änderung von Aufträgen

Der Rückruf oder die Änderung von Aufträgen kann nur außerhalb des Online-Banking-Verfahrens erfolgen, es sei denn, das Kreditinstitut sieht eine solche Möglichkeit innerhalb des Verfahrens ausdrücklich vor. Das Kreditinstitut kann einen Rückruf oder eine Änderung allerdings nur beachten, wenn ihm diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufs möglich ist.

## 15 Anwendbares Recht

Auf die Geschäftsbeziehung zwischen dem Konto-/Depotinhaber und dem Kreditinstitut findet deutsches Recht Anwendung, es sei denn, dieses verweist auf eine ausländische Rechtsordnung.