

# Auftrag zur Online-Banking Nutzung

Name, Kunden-Nr., TAN-Optionsfelder und  
Unterschriftbitte ergänzen und zurücksenden an:

Online-Banking-Teilnehmer<sup>1</sup>

Deutsche Apotheker- und Ärztebank  
Zentrales Service Zentrum  
30135 Hannover

Kunden-Nr.:

Bitte nehmen Sie diesen Auftrag zur Online-Banking Nutzung entgegen.

Verfügungen über Online-Banking sind je Kalendertag und Konto zu begrenzen auf 25.000,00 € (ggf. ändern).  
Mit der apoBank können ein oder mehrere Sicherheitsverfahren genutzt werden.

## Standard: mobileTAN

Als Kunde der apoBank möchte ich das mobileTAN-Verfahren nutzen.

Bitte senden Sie die mobileTAN als SMS an die Mobiltelefonnummer:

Die Nutzung des mobileTAN-Services ist derzeit kostenlos. Es gilt insoweit das „Preis- und Leistungsverzeichnis“.

## Optional: Sm@rtTAN optic – TAN-Generierung mit der apoBankcard

Ich möchte (auch) das Verfahren Sm@rtTAN optic mit der apoBankcard nutzen.

Ich möchte dafür meine Karte-Nr. nutzen.

Die Nutzung ist für alle Ihre Konten mit nur einer apoBankcard möglich.

Ich besitze keine persönliche apoBankcard bestelle eine für das Konto mit der

IBAN:

Preise laut gültigem „Preis- und Leistungsverzeichnis“.

Ich bestelle ein Kartenlesegerät für Sm@rtTAN optic zum Einmalpreis von 10,00 €.  
Bitte buchen Sie den Betrag von meinem Konto mit der

IBAN:

ab.

Ich besitze bereits ein Kartenlesegerät, das Sm@rtTAN optic (Version 1.4) unterstützt.

Eine Übersicht der nutzbaren Kartenlesegeräte finden Sie unter <http://www.apobank.de/online> in der Kategorie Downloads.

## Optional: HBCI / FinTS mit elektronischer Signatur (HBCI-Software oder Chipkarten-Version)

Bitte senden Sie mir hierzu Informationen und die Zusatzvereinbarung.

Ich bestätige den Erhalt der vorvertraglichen Informationen für Fernabsatzverträge und der Sonderbedingungen für das Online-Banking.

Ort

Datum

Unterschrift:

x

x

x

<sup>1</sup> Bei Abschluss durch einen Minderjährigen bitte eine entsprechende Zustimmungserklärung zusätzlich verwenden.

# Vorvertragliche Informationen zum Online-Banking



Die nachstehenden vorvertraglichen Informationen gelten bis auf Weiteres und stehen nur in deutscher Sprache zur Verfügung. Fragen hierzu beantwortet gerne Ihr(e) Kundenbetreuer(in).

## I. Allgemeine Informationen

### Name und Anschrift der Bank (Zentrale)

Deutsche Apotheker- und Ärztekasse eG  
Richard-Oskar-Mattern-Straße 6  
40547 Düsseldorf  
Telefon +49 211 5998 0 E-Mail info@apobank.de  
Telefax +49 211 593877 im Internet unter www.apobank.de

Sie können sich auch an Ihre zuständige Filiale wenden. Deren Kontaktdaten erhalten Sie auch über unsere Zentrale.

### Gesetzlich Vertretungsberechtigter der Bank ist der Vorstand

Herbert Pfennig (Vorsitzender), Ulrich Sommer (stv. Vorsitzender), Olaf Klose, Eckhard Lüdering, Dr. Thomas Siekmann, Holger Wessling

**Eintragung (der Hauptniederlassung) im Genossenschaftsregister Amtsgericht Düsseldorf**  
unter GnR 410

Umsatzsteueridentifikationsnummer DE119260415

**Hauptgeschäftstätigkeit der Bank ist der Betrieb von Bankgeschäften**  
aller Art und von damit zusammenhängenden Geschäften.

**Zuständige Aufsichtsbehörde für die Zulassung von Kreditinstituten**  
Europäische Zentralbank, Sonnemannstraße 20, 60314 Frankfurt am Main, im Internet unter www.ecb.europa.eu

**Zuständige Aufsichtsbehörde für die Zulassung des Pfandbriefgeschäfts und für den Schutz der kollektiven Verbraucherinteressen**  
Bundesanstalt für Finanzdienstleistungsaufsicht, Graurheindorfer Str. 108, 53117 Bonn bzw. Marie-Curie-Str. 24-28, 60439 Frankfurt am Main, im Internet unter www.bafin.de

### Vertragsprache

Maßgebliche Sprache für dieses Vertragsverhältnis und die Kommunikation mit dem Kunden während der Laufzeit des Vertrages ist deutsch.

### Rechtsordnung/Gerichtsstand

Für den Vertragsschluss und die gesamte Geschäftsverbindung zwischen dem Kunden und der Bank gilt deutsches Recht.  
Es gibt keine vertragliche Gerichtsstandsklausel.

### Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit

- **Beschwerdestelle der Bank:** Deutsche Apotheker- und Ärztekasse eG, Qualitätsmanagement, Richard-Oskar-Mattern-Straße 6, 40547 Düsseldorf
- **Ombudsmannverfahren** beim Bundesverband der genossenschaftlichen Bankengruppe: Darüber hinaus besteht für Sie die Beilegung von Streitigkeiten mit der Bank die Möglichkeit, den Ombudsmann der genossenschaftlichen Bankengruppe anzurufen. Näheres regelt die Verfahrensordnung für die außergerichtliche Schlichtung von Kundenbeschwerden im Bereich der deutschen genossenschaftlichen Bankengruppe, die Ihnen auf Wunsch zur Verfügung gestellt wird. Die Beschwerde richten Sie bitte schriftlich an: Kundenbeschwerdestelle beim Bundesverband der Deutschen Volksbanken und Raiffeisenbanken - BVR, Schellingstr. 4, 10785 Berlin

### Hinweis zum Bestehen einer freiwilligen Einlagensicherung

Die Bank ist der BVR Institutssicherung GmbH und der Sicherungseinrichtung des Bundesverbandes der Deutschen Volksbanken und Raiffeisenbanken e. V. angeschlossen, im Internet unter www.bvr.de/SE.

## II. Informationen zum Online-Banking

Auf der Grundlage einer Vereinbarung mit der Bank über die Nutzung des Online-Banking kann der Kunde Konto- und Depotabfragen tätigen bzw. Bankgeschäfte entweder mit elektronischer Signatur oder PIN/ TAN-Verfahren über das Internet in dem vom Kreditinstitut gebotenen Umfang abwickeln (im Folgenden einheitlich als Online-Banking bezeichnet). Voraussetzung dafür ist, dass der Kunde ein Konto bzw. Depot bei der Bank unterhält. Der Nutzungsumfang des Online-Banking kann dabei auf bestimmte Geschäftsvorfälle und auf Höchstbeträge begrenzt werden.

Der Kunde erhält für die Übermittlung von Erklärungen oder Aufträgen, abhängig von angebotenen Verfahren, entsprechende Sicherheitsmedien.

Für das PIN/ TAN-Verfahren erhält der Kunde zum einen eine persönliche Identifikationsnummer (Online-PIN) sowie (bei sm@rtTAN) einen TAN-Generator in

Form einer Chipkarte oder bei Nutzung der mobileTAN die TAN per SMS, wofür zum Empfang ein entsprechendes Endgerät (z. B. Mobiltelefon) erforderlich ist. Für das elektronische Signatur-Verfahren erhält der Kunde eine Signatur-Chipkarte mit den Zugangsdaten der Bank oder die Zugangsdaten der Bank, um selbst ein Identifikationsmedium (HBCI-Sicherheitsdatei) zu erstellen, auf dem sich der Signaturschlüssel befindet.

Für die Nutzung einer Chipkarte ist zusätzlich ein geeignetes Kartenlesegerät erforderlich.

Die aktuellen Preise für die Dienstleistungen der Bank im Zusammenhang mit dem Online-Banking ergeben sich aus dem beiliegendem Preis- und Leistungsverzeichnis.

Die Änderung von Entgelten während der Laufzeit der Vereinbarung über die Nutzung des Online-Banking mit den genannten Sicherheitsmedien erfolgt nach Maßgabe von Nr. 12 Abs. 1 und Abs. 7 der **Allgemeinen Geschäftsbedingungen** der Bank.

Kosten, die nicht von der Bank abgeführt oder in Rechnung gestellt werden (z. B. Telefon, Internet, Porti), hat der Kunde selbst zu tragen. Es gibt keinen Leistungsvorbehalt, es sei denn, dieser ist ausdrücklich vereinbart. Die anfallenden Entgelte werden auf dem vom Kunden hierfür angegebenen Konto zum Quartalsende belastet.

Die Bank erfüllt ihre Verpflichtungen aus der Vereinbarung über die Nutzung des Online-Banking, indem sie dem Kunden die erforderlichen Sicherheitsmedien bzw. Zugangsdaten zur eigenen Erzeugung eines Sicherheitsmediums zur Verfügung stellt und den Kunden für die Nutzung des Online-Banking freischaltet. Sie wird des Weiteren die vom Kunden freigegebenen, mittels Online-Banking übermittelten Aufträge im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeiten.

Die Vereinbarung über die Nutzung des Online-Banking mit dem jeweiligen Sicherheitsmedium kann vom Kunden jederzeit gekündigt werden. Im Übrigen gelten die in Nr. 18 und 19 der **Allgemeinen Geschäftsbedingungen** für die Kunden und die Bank festgelegten Kündigungsregeln. Es besteht keine Mindestlaufzeit.

Die Bank erwirbt als Sicherheit für ihre Forderungen ein Pfandrecht an den Wertpapieren und Sachen, an denen eine inländische Geschäftsstelle Besitz erlangt oder noch erlangen wird. Die Bank erwirbt ein Pfandrecht auch an den Ansprüchen, die dem Kunden gegen die Bank aus der bankmäßigen Geschäftsverbindung zustehen oder künftig zustehen werden. Das Pfandrecht dient der Sicherung aller bestehenden, künftigen und bedingten Ansprüche, die der Bank gegen den Kunden zustehen. Für den gesamten Geschäftsverkehr gelten ergänzend die **Allgemeinen Geschäftsbedingungen** der Bank. Der Wortlaut dieser Bedingungen kann im Internet unter www.apobank.de oder in den Geschäftsräumen der Bank eingesehen werden; auf Verlangen werden die Bedingungen auch ausgehändigt. Daneben gelten die beiliegenden **Sonderbedingungen für das Online-Banking**, die Abweichungen oder Ergänzungen zu diesen **Allgemeinen Geschäftsbedingungen** enthalten. Die genannten Bedingungen stehen nur in deutscher Sprache zur Verfügung. Bei Änderungsvereinbarungen ergeben sich weiterführende Informationen auch aus der ursprünglichen Vertragsurkunde.

## III. Informationen zum Zustandekommen des Vertrags

Der Kunde gibt gegenüber der Bank ein ihn bindendes Angebot ab, indem ein unterzeichneter Auftrag der Bank zugeht. Der Vertrag kommt zustande, wenn die Bank dem Kunden die Annahme des Vertrages erklärt, indem sie das Online-Banking einrichtet und dem Kunden eine Bestätigung über die Einrichtung zugeht.

#### IV. Widerrufsbelehrung

##### Widerrufsbelehrung

##### Widerrufsrecht

Sie können Ihre Vertragserklärung innerhalb von 14 Tagen ohne Angabe von Gründen mittels einer eindeutigen Erklärung widerrufen. Die Frist beginnt nach Erhalt dieser Belehrung auf einem dauerhaften Datenträger, jedoch nicht vor Vertragsschluss und auch nicht vor Erfüllung unserer Informationspflichten gemäß Artikel 246b § 2 Absatz 1 in Verbindung mit § 1 Absatz 1 Nummer 7 bis 12, 15 und 19 sowie Artikel 248 § 4 Absatz 1 EGBGB. Zur Wahrung der Widerrufsfrist genügt die rechtzeitige Absendung des Widerrufs, wenn die Erklärung auf einem dauerhaften Datenträger (z. B. Brief, Telefax, E-Mail) erfolgt. Der Widerruf ist zu richten an:

##### Deutsche Apotheker- und Ärztebank eG

Richard-Oskar-Mattern-Straße 6  
40547 Düsseldorf

##### Widerrufsfolgen

Im Falle eines wirksamen Widerrufs sind die beiderseits empfangenen Leistungen zurückzugewähren. Sie sind zur Zahlung von Wertersatz für die bis zum Widerruf erbrachte Dienstleistung verpflichtet, wenn Sie vor Abgabe Ihrer Vertragserklärung auf diese Rechtsfolge hingewiesen wurden und ausdrücklich zugestimmt haben, dass wir vor dem Ende der Widerrufsfrist mit der Ausführung der Gegenleistung beginnen. Besteht eine Leistung zum Wertersatz, kann dies dazu führen, dass Sie die vertraglichen Zahlungsverpflichtungen für den Zeitraum bis zum Widerruf dennoch erfüllen müssen. Ihr Widerrufsrecht erlischt vorzeitig, wenn der Vertrag von beiden Seiten auf Ihren ausdrücklichen Wunsch hin vollständig erfüllt ist, bevor Sie Ihr Widerrufsrecht ausgeübt haben. Verpflichtungen zur Erstattung von Zahlungen müssen innerhalb von 30 Tagen erfüllt werden. Die Frist beginnt für Sie mit der Absendung Ihrer Widerrufserklärung, für uns mit deren Empfang.

##### Besonderer Hinweis

Bei Widerruf dieses Vertrags sind Sie auch an einen mit diesem Vertrag zusammenhängenden Vertrag nicht mehr gebunden, wenn der zusammenhängende Vertrag eine Leistung betrifft, die von uns oder einem Dritten auf der Grundlage einer Vereinbarung zwischen uns und dem Dritten erbracht wird.

Ende der Widerrufsbelehrung

Datum des Ausdrucks 09.2016

Ende der Informationsschrift

## Bereitstellung von Informationen und Sicherheit von Internetzahlungen.

Unsere Internetzahlungsdienste bieten Ihnen ein Höchstmaß an Schutz im Netz. Dabei unterstützen wir Sie regelmäßig mit den aktuellsten Informationen zum Thema Sicherheit im Internet. Lesen Sie regelmäßig auf unseren Internetseiten die Sicherheits-hinweise, Warnungen und Beispiele von Betrugsversuchen. Beachten Sie grundsätzlich folgende Regeln zur Sicherheit.

### Sicher im Internet.

#### So erhalten Sie unsere Informationen.

Die apoBank nutzt folgende Medien zur sicheren Informationsübertragung:

- Den elektronischen Postkorb innerhalb der Online-Filiale (Internet-Banking)
- Unsere gesicherte Webseite [www.apobank.de](http://www.apobank.de)
- Den Kontoauszug auf Papier
- Den klassischen Postbrief

Nachrichten zur Sicherheit von Internetzahlungsdiensten, die Sie über andere Wege als die hier genannten erreichen, sind nicht vertrauenswürdig. Nehmen Sie im Zweifel Kontakt mit uns auf.

#### So bewegen Sie sich sicher im Netz.

Die Notwendigkeit folgender Vorkehrungen sollte für Sie selbstverständlich sein:

- Passwörter nicht speichern und nicht an Dritte weitergeben
- Sicherheits-Token an einem sicheren Ort aufbewahren
- Persönliche Angaben und sonstige Daten vertraulich behandeln
- Virenschutzprogramme, Firewalls und Sicherheits-Patches installieren und regelmäßig aktualisieren
- Nur geprüfte und als echt zertifizierte Software herunterladen
- Nur die Original-Webseite für Internetzahlungen nutzen

#### So nutzen Sie unsere Online-Filiale (Internet-Banking) sicher.

Wir empfehlen Ihnen apoProtect als Browser für die Nutzung des Internet-Banking. Die Software stellen wir Ihnen automatisch in Ihrem elektronischen Postkorb gratis zur Verfügung. Durch den Einsatz von apoProtect sind Sie noch besser vor Schadsoftware geschützt, welche die Standardbrowser angreift und die Anzeige z. B. im Firefox oder Internet-Explorer manipuliert. Detaillierte Informationen finden Sie auf unseren Internetseiten.

## So melden Sie Unregelmäßigkeiten und Vorfälle in Bezug auf Internetzahlungen und zugehörige Dienste.

Für die Meldung von Unregelmäßigkeiten und Vorfällen in Bezug auf Internetzahlungen und zugehörige Dienste steht Ihnen die Funktion „Schreiben Sie uns“ auf der Internetseite (in der Fußzeile unter Kontakt) rund um die Uhr (24/7) zur Verfügung. Während der üblichen Geschäftszeiten besteht Möglichkeit für Fragen, Beschwerden oder Anfragen zur Unterstützung in Bezug auf Internetzahlungsdienste und zugehörige Dienste unseren Telefonservice Electronic-Banking unter **+49 211 5998 8000** anzurufen.

Ihre schriftlichen Meldungen werden wir über die oben genannten Medien zur sicheren Informationsübertragung beantworten.

## Konto-Limite und Sperren.

Für unsere Internetzahlungsdienste gelten – von Ihnen festgelegte – individuelle Limite.

### Limite beim Online-Banking.

Für jedes Konto ist ein Kontolimit entsprechend Ihrer persönlichen Online-Banking-Vereinbarung festgelegt. Eine individuelle Änderung ist jederzeit möglich. Weitere Limite z. B. für einzelne Personen pro Konto oder Person pro Zugangsweg (Online, Telefon) können zusätzlich vereinbart werden. Wenden Sie sich dazu einfach an Ihren persönlichen Berater.

### Kreditkarten-Limit.

Für Ihre Kreditkarte gilt das Limit Ihres persönlichen Kreditkartenvertrages. Bei Fragen ist Ihr Berater gerne für Sie da.

### Sperrung von Konto und Online-Zugang.

In der Online-Filiale können Sie Ihr Konto, Ihren Online-Zugang und Bevollmächtigte sperren. Oder Sie nutzen die Sperrhotline **116 116**.

### Kartensperrung.

Notfall-Telefonnummern bei Verlust Ihrer Bankcard oder Ihrer Kreditkarten:

#### ▪ Bankcard

- Sperrannahme bei Verlust oder Diebstahl
  - Zentraler Sperrannahmedienst: **+49 1805 021 021** (0,14 Euro/Minute Festnetzpreis; Mobilfunkhöchstpreis: 0,42 Euro/Minute)
  - Kontoführende apoBank-Filiale (während der Geschäftszeiten)

#### ▪ Kreditkarten der apoBank

- Sperrannahme bei Verlust oder Diebstahl
  - 24-Stunden-Sperrannahmedienst der Firma CardProcess: **+49 721 1209 66001**

# Sonderbedingungen für das Online-Banking

Fassung: Oktober 2011

## 1 Leistungsangebot

1.1 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.

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

1.3 Zur Nutzung des Online-Banking gelten die mit der Bank gesondert vereinbarten Verfügungslimits. Eine Änderung dieser Limits kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

## 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 Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (vgl. Nr. 3) und Aufträge zu autorisieren (vgl. Nr. 4).

### 2.1 Personalisierte Sicherheitsmerkmale sind:

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

### 2.2 Authentifizierungsinstrumente

Die TAN bzw. die elektronische Signatur können dem Teilnehmer auf folgenden Authentifizierungsinstrumenten 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 (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
- auf einer Chipkarte mit Signaturfunktion oder
- auf einem sonstigen Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden.

Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

## 3 Zugang zum Online-Banking

Der Teilnehmer erhält Zugang zum Online-Banking, wenn

- der Teilnehmer 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 (vgl. Nr. 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 (z. B. 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 (z. B. 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

5.1 Die Bearbeitung der Online-Banking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. 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 darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

5.2 Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat sich mit dem Personalisierten Sicherheitsmerkmal autorisiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. 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 (z. B. ausreichende Kontodeckung gemäß den Sonderbedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Nr. 5.2 vor, führt die Bank die Online-Banking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

5.3 Liegen die Ausführungsbedingungen nach Nr. 5.2 nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen und dem Teilnehmer eine Information 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 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 Sorgfaltspflichten des Teilnehmers

### 7.1 Technische Verbindung zum Online-Banking

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

### 7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

#### 7.2.1 Der Teilnehmer hat

- seine Personalisierten Sicherheitsmerkmale (vgl. Nummer 2.1) geheim zu halten und nur im Rahmen einer Auftragserteilung über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln sowie

- sein Authentifizierungsinstrument (vgl. Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren

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

7.2.2 Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

- Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (z. B. 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 (z. B. 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 Authentifizierungsinstrument verwahrt werden.

- Der Teilnehmer darf zur Autorisierung z. B. eines Auftrags, der Aufhebung einer Sperre nicht mehr als eine TAN verwenden.

- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht für das Online-Banking genutzt werden.

### 7.3 Sicherheit des Kundensystems

Der Teilnehmer muss die Sicherheitshinweise 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 (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z. B. 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 Unterrichtungspflichten

### 8.1 Sperranzeige

8.1.1 Stellt der Teilnehmer den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines Persönlichen Sicherheitsmerkmals fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine

Sperranzeige jederzeit auch über eine gesondert mitgeteilte Telefonnummer aufgeben.

8.1.2 Der Teilnehmer hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen.

8.1.3 Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt – den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder – das Authentifizierungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet, muss er ebenfalls eine Sperranzeige abgeben.

#### **8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge**

Der Kontoinhaber 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**

9.1.1 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 Authentifizierungsinstrument.

#### **9.2 Sperre auf Veranlassung der Bank**

9.2.1 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 Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder – der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht

9.2.2 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 bzw. das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber bzw. den Online-Banking-Teilnehmer.

#### **9.4 Automatische Sperre eines chip-basierten Authentifizierungsinstruments**

9.4.1 Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn der Nutzungscod für die elektronische Signatur dreimal in Folge falsch eingegeben wird.

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

9.4.3 Die in den Absätzen 1 und 2 genannten Authentifizierungsinstrumente 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 (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

#### **10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments**

##### **10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige**

10.2.1.1 Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob dem Teilnehmer an dem Verlust, Diebstahl oder sonstigen Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

10.2.1.2 Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verloren gegangen, gestohlen oder sonst abhand-

den 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 der Personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

10.2.1.3 Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 Euro nach den Nrn. 10.2.1.1 und 10.2.1.2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen gehandelt hat.

10.2.1.4 Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Nrn. 10.2.1.1 bis 10.2.1.3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nr. 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

10.2.1.5 Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere dann vorliegen, wenn er

- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (vgl. Nr. 8.1.1),
- das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (vgl. Nr. 7.2.2, 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde (vgl. Nr. 7.2.2, 2. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (vgl. Nr. 7.2.2, 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (vgl. Nr. 7.2.2, 4. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (vgl. Nr. 7.2.2, 5. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet (vgl. Nr. 7.2.2, 6. Spiegelstrich),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Online-Banking nutzt (vgl. Nr. 7.2.2, 7. Spiegelstrich).

10.2.1.6 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 bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige**

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

##### **10.2.3 Haftung der Bank ab der Sperranzeige**

Sobald die Bank eine Sperranzeige des 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.

### **11 Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit**

Für die Beilegung von Streitigkeiten mit der Bank kann sich der Teilnehmer an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- oder Beschwerdestellen wenden.

## Vorwort

**Zur Beachtung:** Jede Bank ist ein Dienstleistungsunternehmen, das seine Aufgaben nur erfüllen kann, wenn es dafür ein angemessenes Entgelt erhält. Ein Gebührenverzeichnis kann nicht alle denkbaren Leistungen der Bank enthalten.

Deshalb kann die Bank auch für die im Gebührenverzeichnis nicht aufgeführten Tätigkeiten, soweit sie im Interesse des Kunden durchgeführt werden, eine angemessene Gegenleistung berechnen. Bitte beachten Sie dies bei der Gebührenberechnung. Daneben werden die im Zusammenhang mit der Geschäftsverbindung entstandenen Fremdkosten an Kunden weitergegeben.

## Erläuterungen und Abkürzungen

**Mehrwertsteuer:** Sämtliche angegebenen Gebühren gelten als mehrwertsteuerfrei, sofern nicht bei der Gebühr auf die zuzüglich zu berechnende oder inklusive enthaltene Mehrwertsteuer hingewiesen wird.

**IBAN/BIC:** IBAN ist die Abkürzung für die Internationale Bankkontonummer (International Bank Account Number). BIC ist die Abkürzung für die internationale Bankleitzahl/Bank-Identifikationsnummer (Bank Identifier Code).

**EWER:** Zum Europäischen Wirtschaftsraum gehören derzeit die EU-Staaten Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechien, Ungarn, Vereinigtes Königreich von Großbritannien und Nordirland sowie Zypern und die Staaten Island, Liechtenstein und Norwegen.

**EWER-Währungen:** Zu den EWER-Währungen gehören derzeit: Euro, Britisches Pfund, Bulgarische Lew, Dänische Krone, Isländische Krone, Kroatianische Kuna, Norwegische Krone, Polnische Zloty, Rumänische Leu, Schwedische Krone, Schweizer Franken, Tschechische Krone, Ungarische Forint.

**Geschäftstage:** Geschäftstag ist jeder Tag, an dem die an der Ausführung eines Zahlungsvorganges beteiligten Zahlungsdienstleister den für die Ausführung von Zahlungsvorgängen erforderlichen Geschäftsbetrieb unterhalten. Die Bank unterhält den für die Ausführung von Zahlungen erforderlichen Geschäftsbetrieb an allen Werktagen, mit Ausnahme Sonnabende, 24. (Heiligabend) und 31. (Silvester) Dezember.

## Aufbau des Preis- und Leistungsverzeichnisses

- A Zahlungsverkehr
- B Kontoführung
  - B.1 Kontoeröffnung/-änderung
  - B.2 Postengebühren
  - B.3 Kontoauszüge und Zweitschriften
  - B.4 apoBankcard
  - B.5 Kreditkarten (Einzelprodukte)
- C Kreditgeschäft
- D Passivgeschäft
  - D.1 Spareinlagen
  - D.2 Termineinlagen
- E Überweisungsverkehr
- F Wertpapiergeschäft
- G Außenhandel
- H Schließfächer und Verwahrstücke
- I Sonstige Gebühren
- K Wertstellungstabelle
- L Annahme- und Ausführungsfristen
- M Sonstige Beschwerdemöglichkeit und außergerichtliches Streitschlichtungsverfahren

Als Auszug aus dem Preis- und Leistungsverzeichnis ist das Kapitel I beigefügt.

## I Sonstige Gebühren

Stand: 26.03.2013

*	Mit „ggf. zzgl. MwSt.“ ausgewiesene Gebühren sind steuerfrei, wenn Sie im Zusammenhang mit einer Kreditgewährung oder sonstigen steuerfreien Geschäften der Bank stehen. Steuerpflicht besteht dagegen für Kunden der Bank im Rahmen steuerpflichtiger Geschäfte, an andere Kreditinstitute oder deren Kunden.	
<b>1</b>	<b>Auskünfte (für Kunden)</b>	
1.1	Nachforschung (im Auftrag des Kunden ausgeführt), wenn die Nachforschung durch vom Kunden zu vertretende Umstände verursacht wurde	
	... im Inland	▶ 20,00 € ggf. zzgl. MwSt.*
	... im Ausland	▶ 40,00 € ggf. zzgl. MwSt.*
1.2	Büroauskünfte	▶ 20,00 € ggf. zzgl. MwSt.*
1.3	Auskünfte über beantragten/verbrauchten Freibetrag pro Jahr	▶ 10,00 € zzgl. MwSt.
<b>2</b>	<b>Materialien</b>	
2.1	Vordrucke in kleinen Mengen (Schecks, Überweisungsträger etc.)	▶ gebührenfrei
2.2	Vordrucke in größeren Mengen (blanko)	▶ gemäß besonderer Anweisung zzgl. MwSt.
3	Telefonkosten (nicht Privatgespräche): Umfangreiche Gespräche im Interesse des Kunden	▶ je nach Dauer und Entfernung, mindestens 20,00 € ggf. zzgl. MwSt.*
4	Kosten pro versandter SMS für mobileTAN im Inland	▶ gebührenfrei
5	TAN Generator mit optischer Schnittstelle „TAN Optimus comfort“	▶ 7,50 € inkl. MwSt. zzgl. 2,50 € Versand
6	HBCI-Freischaltung für HBCI-Software, Zusendung HBCI INI-Brief	▶ 20,00 €
7	Secoder Chipkartenleser HBCI "Reiner SCT cyberjack" RFID Standard	▶ 49,90 € inkl. MwSt. zzgl. 4,90 € Versand
<b>8</b>	<b>GenoCash</b>	
8.1	Softwarelizenz GenoCash Basis inkl. Cash-Management + EBICS	▶ 195,00 € zzgl. MwSt.
8.2	Anwendungsmodule IZV, SEPA oder AZV inkl. Wartung und Updates	▶ 95,00 € zzgl. MwSt. jeweils
8.3	Installation der apoBank vor Ort	▶ 75,00 € zzgl. MwSt. pro Stunde vor Ort
8.4	Servicegebühren sonstige ZV-Dienstleistungen	▶ 95,00 € zzgl. MwSt. pro Stunde
8.5	Telefonischer Support Telefon 0800 2171790	▶ gebührenfrei
9	Fotokopien für Kunden (pro Blatt)	▶ 1,00 € zzgl. MwSt., mindestens 5,00 €
10	Anfrage beim Einwohnermeldeamt/Amtsgericht etc.	▶ 10,00 € ggf. zzgl. MwSt.* + Fremdggebühren, soweit gesetzlich zulässig