

# Auftrag Freischaltung für das Fondsbanking und den InfoManager

Der Auftrag kann per **Telefax an +49 (0) 9281 7258 - 46118** oder per Mailanhang jeweils mit Kundenunterschrift an **info@fondsdepotbank.de** gesendet werden.

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Depot-Nr.

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Geldkonto-Nr.

Dieser Auftrag soll außerdem für das/die folgende/n Depot/s/Konto/en gelten:

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Nr.

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Nr.

## A. Angaben Depot-/Geldkontoinhaber (im Nachfolgenden "Inhaber" genannt)

### 1. Inhaber

weiblich  männlich  divers  Prof.  Dr.  Firma

bzw. 1. gesetzlicher Vertreter

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Name bzw. Firma

Vorname/n gemäß Legitimationsdokument bzw. Rechtsform

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Straße

Nummer

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

PLZ

Ort

Land

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Telefon <sup>1</sup>

E-Mail

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Bereits vorhandene Zugangskennung im Rahmen des Fondsbanking bzw. InfoManager

### 2. Inhaber

weiblich  männlich  divers  Prof.  Dr.

bzw. 2. gesetzlicher Vertreter

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Name

Vorname/n <sup>2</sup>

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Straße

Nummer

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

PLZ

Ort

Land

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Telefon <sup>1</sup>

E-Mail

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Bereits vorhandene Zugangskennung im Rahmen des Fondsbanking bzw. InfoManager

**Hinweis:** Bitte füllen Sie die oben genannten Adressangaben vollständig aus. An die jeweils angegebene Adresse werden Ihre Zugangs- sowie Authentifizierungsdaten und mit gesonderter Post Ihre persönliche Identifikationsnummer (im Nachfolgenden „PIN“ genannt) gesandt.

## B. Bevollmächtigter (Freischaltung nur bei bereits hinterlegter Vollmacht möglich)

**Hinweis:** Mit diesem Formular "Auftrag Freischaltung für das Fondsbanking und den InfoManager" ist keine Bevollmächtigung möglich. Eine Freischaltung erfolgt nur, wenn der nachfolgend genannte Bevollmächtigte im Depot bereits im/in o.g. Depot/s/Geldkonto/-konten hinterlegt ist.

Ich besitze eine Vollmacht zu Lebzeiten und über den Tod hinaus.

Ich bin vertretungsberechtigte Person der oben genannten Firma.

### Angaben Bevollmächtigter/r

weiblich  männlich  divers  Prof.  Dr.

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Name

Vorname/n <sup>2</sup>

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Straße

Nummer

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

PLZ

Ort

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Telefon <sup>1</sup>

E-Mail

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Bereits vorhandene Zugangskennung im Rahmen des Fondsbanking bzw. InfoManager

Pflichtfeld

**1. Inhaber**

Name bzw. Firma

**2. Inhaber**

Vorname/n bzw. Rechtsform

Name

Vorname/n

Geldkonto-Nr.

Depot-Nr.

**C. Freischaltung für das Fondsbanking**

**Fondsbanking**

Das Fondsbanking ermöglicht die Einsichtnahme von Depotbeständen, Kontoständen, Spar- und Auszahlplänen, Depotumsätzen und persönlichen Daten über das Internet (Leseberechtigung).

Ferner kann der Nutzer Aufträge zu Spar- und Auszahlplänen über das Internet erteilen, Überweisungsaufträge veranlassen und Daueraufträge einrichten und verwalten sowie gezogene Lastschriften im Rahmen der Rückgabefrist zurück buchen (Transaktionsberechtigung).

**Ich/Wir beantrage/n im Rahmen des Fondsbanking der Fondsdepot Bank GmbH (im Nachfolgenden "Bank" genannt) die Freischaltung für o. g. Depot/s/Geldkonto/-konten in Verbindung mit einer Leseberechtigung, sofern nachfolgend nichts anderes gekennzeichnet ist.**

**Gleichzeitig beantrage/n ich/wir die Transaktionsberechtigung für o.g. Depot/s und/oder Geldkonto/-konten. Hierfür ist die Erteilung eines neuen Mandats durch Angabe der Bankverbindung zwingend erforderlich.**

**Hinweis:** Eine Freischaltung der Transaktionsberechtigung ist ausschließlich für das Fondsdepot möglich, sofern nicht Produkte betroffen sind, bei denen Einschränkungen produktspezifischer Art im Hinblick auf die Transaktionsberechtigung vorliegen. Bei Fragen wenden Sie sich bitte an Ihren Berater.

**Hinweis für Firmenkunden:** Für das Fondsbanking sind nur natürliche Personen nutzungsberechtigt. Bitte tragen Sie den Bevollmächtigten als vertretungsberechtigte Person ein.

**Einrichtung Referenzbankverbindung/Mandatserteilung Depot**

**Zu meiner/unserer Sicherheit wird die Bank Aufträge zum Kauf oder Verkauf von Anteilen oder Aktien an Investmentvermögen jeglicher Art (inkl. Steuererstattungsbeträge [nur Privatvermögen]) nur ausführen, wenn der Gegenwert von der genannten Referenzbankverbindung meines/unseres Depots eingezogen wird oder der Transfer des Verkaufserlöses gemäß meiner/unserer Weisung auf meine/unserer genannte Referenzbankverbindung erfolgen soll.**

**SEPA-Lastschriftmandat**

Gläubiger-Identifikationsnummer der Bank: **DE55ZZZ00000261267**

Die Mandatsreferenz wird Ihnen nach Einrichtung des Mandats separat schriftlich mitgeteilt (z. B. bei erstmaligem Einzug einer Lastschrift).

Ich/Wir ermächtige/n die Bank, Geldbeträge von meinem/unserem Konto mittels Lastschrift einzuziehen. Zugleich weise/n ich/wir mein/unser Kreditinstitut an, die von der Bank auf dieses Konto gezogene Lastschrift einzulösen.

Ich/Wir stelle/n sicher, dass eine SEPA-Basislastschrift von der Bankverbindung erfolgen kann und habe/n keine Sparkonten angegeben.

**Wichtige Informationen:**

- Ich/Wir kann/können innerhalb von 8 Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit dem kontoführenden Kreditinstitut vereinbarten Bedingungen.
- Ich/Wir nehmen zur Kenntnis, dass Kaufaufträge per Lastschrift nur bis zu einem Betrag von 50.000,00 EUR je Auftrag ausgeführt werden können. Bei Beträgen über 50.000,00 EUR werde/n ich/wir den Anlagebetrag auf das Einzahlungskonto der Fondsdepot Bank GmbH überweisen.
- Aufträge zu Käufen und Sparplänen per Lastschrift kann ich/können wir nur auf einem gültigen Formular der Fondsdepot Bank GmbH erteilen.
- Mandatserteilung: Das SEPA-Lastschriftmandat verliert seine Gültigkeit, wenn der Zahlungspflichtige oder Zahlungsempfänger dieses schriftlich widerruft bzw. es nach dem letzten Lastschritteinzug 36 Monate nicht in Anspruch genommen wurde. In diesen Fällen und bei Änderung des Girokontoinhabers ist die Erteilung eines neuen SEPA-Lastschriftmandates erforderlich.

**Referenzbankverbindung**

Girokontoinhaber (Name, Vorname/n)

Kreditinstitut (Name, Ort)

BIC

IBAN

Ort, Datum



Unterschrift/en des/der Depot-/Kontoinhaber/s bzw. des/der gesetzlichen Vertreter/s (Vollmachtgeber)

**Der Girokontoinhaber muss identisch sein mit dem oder einem der Inhaber bzw. mit dem oder einem der gesetzlichen Vertreter/Bevollmächtigten zu Lebzeiten und über den Tod hinaus.**

Pflichtfeld

**1. Inhaber**

\_\_\_\_\_  
Name bzw. Firma

**2. Inhaber**

\_\_\_\_\_  
Vorname/n bzw. Rechtsform

\_\_\_\_\_  
Name

\_\_\_\_\_  
Vorname/n

\_\_\_\_\_  
Geldkonto-Nr.

\_\_\_\_\_  
Depot-Nr.

**D. Freischaltung für den InfoManager**

**InfoManager**

Der InfoManager ist ein elektronisches Postfach, in dem bestimmte Dokumente, die im Rahmen der Depot-/Kontoführung produziert werden (z. B. Depot-/Kontoabrechnung, Ausschüttungsmittelungen, Kosteninformation), zum Download hinterlegt werden.

**Ich/Wir beauftrage/n die Bank zur Freischaltung des InfoManager. Bitte veranlassen Sie die Freischaltung für o. g. Depot/s/ Geldkonto/-konten.**

Über den Eingang neuer Dokumente in meinem/unserem InfoManager wird mich/uns die Bank per E-Mail an die angegebene/n E-Mail-Adresse/n benachrichtigen. Wird bei Angaben des Inhabers nur eine E-Mail-Adresse angegeben, erfolgt der Versand der E-Mail nur an diese E-Mail-Adresse.

**E. Schlusserklärungen**

**Hinweis:** Für die Freischaltung des Fondsbanking und des InfoManager erhält/erhalten der/die Inhaber mit der Post seine/ihre Zugangs- sowie Authentifizierungsdaten und mit gesonderter Post eine persönliche Identifikationsnummer (im Nachfolgenden "PIN" genannt) für Depot/s/ Geldkonto/-konten. Zur Änderung der PIN benötigen Sie eine generierte TAN. Bei Gemeinschaftsdepots/-konten erhält jeder Inhaber separate Zugangsdaten.

**Ergänzend zu den im Rahmen der Depoteröffnung bereits benannten Geschäftsbedingungen gelten zusätzlich noch die "Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager".**

**Mit der Freischaltung des o. g. Bevollmächtigten erkläre/n ich/wir mich/uns hiermit einverstanden.**

**Unterschrift/en zum Auftrag**

**Hinweis:** Es sind die Unterschriften aller Inhaber bzw. gesetzlichen Vertreter erforderlich.

**Mit meiner/unseren nachfolgenden Unterschrift/en bestätige/n ich/wir den Auftrag.**

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Ort, Datum

X \_\_\_\_\_  
Unterschrift 1. Inhaber bzw. 1. gesetzlicher Vertreter

X \_\_\_\_\_  
Unterschrift 2. Inhaber bzw. 2. gesetzlicher Vertreter

\_\_\_\_\_  
Ort, Datum

X \_\_\_\_\_  
Unterschrift Bevollmächtigter

**Fußnotenverzeichnis:**

<sup>1)</sup> Die Erteilung dieser Auskunft ist freiwillig.  
<sup>2)</sup> Sämtliche Vornamen gemäß Ausweisdokument.

# Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager (Stand 1. Januar 2022)

Im Nachfolgenden wird der Begriff Fondsbanking durch Online Banking ersetzt.

## Teil A: Online Banking

### 1. Leistungsangebot

- (1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels Online Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online Banking abrufen. Des Weiteren sind zusätzlich sie gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absatz Absätze 33 und 34 Zahlungsdienstaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.
- (2) Kunde und Bevollmächtigte werden einheitlich als „Teilnehmer“, Konto und Depot einheitlich als „Konto“ bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.
- (3) Zur Nutzung des Online Banking gelten die mit der Bank gesondert vereinbarten Verfügungsmitte.

### 2. Voraussetzungen zur Nutzung des Online Banking

- (1) Der Teilnehmer kann das Online Banking nutzen, wenn die Bank ihn authentifiziert hat.
- (2) Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechnete Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).
- (3) Authentifizierungselemente sind
  - Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer PIN)
  - Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern TAN) die den Besitz des Teilnehmers nachweisen, wie die girocard mit TAN-Generator oder das mobile Endgerät, oder
  - Seinsselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).
- (4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinsselements an die Bank übermittelt.

### 3. Zugang zum Online Banking

- (1) Der Teilnehmer erhält Zugang zum Online Banking der Bank, wenn
  - er seine individuelle Teilnehmererkennung (z. B. Kontonummer, Anmelde-name) angibt und
  - er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
  - keine Sperre des Zugangs (siehe Nummern 8.1 und 9 dieser Bedingungen) vorliegt.Nach Gewährung des Zugangs zum Online Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge erteilt werden.
- (2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z. B. zum Zweck der Änderung der Anschrift des Kunden) fordert die Bank den Teilnehmer auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Online Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kontoinhabers und die Kontonummer sind für den vom Teilnehmer genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Zahlungsdaten (§ 1 Absatz 26 Satz 2 ZAG).

### 4. Aufträge

#### 4.1 Auftragserteilung

Der Teilnehmer muss einem Auftrag (zum Beispiel Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (zum Beispiel Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden.

Die Bank bestätigt mittels Online Banking den Eingang des Auftrags.

#### 4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines 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 Widerrufsmöglichkeit im Online Banking ausdrücklich vor.

### 5. Bearbeitung von Aufträgen durch die Bank

- (1) Die Bearbeitung der 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 oder im „Preis- und Leistungsverzeichnis“ angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Online-Banking-Seite der Bank oder „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.

- (2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
  - Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1 dieser Bedingungen).
  - Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (zum Beispiel Wertpapierorder) liegt vor.
  - Das Online-Banking-Datenformat ist eingehalten.
  - Das gesondert vereinbarte Online-Banking-Verfügungsmitte ist nicht überschritten (vgl. Nummer 1 Absatz 3 dieser Bedingungen).
  - Die weiteren Ausführungsbedingungen 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 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 Auftrag nicht ausführen. Sie wird den Teilnehmer hierüber mittels Online Banking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

### 6. Information des Kunden über Online-Banking-Verfügungen

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

### 7. Sorgfaltspflichten des Teilnehmers

#### 7.1 Schutz der Authentifizierungselemente

- (1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummer 3 und 4 dieser Bedingungen).
- (2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:
  - (a) Wissenselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere
    - nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden,
    - nicht außerhalb des Online Banking in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben werden,
    - nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
    - nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinsselements (z. B. mobiles Endgerät mit Anwendung für das Online Banking und Fingerabdrucksensor) dient.
  - (b) Besitzelemente, wie z. B. die girocard mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
    - sind die girocard mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
    - ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können,
    - ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für das Online Banking (z. B. Online-Banking-App, Authentifizierungs-App) nicht nutzen können,
    - ist die Anwendung für das Online Banking (z. B. Online-Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons),
    - dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben werden und
    - muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das On-

line Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online Banking des Teilnehmers aktivieren.

- (c) Seinelemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinelemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online Banking genutzt wird, Seinelemente anderer Personen gespeichert, ist für das Online Banking das von der Bank ausgegebene Wissensselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinelement.
- (3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (zum Beispiel Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.
- (4) Die für das mobile-TAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Online Banking nicht mehr nutzt.
- (5) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 4 darf der Teilnehmer seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden (siehe Nummer 1 Absatz 1 Sätze 3 und 4 dieser Bedingungen). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

## 7.2 Sicherheitshinweise der Bank

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

## 7.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (zum Beispiel mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

## 8. Anzeige- und Unterrichtungspflichten

### 8.1 Sperranzeige

- (1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder
  - die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements
- fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.
- (2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.
- (3) Hat der Teilnehmer den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

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

Der Kunde 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 dieser Bedingungen,

- den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
- seine Authentifizierungselemente zur Nutzung des Online-Banking.

### 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 der Authentifizierungselemente des Teilnehmers dies rechtfertigen oder
  - der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.
- (2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

### 9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

### 9.4 Automatische Sperre eines chip-basierten Besitzelements

- (1) Eine Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur falsch eingegeben wird.
- (2) Ein TAN-Generator als Bestandteil einer Chipkarte, 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 Besitzelemente 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.

## 9.5 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Kunden verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleiters oder des Zahlungsauslösedienstleiters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Bank wird den Kunden über eine solche Zugangsverweigerung auf dem vereinbarten Weg unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Bank die Zugangssperre auf. Hierüber unterrichtet sie den Kunden unverzüglich.

## 10. Haftung

### 10.1 Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Bank bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft.)

### 10.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

#### 10.2.1 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 Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.
- (2) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn
- es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
  - der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleiters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleiters ausgelagert wurden, verursacht worden ist.
- (3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach
- Nummer 7.1 Absatz 2,
  - Nummer 7.1 Absatz 4,
  - Nummer 7.3 oder
  - Nummer 8.1 Absatz 1
- dieser Bedingungen verletzt hat.
- (4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen oder Sein (siehe Nummer 2 Absatz 3 dieser Bedingungen).
- (5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.
- (6) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.
- (7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.
- (8) Ist der Kunde kein Verbraucher, gilt ergänzend Folgendes:
- Der Kunde haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
  - Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

### 10.2.2 Haftung des Kunden bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige

Beruhend nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

### 10.2.3 Haftung 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.

## Teil B: InfoManager

### 1. Hinterlegung von Dokumenten, Verzicht auf postalischen Versand

- (1) Die Bank stellt dem Teilnehmer alle Dokumente, Mitteilungen und Erklärungen (im Nachfolgenden „Dokumente“ genannt) wie z. B. AGB-Änderungen, Mitteilungen über Zinssatzänderungen und Abrechnungen im InfoManager zur Verfügung, soweit nicht ausdrücklich Schriftform vorgeschrieben ist oder ein Wahlrecht zum Erhalt in schriftlicher Form besteht. Der Teilnehmer kann die im InfoManager hinterlegten Dokumente ansehen, ausdrucken und herunterladen.
- (2) Der Teilnehmer verzichtet ausdrücklich auf den postalischen Versand der für das Depot/Konto in den InfoManager eingestellten Dokumente.
- (3) Die Bank behält sich vor, Dokumente postalisch bzw. auf andere Weise dem Teilnehmer zur Verfügung zu stellen, wenn dies gesetzliche Vorgaben erforderlich machen oder es aufgrund anderer Umstände unter Berücksichtigung der Anlegerinteressen zweckmäßig erscheint, weil z. B. der InfoManager zeitweise nicht zur Verfügung steht. Die Bank behält sich vor, die Auswahl der in den InfoManager einzustellenden Dokumente zu ändern.

### 2. Kontrollpflicht, Information des Teilnehmers

- (1) Der Teilnehmer ist verpflichtet, den InfoManager auf den Eingang neuer Dokumente zu kontrollieren, die hinterlegten Dokumente abzurufen sowie deren Inhalt zu überprüfen. Die Kontrolle ist regelmäßig und zeitnah, insbesondere jedoch dann vorzunehmen, wenn aufgrund eines zuvor erteilten Auftrages mit der Einstellung neuer Dokumente zu rechnen ist. Eventuelle Unstimmigkeiten sind der Bank unverzüglich anzuzeigen.
- (2) Die Bank wird den Teilnehmer bei Einstellung eines neuen Dokuments per E-Mail hierüber informieren, soweit der Bank eine aktuelle E-Mail-Adresse des Teilnehmers vorliegt. Diese E-Mail dient jedoch lediglich der Information und entbindet den Teilnehmer nicht von seiner Kontrollpflicht.
- (3) Dokumente, die dem Teilnehmer im InfoManager hinterlegt werden, gelten mit Einstellung und der Möglichkeit des Abrufs als zugegangen.

### 3. Verfügbarkeit, Unveränderbarkeit von Dokumenten, Haftung

- (1) Der Teilnehmer nimmt zur Kenntnis, dass die Verfügbarkeit des InfoManager aufgrund von Störungen von Netzwerk oder Telekommunikationsverbindungen, höherer Gewalt, aufgrund von für den reibungslosen Betriebsablauf erforderlichen Wartungsarbeiten oder sonstiger Umstände eingeschränkt oder

zeitweise ausgeschlossen sein kann.

- (2) Die in den InfoManager eingestellten Dokumente werden dem Teilnehmer im PDF-Format zur Verfügung gestellt. Die Bank garantiert die Unveränderbarkeit der Daten, sofern die Daten im InfoManager gespeichert oder aufbewahrt werden. Werden Dokumente außerhalb des InfoManager gespeichert, aufbewahrt oder in veränderter Form in Umlauf gebracht, wird die Bank hierfür keine Haftung übernehmen.
- (3) Die Anerkennung der im InfoManager gespeicherten Dokumente durch Steuer- oder Finanzbehörden kann durch die Bank nicht gewährleistet werden. Eine vorherige Erkundigung beim zuständigen Finanzamt obliegt dem Teilnehmer.

### 4. Dauer der Hinterlegung

Im InfoManager werden die Dokumente des laufenden sowie des vorherigen Kalenderjahres vorgehalten. Jeweils zum Kalenderjahreswechsel wird die Bank die Dokumente des vorvergangenen Jahres automatisch und ohne zusätzliche Mitteilung an den Teilnehmer aus dem InfoManager entfernen.

### 5. Kündigung, Beendigung der Geschäftsbeziehungen

- (1) Der Teilnehmer kann ohne Angabe von Gründen die Nutzung des InfoManager jederzeit kündigen. Ab Zugang der Kündigung zuzüglich einer angemessenen Bearbeitungszeit werden alle Dokumente entgeltpflichtig per Post an die vom Teilnehmer angegebene Adresse versendet.
- (2) Die Bank kann die Nutzung des InfoManager mit einer Frist von zwei Monaten kündigen. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt hiervon unberührt. Sämtliche nach Wirksamwerden der Kündigung erstellten Dokumente werden gemäß den Allgemeinen Geschäftsbedingungen und den Sonderbedingungen der Fondsdot Bank GmbH dem Teilnehmer postalisch zugesandt.
- (3) Der Teilnehmer verpflichtet sich, bis zum Wirksamwerden der Kündigung bzw. zur Beendigung der Geschäftsbeziehung alle im InfoManager gespeicherten Dokumente zu kontrollieren und diese eventuell auszudrucken oder abzuspeichern. Eine Verpflichtung zum nachträglichen unentgeltlichen Versand von den zu diesem Zeitpunkt in den InfoManager eingestellten Dokumenten besteht nicht.

## Teil C: Schlussbestimmungen

### 1. Kommunikation und technische Anforderungen

- (1) Zur Durchführung von Bankgeschäften über das Online Banking Portal benötigt der Teilnehmer eine eigene Zugangskennung und eine Zugangs-PIN. Nach Eingabe seiner Transaktionsdaten erhält der Teilnehmer bei Nutzung des sogenannten Push TAN Verfahrens eine TAN via APP angezeigt, welche zur Authentifizierung seiner Transaktion gültig ist. Für die Generierung und Anzeige einer einmaligen TAN wird die Fondsdot Bank Push TAN APP benötigt. Diese kann der Teilnehmer auf einem Android oder IOS betriebenen Gerät installieren.

Die Freischaltung der APP für seine Konten muss der Teilnehmer mit dem per Post zugesandten Aktivierungscode veranlassen. Für jede Zugangskennung kann nur ein mobiles Gerät registriert werden.

- (2) Im Falle vermuteten oder tatsächlichen Betrugs oder bei Sicherheitsrisiken wird die Bank den Teilnehmer per Post unterrichten.

### 2. Änderungen der Besondere Bedingungen

Für Änderungen dieser Besondere Bedingungen gilt Ziffer 1.2 der AGB.