FONDSDEPOT BANK

# Depotauftrag Freischaltung für das Fondsbanking und den InfoManager

Formulareingabe löschen

**Dieses Formular kann nur bearbeitet werden, wenn dieses schriftlich vorliegt.**

**Depot-/Konto-Nr.**

**Dieses Formular soll außerdem für die folgenden Depots (z. B. VL-Depots) bzw. Konten gelten:**

**Nr.** **Nr.**

**1. Depot-/Kontoinhaber** bzw. ☐ **1. gesetzlicher Vertreter**

☐ Frau ☐ Herr ☐ Firma

Name | Vorname/n

Straße | Nummer

PLZ | Ort | Bereits vorhandene Zugangskennung im Rahmen des Fondsbanking bzw. InfoManager

**2. Depot-/Kontoinhaber** bzw. ☐ **2. gesetzlicher Vertreter**

☐ Frau ☐ Herr

Name | Vorname/n

Straße | Nummer

PLZ | Ort | Bereits vorhandene Zugangskennung im Rahmen des Fondsbanking bzw. InfoManager

**Bevollmächtigter** (bitte nachfolgend angeben)

☐ **mit Vollmacht zu Lebzeiten und über den Tod hinaus** ☐ **ist vertretungsberechtigte Person der oben genannten Firma**

**Hinweis:**
**Mit diesem Formular „Depotauftrag Freischaltung für das Fondsbanking und den InfoManager" ist keine Bevollmächtigung möglich. Bitte erteilen Sie, sofern noch nicht geschehen, mithilfe des entsprechenden Formulars eine Vollmacht. Dieses Formular stellt Ihnen die Fondsdepot Bank GmbH gerne zur Verfügung.**

☐ Frau ☐ Herr

Name | Vorname/n

Straße | Nummer

PLZ | Ort | Bereits vorhandene Zugangskennung im Rahmen des Fondsbanking bzw. InfoManager

## Fondsbanking

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

☐ **Gleichzeitig beantrage/n ich/wir die Transaktionsberechtigung für o. g. Depots. Hierfür ist die Angabe der Mandatsreferenz-Nr. bzw. Erteilung eines neuen Mandats durch Angabe der Bankverbindung auf Seite 2/2 zwingend erforderlich.**

**Hinweis:** Eine Freischaltung der Transaktionsberechtigung ist ausschließlich für das Fondsdepot Bank Standard-Depot möglich. Bei Fragen wenden Sie sich bitte an Ihren Berater.

Bitte füllen Sie die oben stehenden Adressangaben vollständig aus. An die jeweils angegeben Adresse werden Ihre Zugangs- sowie Authentifizierungsdaten und mit gesonderter Post Ihre persönliche Identifikationsnummer (im Nachfolgenden „PIN" genannt) gesandt.

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

**Bitte zurücksenden an: Fondsdepot Bank GmbH, 95025 Hof**



1. Ausdruck (Original) für die Bank/2. Ausdruck bzw. Kopie für Ihre Unterlagen

FONDSDEPOT BANK

**1. Depotinhaber**

Name | Vorname/n | **Depot-/Konto-Nr.**

Straße | Nummer | PLZ | Ort

## Einrichtung Referenzbankverbindung/Erteilung eines Mandats für SEPA-Basislastschriften zu dem/den Depot/s

**Zu meiner/unserer Sicherheit werden Sie 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 oder der Transfer des Verkaufserlöses gemäß meiner/unserer Weisung auf meine/unsere genannte Referenzbankverbindung erfolgen soll.**

## Bankverbindung/SEPA-Lastschriftmandat

Sofern Sie bereits eine Mandatsreferenz besitzen und der Lastschrifteinzug von dieser Referenzbankverbindung eingezogen werden soll, so ist die Angabe der Mandatsreferenz-Nr. ausreichend. **Mandatsreferenz-Nr.**

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

**Hinweis:**
- 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. nach dem letzten Lastschrifteinzug 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 Girokontoinhaber/s (falls abweichend von dem/den Depotinhaber/n)

## InfoManager

Der InfoManager ist ein elektronisches Postfach, in dem für den/die Depot-/Kontoinhaber bestimmte Dokumente, die im Rahmen der Depotführung produziert werden (z. B. Depot-/Kontoauszüge, Ausschüttungsmitteilungen, Kosteninformationen), zum Download hinterlegt werden.

**Ich/Wir beauftrage/n die Bank zur Freischaltung des InfoManager. Bitte veranlassen Sie die Freischaltung für o. g. Depots/Konten.**

Für die Freischaltung des InfoManager erhält der Depotinhaber mit der Post die Zugangs- sowie Authentifizierungsdaten und mit gesonderter Post eine persönliche Identifikationsnummer (im Nachfolgenden „PIN" genannt) für das/die auf Seite 1 genannte/n Depot/s. Zur Änderung der PIN benötigen Sie eine generierte TAN.

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

E-Mail 1 | E-Mail 2

**Die mit diesen Unterlagen zur Verfügung gestellten Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager habe/n ich/wir gelesen und erkenne/n ich/wir unverändert an. Mit der Freischaltung des o. g. Bevollmächtigten erkläre/n ich/wir mich/uns hiermit einverstanden.**

**Hinweis:** Es sind die Unterschriften aller Depot-/Kontoinhaber bzw. gesetzlichen Vertreter erforderlich.

✗ Unterschrift 1. Depotinhaber bzw. 1. gesetzlicher Vertreter

✗ Unterschrift 2. Depotinhaber bzw. 2. gesetzlicher Vertreter

Ort, Datum

✗ Unterschrift Bevollmächtigter

**Bitte zurücksenden an: Fondsdepot Bank GmbH, 95025 Hof**

# Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager (Stand 1. Juni 2019)

Im nachfolgenden wird der Begriff Fondsbanking durch Online Banking ersetzt.

## Teil A: Online Banking

### 1. Leistungsangebot

(1) Der Konto-/Depotinhaber 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. Sie sind zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrages einen Zahlungsauslösedienst gemäß § 1 Absatz 33 Zahlungsdiensteaufsichtsgesetz und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienst gemäß § 1 Absatz 34 Zahlungsdiensteaufsichtsgesetz zu nutzen.
(2) Konto-/Depotinhaber 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 Verfügungslimite.

### 2. Voraussetzungen zur Nutzung des Online Banking

Der Teilnehmer benötigt für die Nutzung des Online Banking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4). Statt eines Personalisierten Sicherheitsmerkmals kann auch ein biometrisches Merkmal des Teilnehmers zum Zwecke der Authentifizierung bzw. Autorisierung vereinbart werden.

**2.1 Personalisierten Sicherheitsmerkmale**

Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die die Bank dem Teilnehmer zum Zwecke der Authentifizierung bereitstellt. Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind beispielsweise
– die persönliche Identifikationsnummer (PIN),
– einmal verwendbare Transaktionsnummern (TAN),
– der Nutzungscode für die elektronische Signatur.

**2.2 Authentifizierungsinstrumente**

Authentifizierungsinstrumente sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurden und die vom Teilnehmer zur Erteilung eines Online-Banking-Auftrags verwendet werden. Insbesondere mittels folgender Authentifizierungsinstrumente kann das Personalisierte Sicherheitsmerkmal (z. B. TAN) dem Teilnehmer zur Verfügung gestellt werden:
– PIN-Brief,
– Liste mit einmal verwendbaren TAN,
– TAN-Generator, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist,
– Online-Banking-App auf einem mobilen Endgerät (zum Beispiel Mobiltelefon) zum Empfang oder Erzeugung von TAN,
– mobiles Endgerät (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
– Chipkarte mit Signaturfunktion oder
– sonstiges Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden.

### 3. Zugang zum Online Banking

Der Teilnehmer erhält Zugang zum Online Banking, wenn
– dieser die Kontonummer oder seine individuelle Teilnehmerkennung und seine PIN oder elektronische Signatur übermittelt oder sein biometrisches Merkmal eingesetzt hat,
– die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
– keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.

Nach Gewährung des Zugangs zum Online Banking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.
Die Sätze 1 und 2 gelten auch, wenn der Teilnehmer Zahlungsaufträge über einen Zahlungsauslösedienst auslöst und Zahlungskontoinformationen über einen Kontoinformationsdienst anfordert (siehe Nummer 1 Absatz 1 Satz 3).

### 4. Online-Banking-Aufträge

**4.1 Auftragserteilung und Autorisierung**

Der Teilnehmer muss Online-Banking-Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit mit dem von der Bank bereit gestellten Personalisierten Sicherheitsmerkmal (z. B. TAN) oder mit dem vereinbarten biometrischen Sicherheitsmerkmal autorisieren und der Bank mittels Online Banking übermitteln. Die Bank bestätigt mittels Online Banking den Eingang des Auftrags. Die Sätze 1 und 2 gelten auch, wenn der Teilnehmer einen Zahlungsauftrag über einen Zahlungsauslösedienst (siehe Nummer 1 Absatz 1 Satz 3) auslöst und übermittelt.

**4.2 Widerruf von Aufträgen**

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

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

(1) Die Bearbeitung der Online-Banking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung) auf der Online-Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis" bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank angegebenen oder im „Preis- und Leistungsverzeichnis" bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis" der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.
(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- Der Teilnehmer hat den Auftrag autorisiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (zum Beispiel Wertpapierorder) liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.
- Die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Online-Banking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.
(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen. Sie wird dem 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 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 über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle (zum Beispiel Internetadresse) herzustellen. Zur Auslösung eines Zahlungsauftrags und zum Abruf von Informationen über ein Zahlungskonto kann der Teilnehmer die technische Verbindung zum Online Banking auch über einen Zahlungsauslösedienst beziehungsweise einen Kontoinformationsdienst (siehe Nr. 1 Absatz 1 Satz 3) herstellen.

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

(1) Der Teilnehmer hat:
- seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten sowie
- sein Authentifizierungsinstrument (siehe 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 der Kenntnis des dazugehörigen Personalisierten Sicherheitsmerkmals das Online-Banking-Verfahren missbräuchlich nutzen. Die Geheimhaltungspflicht bezüglich der Personalisierten Sicherheitsmerkmale nach Satz 1 gilt nicht, wenn der Teilnehmer diese zur Erteilung eines Zahlungsauftrags oder zum Abruf von Informationen über ein Zahlungskonto an den von ihm ausgewählten Zahlungsauslösedienst beziehungsweise Kontoinformationsdienst übermittelt (siehe Nummer 1 Absatz 1 Satz 3).
(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:
- Das Personalisierte Sicherheitsmerkmal darf nicht ungesichert elektronisch gespeichert werden.
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das Personalisierte Sicherheitsmerkmal darf nicht per E-Mail weitergegeben werden.
- Das Personalisierte Sicherheitsmerkmal (z. B. PIN) darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung zum Beispiel eines Auftrags oder der Aufhebung einer Sperre nicht mehr als eine TAN verwenden.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (zum Beispiel Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.

**7.3 Sicherheithinweis der Bank**

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

**7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten**

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

## 8. Anzeige- und Unterrichtungspflichten

**8.1 Sperranzeige**

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder eines seiner Personalisierten Sicherheitsmerkmale

fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

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

(3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt

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

## 9. Nutzungssperre

**9.1 Sperre auf Veranlassung des Teilnehmers**

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1,

- den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument.

**9.2 Sperre auf Veranlassung der Bank**

(1) Die Bank darf den Online-Banking-Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.

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

**9.3 Aufhebung der Sperre**

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

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

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

(2) Ein TAN-Generator 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 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, fehlerhaft oder verspätet ausgeführten Online-Banking-Verfügung**

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

**10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung eines Personalisierten Sicherheitsmerkmals oder eines Authentifizierungsinstruments**

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

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungsinstruments, haftet der Kontoinhaber 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 Kontoinhaber 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 Authentifizierungsinstruments vor dem nicht autorisierten Zahlungsvorgangzu bemerken, oder
- der Verlust des Authentifizierungsinstruments durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters 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 Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere 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 (siehe Nummer 8.1 Absatz 1),
- das Personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe Nummer 7.2 Absatz 2 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1),
- das Personalisierte Sicherheitsmerkmal per E-Mail weitergegeben hat (siehe Nummer 7.2 Absatz 2 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 4. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2 5. Spiegelstrich),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Online Banking nutzt (siehe Nummer 7.2 Absatz 2 6. Spiegelstrich).

(4) Abweichend von den Absätzen 1 und 3 ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt hat, obwohl die Bank zur starken Kundenauthentifizierung nach § 68 Absatz 4 Zahlungsdiensteaufsichtsgesetz verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, das der Teilnehmer weiß, z. B. PIN), Besitz (etwas, das der Teilnehmer besitzt, z. B. TAN-Generator) oder Inhärenz (etwas, das der Teilnehmer ist, z. B. Fingerabdruck).

(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 Kontoinhaber 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 Kontoinhaber kein Verbraucher, gilt ergänzend Folgendes:

- Der Kontoinhaber 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 Depotinhabers bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige**

Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen 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 Depotinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

**10.2.3 Haftung der Bank ab der Sperranzeige**

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

**10.2.4 Haftungsausschluss**

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

## 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 Depotabrechnungen im InfoManager zur Verfügung, soweit nicht ausdrücklich Schriftform vorgeschrieben ist. 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 in den InfoManager eingestellten Dokumente.
(3) Die Bank behält sich vor, Dokumente postalisch bzw. auf andere Weise dem Teilnehmern 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. 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 Teilnehmern 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 Allgemeine Geschäftsbedingungen und den Sonderbedingungen der Fondsdepot Bank GmbH dem Teilnehmern 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 Fondsdepot 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 für die Nutzung des Fondsbanking und des InfoManager gilt Ziffer 1.2 der AGB.