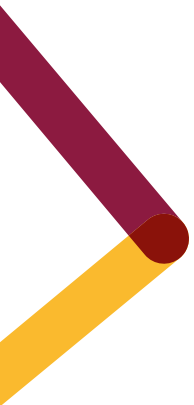
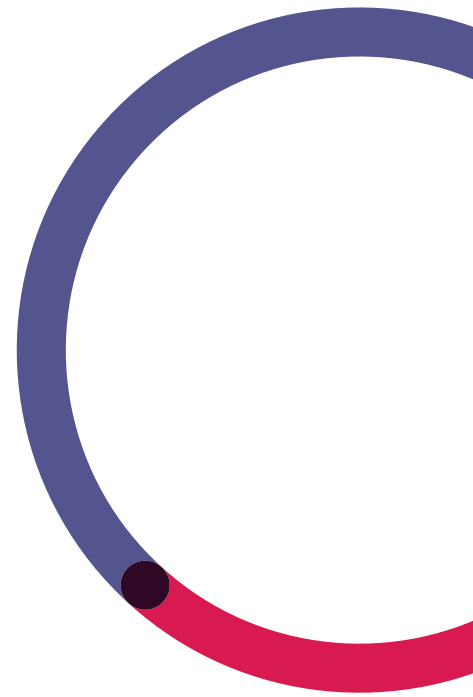


# Sonderbedingungen für das Online-Banking

03/2016



## 1. Leistungsangebot und Definitionen

- 1.1** Der Konto-/Depotinhaber kann Bankgeschäfte mittels Online-Banking in dem von der ABN AMRO Bank N.V., Frankfurt Branch (im Folgenden „**Bank**“ genannt) angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Online-Banking abrufen. „**Online-Banking**“ bezeichnet die verschlüsselte Seite, zu der der Konto-/Depotinhaber über die Webseite der Bank gemäß Nummer 4 dieser Sonderbedingungen Zugang erhält.
- 1.2** Begriffe, die in den Allgemeinen Geschäftsbedingungen oder in Sonderbedingungen definiert und verwendet werden, haben für diese Sonderbedingungen für das Online-Banking die gleiche Bedeutung.

## 2. Voraussetzungen zur Nutzung des Online-Bankings

- 2.1** Der Konto-/Depotinhaber benötigt für die Abwicklung von Bankgeschäften mittels Online-Banking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und für bestimmte Aufträge und Aktivitäten gegebenenfalls das vereinbarte Authentifizierungsinstrument, um sich gegenüber der Bank als berechtigter Konto-/Depotinhaber auszuweisen (vgl. Nummer 4) und Aufträge zu autorisieren (vgl. Nummer 5).
- a. „**Personalisierte Sicherheitsmerkmale**“ sind
- die persönliche Nutzer-ID (wie in Nummer 3 definiert) und
  - das persönliche Kennwort (wie in Nummer 3 definiert).
- b. „**Authentifizierungsinstrument**“ ist jeweils die gegebenenfalls erforderliche mTAN (mobile Transaktionsnummer), die die Bank dem Kunden per SMS mittels eines mobilen Endgerätes (z. B. Mobiltelefon mit deutscher Mobilfunknummer) zur Ausführung bestimmter Aufträge mitteilt.
- 2.2** Im Falle von Gemeinschaftskonten/-depots verwenden die Konto-/Depotinhaber ausschließlich die ihnen jeweils zugeteilte Nutzer-ID und das von ihnen jeweils gewählte Kennwort. Die Konto-/Depotinhaber eines Gemeinschaftskontos/-depots erhalten getrennte Nutzer-IDs und müssen verschiedene Kennwörter wählen.
- 2.3** Für die Nutzung des Online-Bankings benötigt der Konto-/Depotinhaber einen Internetzugang. Dieser wird nicht von der Bank bereitgestellt. Um das Online-Banking nutzen zu können, benötigt der Konto-/Depotinhaber zurzeit einen Browser, der eine SSL-Verschlüsselung unterstützt. Die Bank behält sich vor, den Verschlüsselungsstandard und/oder die technischen Voraussetzungen jederzeit zu ändern, um die notwendige Sicherheit des Online-Bankings zu gewährleisten. Über eine Änderung des Verschlüsselungsstandards und/oder der technischen Voraussetzungen wird die Bank den Konto-/Depotinhaber rechtzeitig informieren.
- 2.4** Die sonstigen technischen Voraussetzungen für die Nutzung des Online-Bankings werden im Internet unter [www.moneyou.de](http://www.moneyou.de) (die „**Webseite der Bank**“) beschrieben.

## 3. Konto-/Depoteröffnungsverfahren

Das Konto-/Depoteröffnungsverfahren eines zukünftigen Konto-/Depotinhabers beinhaltet insbesondere folgende Schritte:

- Der Antragsteller stellt unter Auswahl seines persönlichen Kennwortes (das „**Kennwort**“) einen Antrag auf Konto-/Depoteröffnung auf der Webseite der Bank.
- Der Antragsteller bestätigt durch Anklicken der Kontrollkästchen, dass er alle Voraussetzungen zur Eröffnung eines Kontos/Depots erfüllt (z. B. mindestens 18 Jahre alt; ständiger Wohnsitz in Deutschland; Inhaber eines deutschen Girokontos; Verfügbarkeit eines Mobiltelefons und einer E-Mail-Adresse; Antragsteller ist keine politisch exponierte Person.) Die Bank führt Depots nicht für Personen mit US-Bezug. US-Bezug ist insbesondere bei Personen gegeben, die in den USA steuerpflichtig sind oder die eine US-amerikanische Staatsangehörigkeit (einschließlich Doppelstaatsbürgerschaft), eine US Green Card, einen US-Wohnsitz, eine US-Versandadresse oder eine US-Telefonnummer haben. Liegt ein US-Bezug nach den genannten Kriterien vor oder ergibt sich ein US-Bezug im Laufe der Geschäftsbeziehung, ist dies der Bank unverzüglich mitzuteilen und, sofern bereits eine Konto-/Depotbeziehung besteht, diese aufzulösen (siehe Nr. 14.4 der Sonderbedingungen für Wertpapiergeschäfte).
- Der Antragsteller erklärt sich durch Anklicken der Kontrollkästchen mit der Einbeziehung und Geltung aller aufgeführten rechtlichen Bestimmungen einverstanden und bestätigt darüber hinaus auf dem Informationsbogen für Einleger durch Anklicken des Kontrollkästchens, diesen erhalten zu haben.
- Nach Übermittlung der Kundendaten generiert das System der Bank einen individuellen 10-stelligen Benutzernamen (die „**Nutzer-ID**“), welcher zusammen mit weiteren Anweisungen zur Konten-/Depotaktivierung in einer Willkommensnachricht an den zukünftigen Konto-/Depotinhaber per E-Mail versandt wird.
- Der Antragsteller kann sich mit den Personalisierten Sicherheitsmerkmalen auf den dazu vorgesehenen Masken der Webseite der Bank einloggen, um seine Konto-/Depotnummer und weitere Anweisungen und Statusmeldungen zur Konten-/Depotaktivierung zu erfahren.
- Der Antragsteller führt das PostIdent-Verfahren oder Videoident-Verfahren zur Feststellung seiner Identität durch (im Falle eines Gemeinschaftskontos/-depots führen beide Konto-/Depotinhaber das PostIdent-Verfahren oder Videoident-Verfahren durch).
- Der Antragsteller bestätigt die Kenntnisnahme und sein Einverständnis mit den zugrundeliegenden Allgemeinen Geschäftsbedingungen, Sonderbedingungen sowie sonstigen Bedingungen durch den Abschluss des PostIdent-Verfahrens bzw. des Videoident-Verfahrens und Erstüberweisung auf das Moneyou Konto.
- Die Bank prüft die von dem Antragsteller angegebenen Daten.
- Der Antragsteller muss sich innerhalb von 60 Tagen nach Zusendung der Nutzer-ID erstmals im Online-Banking einloggen und alle weiteren zur Konto- und Depoteröffnung erforderlichen Schritte durchgeführt haben. Zu diesen Schritten zählen insbesondere eine

erste Einzahlung von seinem Referenzkonto auf das Moneyou Tagesgeldkonto und die Durchführung des PostIdent-Verfahrens oder des VideoIdent-Verfahrens. Zu weiteren Verfügungen über das Moneyou Tagesgeldkonto und Depot ist der Konto-/Depotinhaber bis zur Annahme des Konto-/Depoteröffnungsantrags durch die Bank nicht befugt. Erfolgt die Durchführung der für die Kontoeröffnung erforderlichen Schritte, wie z. B. das erstmalige Einloggen im Online-Banking, die Einzahlung auf das Moneyou Tagesgeldkonto oder die Durchführung des PostIdent-Verfahrens oder VideoIdent-Verfahrens nicht fristgerecht, so ist der Antrag als nicht gestellt anzusehen.

- Der Antragsteller erhält nach positivem Ergebnis der Prüfung eine Annahmestätigung per E-Mail von der Bank und die Bank schaltet das Konto/Depot zur Nutzung frei. Im Falle einer Ablehnung des Kontoeröffnungsantrags des Antragstellers wird eine etwaige bereits geleistete Einzahlung auf das Referenzkonto zurückgebucht und der Antragsteller entsprechend informiert. Die Bank ist in diesem Fall nicht zur Zahlung von Zinsen verpflichtet.

Ein Kontoführungs- und Depotvertrag kommt nur zustande, wenn der Antragsteller alle Voraussetzungen erfüllt hat und er die Annahmestätigung von der Bank erhalten hat. Die Bank behält sich das Recht vor, Konto-/Depoteröffnungsanträge ohne Angabe von Gründen abzulehnen und die Voraussetzungen für einen Konto-/Depoteröffnungsantrag zu ändern.

## 4. Zugang zum Online-Banking

**4.1** Der Konto-/Depotinhaber erhält Zugang zum Online-Banking, wenn

- der Konto-/Depotinhaber seine Nutzer-ID und seine Personalisierten Sicherheitsmerkmale in die auf der Webseite der Bank vorgesehenen Masken übermittelt hat;
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs vorliegt.

**4.2** Nach Gewährung des Zugangs zum Online-Banking kann der Konto-/Depotinhaber Informationen abrufen oder Aufträge erteilen.

**4.3** Der Konto-/Depotinhaber kann sein Kennwort und seine Nutzer-ID nach einem Zugang zum Online-Banking ändern.

## 5. Online-Banking-Aufträge

### 5.1 Auftragserteilung und Autorisierung

Der Konto-/Depotinhaber muss Online-Banking-Aufträge (z. B. Überweisungen an das Referenzkonto) zu deren Wirksamkeit mit den vereinbarten Personalisierten Sicherheitsmerkmalen und soweit von der Bank gefordert, dem Authentifizierungsinstrument autorisieren und der Bank mittels Online-Banking übermitteln. Die Bank bestätigt mittels

Online-Banking den Eingang des Auftrags. Schriftliche Aufträge oder Aufträge in anderer Weise als über das Online-Banking werden von der Bank nicht akzeptiert.

### 5.2 Widerruf von Aufträgen

Der Widerruf eines Online-Banking-Auftrags ist nach Zugang nicht mehr möglich.

### 5.3 Speichern von Aufträgen

Im Rahmen des Online-Bankings erteilte Aufträge wird die Bank, während der Konto-/Depotinhaber auf der persönlichen Online-Banking-Seite eingeloggt ist, so zur Verfügung stellen, dass sie von dem Konto-/Depotinhaber ausgedruckt oder heruntergeladen werden können. Zu einem späteren Zeitpunkt muss die Bank Aufträge nicht in elektronischer oder sonstiger Form dem Konto-/Depotinhaber zur Verfügung stellen.

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

**6.1** 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 darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

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

- a. der Konto-/Depotinhaber hat sich mit seinen personalisierten Sicherheitsmerkmalen und, falls von der Bank verlangt, dem Authentifizierungsinstrument legitimiert,
- b. die Berechtigung des Konto-/Depotinhabers für die jeweilige Auftragsart liegt vor,
- c. das Online-Banking-Datenformat ist eingehalten,
- d. die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Konto-/depotdeckung gemäß den Bedingungen für den Überweisungsverkehr und den Sonderbedingungen für Wertpapiergeschäfte) 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 (z. B. Bedingungen für den Überweisungsverkehr und den Sonderbedingungen für Wertpapiergeschäfte) aus.

**6.3** Liegen die Ausführungsbedingungen nach Nummer 6.2 nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen und den Konto-/Depotinhaber über die Nichtausführung und – soweit möglich – über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt

haben, berichtet werden können, mittels Online-Banking eine Information zur Verfügung stellen.

## 7. Information des Konto-/Depotinhabers über Online-Banking-Verfügungen

Der Konto-/Depotinhaber erhält von der Bank jeweils nach Ende eines Kalenderjahres einen Konto-/Depotabschluss, der als Rechnungsabschluss dient. Der Konto-/Depotinhaber wird entsprechend über das Postfach oder an die von dem Kunden angegebene E-Mail-Adresse im Sinne von Nummer 8 informiert. Der Konto-/Depotabschluss (Rechnungsabschluss) ist im Online-Banking abrufbar. Die Bank erteilt dem Konto-/Depotinhaber keine Konto-/Depotauszüge in Druckform. Elektronische Übersichten über die getätigten Verfügungen sind mittels Online-Banking durch den Konto-/Depotinhaber jederzeit abrufbar und können heruntergeladen, gespeichert und ausgedruckt werden. Die Bank stellt dem Konto-/Depotinhaber im Rahmen des technisch Möglichen kontinuierlich Informationen über die Ausführung von Überweisungen online zum Abruf zur Verfügung.

## 8. Postfach

**8.1** Im Rahmen der Geschäftsbeziehung zwischen der Bank und dem Konto-/Depotinhaber gilt die Nutzung des elektronischen Postfachs (das „**Postfach**“) sowie die Versendung von E-Mails auf die von dem Kunden angegebene Kunden-E-Mail-Adresse (die „**Kunden-E-Mail-Adresse**“) als vereinbarter Kommunikationsweg. Nachrichten der Bank werden entweder an die Kunden-E-Mail-Adresse versandt oder in dem Postfach online zur Verfügung gestellt. Der Konto-/depotinhaber hat ferner die Möglichkeit, der Bank Anfragen und bestimmte Nachrichten über das Postfach zu senden.

**8.2** Der Konto-/Depotinhaber verzichtet durch die Nutzung des Postfachs und des Online-Bankings bzw. der Kunden-E-Mail-Adresse ausdrücklich auf den postalischen Versand aller Dokumente und Nachrichten durch die Bank in papiergebundener Form. Dokumente, die aufgrund rechtlicher Anforderungen von der Bank erteilt werden müssen, insbesondere Konto-/Depotauszüge und Konto-/Depotabschlüsse (Rechnungsabschlüsse), sowie Nachrichten betreffend den Geschäftsverkehr mit der Bank, werden dem Konto-/Depotinhaber daher grundsätzlich nur in elektronischer Form in das Postfach bzw. der Funktion „Konto-/Depotauszug“ bzw. „Konto-/Depotabschluss“ im Rahmen des Online-Bankings übermittelt und zum Abruf zur Verfügung gestellt. Die Bank ist berechtigt, dem Konto-/Depotinhaber die hinterlegten Dokumente und Nachrichten auf dem Postweg oder auf andere Weise zu übermitteln, wenn dies gesetzliche Vorgaben erforderlich machen oder die Bank dies aufgrund anderer Umstände (z. B. technischer Probleme) unter Berücksichtigung des Kontoinhaber-/Depotinhaberinteresses als zweckmäßig erachtet. Allgemeine Nachrichten z. B. in Bezug auf die Änderung der Zinssätze werden in aller Regel an die Kunden-E-Mail-Adresse versandt.

**8.3** Im Rahmen des Online-Banking an den Konto-/Depotinhaber übermittelte Dokumente und Nachrichten gelten mit der Bereitstellung und der Möglichkeit des Abrufs als zugegangen. Der Zugang gilt als am darauf folgenden Werktag bewirkt, wenn die Einstellung nach 18:00 Uhr oder an einem Tag erfolgt, der kein Geschäftstag ist.

**8.4** Der Konto-/Depotinhaber verpflichtet sich, regelmäßig, mindestens jedoch einmal pro Monat, das Postfach und die Nachrichten auf seiner Kunden-E-Mail-Adresse einzusehen. Er kontrolliert die auf die dort verwiesenen und im Online-Banking abrufbaren Dokumente auf Richtigkeit und Vollständigkeit. Beanstandungen sind der Bank unverzüglich, spätestens vor Ablauf von 6 Wochen nach Zugang der Dokumente gemäß Nummer 8.3 mitzuteilen.

**8.5** Die Bank garantiert die Unveränderlichkeit der Daten in dem Postfach, sofern die Daten innerhalb des Postfachs gespeichert und aufbewahrt werden. Werden Dokumente außerhalb des Postfachs bzw. der Funktion „Konto-/Depotauszug“ bzw. „Konto-/Depotabschluss“ gespeichert, aufbewahrt oder in veränderter Form in Umlauf gebracht, übernimmt die Bank hierfür keine Haftung.

**8.6** Die Bank speichert die in dem Postfach und unter der Funktion „Konto-/Depotauszug“ bzw. „Konto-/Depotabschluss“ enthaltenen Dokumente im Rahmen der gesetzlichen Aufbewahrungsfristen. Nach Ablauf dieser Frist kann die Bank die entsprechenden Dokumente und Nachrichten aus dem Postfach entfernen, ohne dass der Konto-/Depotinhaber hierüber eine gesonderte Nachricht erhält.

**8.7** Der Konto-/Depotinhaber kann der Bank Mitteilungen über die dazu vorgesehene Maske im Online-Banking, über das Postfach, per E-Mail an die auf der Webseite der Bank angegebene E-Mail-Adresse, postalisch an die auf der Webseite der Bank angegebene Anschrift der Bank oder telefonisch über die auf der Webseite der Bank angegebene Telefonnummer zukommen lassen.

## 9. Sorgfaltspflicht des Konto-/Depotinhabers

### 9.1 Technische Verbindung zum Online-Banking

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

### 9.2 Geheimhaltung und sichere Aufbewahrung der personalisierten Sicherheitsmerkmale und des gegebenenfalls vorhandenen Authentifizierungsinstrumentes

a. Der Konto-/Depotinhaber hat seine Personalisierten Sicherheitsmerkmale und das Authentifizierungsinstrument (siehe Nummer 2) geheim zu halten und nur über die auf der Webseite der Bank vorgesehenen Masken für den Zugang zum Online-Banking an diese zu übermitteln. Jede andere Person, die im Besitz der Personalisierten Sicherheitsmerkmale und von Authentifizierungsinstrumenten ist, kann das Online-Banking-Verfahren missbräuchlich nutzen.

- b. Insbesondere ist Folgendes zum Schutz der Personalisierten Sicherheitsmerkmale sowie des Authentifizierungsinstrumentes zu beachten:
- (i) Die Personalisierten Sicherheitsmerkmale (außer der Nutzer-ID) und das Authentifizierungsinstrument dürfen nicht elektronisch gespeichert werden (z. B. auf der von dem Konto-/Depotinhaber genutzten Hardware und Software (das „**Kundensystem**“)).
  - (ii) Bei Eingabe der Personalisierten Sicherheitsmerkmale und der Authentifizierungsinstrumente ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
  - (iii) Die Personalisierten Sicherheitsmerkmale und das Authentifizierungsinstrument dürfen nicht außerhalb der auf der Webseite der Bank vorgesehenen Masken für den Zugang zum Online-Banking eingegeben werden (z. B. nicht auf Online-Händlerseiten).
  - (iv) Die Personalisierten Sicherheitsmerkmale und das Authentifizierungsinstrument dürfen nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
  - (v) Die Nutzer-ID und das Kennwort sowie die Personalisierten Sicherheitsmerkmale und das Authentifizierungsinstrument dürfen nicht zusammen verwahrt werden.
  - (vi) Der Konto-/Depotinhaber darf zur Autorisierung z. B. eines Auftrages nicht mehr als eine mTAN verwenden.
  - (vii) Das Empfangsgerät, mit dem die mTAN empfangen wird (z. B. Mobiltelefon), darf nicht gleichzeitig für das Online-Banking benutzt werden.
  - (viii) Auf Veranlassung der Bank ist das Kennwort für den Zugang zum Online-Banking in unregelmäßigen Abständen, unabhängig hiervon wenigstens jedoch alle 6 Monate zu ändern.

### 9.3 Sicherheit des Kontoinhaber-/Depotinhabersystems

Der Konto-/Depotinhaber muss die Sicherheitshinweise auf der Webseite der Bank zum Online-Banking, insbesondere die Maßnahme zum Schutz des eingesetzten Kundensystems, beachten. Insbesondere muss der Konto-/Depotinhaber geeignete, dem aktuellen Sicherheitsstandard entsprechende Hard- und Software und die marktgängigen Sicherheitsmaßnahmen zum Schutz gegen Viren und anderen Missbrauch verwenden. Nach dem Einloggen durch Angabe der Personalisierten Sicherheitsmerkmale darf der Konto-/Depotinhaber seinen Rechner nicht unbeaufsichtigt lassen, wenn er sich vorher nicht aus dem Online-Banking wieder ausgeloggt hat.

### 9.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Konto-/Depotinhaber Daten aus seinem Online-Banking-Auftrag im Kundensystem oder über ein anderes Gerät des Konto-/Depotinhabers (z. B. Mobiltelefon) zur Bestätigung anzeigt, ist der Konto-/Depotinhaber verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

## 10. Anzeige- und Unterrichtungspflichten

### 10.1 Sperranzeige

- a. Stellt der Konto-/Depotinhaber die missbräuchliche Verwendung oder die nicht autorisierte Nutzung seiner Personalisierten Sicherheitsmerkmale oder seines Authentifizierungsinstrumentes fest, muss der Konto-/Depotinhaber die Bank hierüber unverzüglich gemäß Nummer 8.1 unterrichten (Sperranzeige). Der Konto-/Depotinhaber kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.
- b. Im Falle des Verlusts, des Diebstahls oder der missbräuchlichen oder sonstigen nicht autorisierten Nutzung des Empfangsgerätes zum Empfang von mTAN (z. B. Mobiltelefon) oder der SIM-Karte ist unverzüglich die Sperrung beim jeweiligen Mobilfunkbetreiber zu veranlassen.
- c. Der Konto-/Depotinhaber hat jeden Diebstahl oder Missbrauch der in a. oder b. genannten Sicherheitsmerkmale und Gegenstände unverzüglich bei der Polizei zur Anzeige zu bringen.
- d. Hat der Konto-/Depotinhaber den Verdacht, dass eine andere Person unberechtigt
  - (i) die Kenntnis seiner Personalisierten Sicherheitsmerkmale bzw. des Authentifizierungsinstrumentes erlangt hat oder
  - (ii) die Personalisierten Sicherheitsmerkmale bzw. das Authentifizierungsinstrument verwendet, muss er ebenfalls eine Sperranzeige abgeben. Der Konto-/Depotinhaber ist verpflichtet, sein Kennwort unverzüglich zu ändern, sobald er den Verdacht hat, dass eine andere Person Kenntnis seiner Personalisierten Sicherheitsmerkmale erlangt hat oder seine Personalisierten Sicherheitsmerkmale verwendet.

### 10.2 Haftung des Depotinhabers bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

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

### 10.3 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.

## 11. Nutzungssperre

### 11.1 Sperre auf Veranlassung des Konto-/Depotinhabers

Die Bank sperrt auf Veranlassung des Konto-/Depotinhabers, insbesondere im Fall der Sperranzeige nach Nummer 10.1, den Online-Banking-Zugang und/oder das Authentifizierungsinstrument für ihn sowie alle weiteren Konto-/Depotinhaber.

### 11.2 Sperre auf Veranlassung der Bank

- a. Die Bank darf den Online-Banking-Zugang bzw. das Authentifizierungsinstrument für einen Konto-/Depotinhaber sperren, wenn
  - (i) sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
  - (ii) sachliche Gründe im Zusammenhang mit der Sicherheit der Personalisierten Sicherheitsmerkmale bzw. des Authentifizierungsinstruments dies rechtfertigen oder
  - (iii) der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung der Personalisierten Sicherheitsmerkmale bzw. des Authentifizierungsinstruments besteht.

Die Bank wird den Zugang insbesondere dann sperren, wenn dreimal hintereinander ein falsches Kennwort oder eine falsche Nutzer-ID eingegeben wurde.

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

### 11.3 Aufhebung der Sperre

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

## 12. Haftung

### 12.1 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 und den Sonderbedingungen für Wertpapiergeschäfte).



**ABN AMRO Bank N.V., Frankfurt Branch**

Mainzer Landstr. 1  
60329 Frankfurt am Main

**Kontakt Moneyou**

Postfach 10 15 36  
60015 Frankfurt am Main  
Tel: 069-12 00 67 67

E-Mail: [kundenservice@moneyou.de](mailto:kundenservice@moneyou.de)  
[www.moneyou.de](http://www.moneyou.de)