

## 1. ALLGEMEINES

Bei dem Tagesgeldkonto handelt es sich um ein Einlagenkonto, das ausschließlich im Guthabenbereich geführt wird. Das Tagesgeldkonto dient der Geldanlage und darf nicht für Zwecke des Zahlungsverkehrs verwendet werden. Das Tagesgeldkonto kann auch als Verrechnungskonto für die Verbuchung von (Zins-)Gutschriften aus Einlagenkonten des Kunden bei der Bank und für die Abrechnung von Entgelten und Auslagen im Zusammenhang mit der Abwicklung von Wertpapiergeschäften des Kunden über sein bei der Bank bestehendes Depot sowie für Gutschriften aus Wertpapiererträgen geführt werden.

## 2. KONTOINHABER

Konten werden nur für Verbraucher i.S. des § 13 BGB, d.h. nur für natürliche Personen geführt, die die Konten zu einem Zweck eröffnen, der weder ihrer gewerblichen noch ihrer selbständigen beruflichen Tätigkeit dient, die auch wirtschaftlich Berechtigte sind und ihren Wohnsitz in der Bundesrepublik Deutschland haben. Die Bank eröffnet keine Konten, wenn der Kontoinhaber für einen anderen wirtschaftlich Berechtigten handelt.

Das Konto kann auch für zwei Kontoinhaber (Höchstzahl) geführt werden. In diesem Fall zeichnet jeder Kontoinhaber einzeln und das Tagesgeldkonto wird als Oder-Konto geführt; d.h. jeder Kontoinhaber kann alleine ohne Zustimmung des anderen über das Tagesgeldkonto verfügen.

Wird das Konto für zwei natürliche Personen geführt, bevollmächtigen sich die Kontoinhaber gegenseitig, Erklärungen der Bank entgegen zu nehmen und Erklärungen gegenüber der Bank abzugeben; ausgenommen hiervon ist die Kündigung der Kontoverbindung.

## 3. ONLINE-BANKING

### (a) Grundsatz

Der Konto-/Depotinhaber kann Bankgeschäfte ausschließlich im Online-Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Online-Banking abrufen. Konto-/Depotinhaber werden für die Regelungen in dieser Nummer 3. „Online-Banking“ einheitlich als „Kontoinhaber“, Konto und Depot einheitlich als „Konto“ bezeichnet, es sei denn, dieses ist ausdrücklich anders bestimmt.

### (b) Technische Voraussetzung

Für die Nutzung des Online-Banking benötigt der Kontoinhaber einen Internetzugang. Dieser wird nicht von der Bank bereit gestellt. Um das Online-Banking nutzen zu können, benötigt der Kontoinhaber einen Browser, der

eine 128-Bit-SSL-Verschlüsselung unterstützt. Außerdem benötigt er die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Nutzer auszuweisen und Aufträge zu autorisieren. Statt eines personalisierten Sicherheitsmerkmals kann auch ein biometrisches Merkmal des Kontoinhabers zum Zwecke der Authentifizierung bzw. Autorisierung vereinbart werden. Die Bank behält sich vor, den Sicherheitsstandard und damit die technischen Voraussetzungen jederzeit zu verändern. Die Bank wird den Kontoinhaber bei einer Änderung der notwendigen technischen Voraussetzungen zur Teilnahme am Online-Banking rechtzeitig vorher informieren.

### (c) Nutzung von NIBCode, PIN sowie TAN

Für die Abwicklung seiner Bankgeschäfte benötigt der Kontoinhaber die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale [persönlicher NIBCode, persönliche Identifikationsnummer (PIN) oder sein biometrisches Merkmal, einmal verwendbare Transaktionsnummer (TAN) und Authentifizierungsinstrumente (mobiles Endgerät (z.B. Smartphone, Tablet mit Betriebssystem iOS oder Android) zum Empfang von TAN in der SecureGo-App<sup>2</sup> oder ein mobiles Endgerät (z.B. Mobilfunktelefon / Smartphone) zum Empfang von TAN per SMS (mobileTAN)<sup>3</sup> oder eine NIBCard zur smartTAN plus-Generierung in Verbindung mit einem Chipkartenlesegerät / TAN-Generator)], um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen und Aufträge zu autorisieren. Zur Abwicklung seiner Bankgeschäfte übersendet die Bank dem Kontoinhaber einen persönlichen NIBCode, eine PIN, einen Freischaltcode zur Freischaltung des SecureGo-Verfahrens<sup>2</sup> oder einen Freischaltcode zur Freischaltung des mobileTAN-Verfahrens<sup>3</sup> oder eine NIBCard (Chipkarte) zur Nutzung des smartTAN plus-Verfahrens. Der Kontoinhaber muss seine persönliche PIN nach Bekanntgabe durch die Bank ändern. Bei der Abgabe von Willenserklärungen, Änderungen oder Überweisungen muss der Kontoinhaber neben seinem NIBCode und seiner PIN eine Transaktionsnummer angeben.

Die Willenserklärung des Kontoinhabers ist wirksam abgegeben, wenn er die in der Benutzerführung vorgeschriebene Freigabe zur Übermittlung vorgenommen hat. Bei Willenserklärungen, die die Eingabe einer TAN vorsehen, gilt die Willenserklärung mit Eingabe der TAN als abgegeben.

Die Widerrufbarkeit eines im Online-Banking erteilten Auftrages richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen.

## (1) Besondere Regelungen für das mobile TAN-Verfahren (mTAN)<sup>3</sup>

Für die Teilnahme am mTAN-Verfahren ist ein mobiles Endgerät (z. B. Mobilfunktelefon / Smartphone) mit SMS-Empfang sowie einer SIM-Karte eines deutschen Mobilfunknetzbetreibers erforderlich. Für das mTAN-Verfahren wird die von dem Kontoinhaber angegebene deutsche Mobilfunknummer registriert. Die Bank übermittelt dem Kontoinhaber für jede Transaktion eine TAN durch eine Textmeldung (SMS) auf sein mobiles Endgerät mit der registrierten Mobilfunknummer.

Stellt der Kontoinhaber den Verlust der SIM-Karte fest oder besteht der Verdacht einer missbräuchlichen Nutzung, ist der Kontoinhaber verpflichtet, die Bank unverzüglich zu benachrichtigen, um die Mobilfunknummer für den TAN-Versand sperren zu lassen. Ziffer 3. (g) und (h) bleiben unberührt.

Zur Durchführung von Transaktionen im Online-Banking erhält der Kontoinhaber von der Bank auf Anforderung durch eine entsprechende Online-Anwendung für jede Transaktion eine Textmeldung (SMS) mit einer TAN auf sein mobiles Endgerät mit der registrierten Mobilfunknummer. Die in der SMS angegebene TAN ist nur für die Transaktion gültig, für die sie angefordert wurde. Eine nicht genutzte mobile TAN verliert maximal fünfzehn Minuten nach deren Absendung durch die Bank ihre Gültigkeit.

## (2) Besondere Regelungen für das smartTAN plus-Verfahren

Für die Teilnahme am smartTAN plus-Verfahren ist eine NIBCard und ein Chipkartenlesegerät / TAN-Generator erforderlich. Das Lesegerät generiert nach Eingabe eines im Online-Banking angezeigten Start-Code („Code“) und Transaktionsdaten („Data“) eine TAN. Die generierte TAN ist nur für die Transaktion gültig, für die sie generiert wurde.

Stellt der Kontoinhaber den Verlust seiner NIBCard fest oder besteht der Verdacht einer missbräuchlichen Nutzung, ist der Kontoinhaber verpflichtet, die Bank unverzüglich zu benachrichtigen.

## (3) Besondere Regelungen für das SecureGo-Verfahren<sup>2</sup>

Für die Teilnahme am SecureGo-Verfahren ist ein mobiles Endgerät (z.B. Smartphone/Tablet mit Betriebssystem iOS oder Android) erforderlich. Weiter benötigt der Kontoinhaber die SecureGo-App<sup>2</sup>, die er auf sein mobiles Endgerät herunterladen und freischalten muss. Für die Freigabe einer Transaktion im Online-Banking erhält der Kontoinhaber auf Anforderung eine TAN in der SecureGo-App auf sein mobiles Endgerät. Die verschlüsselt übertragene

SecureGo-TAN ist nur für die eine Transaktion gültig, für die sie generiert wurde. Eine nicht genutzte TAN verliert maximal 15 Minuten nach deren Übertragung ihre Gültigkeit. Stellt der Kontoinhaber den Verlust seines mobilen Endgerätes fest oder besteht der Verdacht einer missbräuchlichen Nutzung, ist er verpflichtet die Bank unverzüglich zu benachrichtigen, um die SecureGo-App für die TAN-Generierung sperren zu lassen. Ziffer 3. (g) und (h) bleiben unberührt.

**(d) – frei –**

**(e) – frei –**

## (f) Bearbeitung der Aufträge im Online-Banking

Die Bearbeitung der im Rahmen des Online-Bankings erteilten Aufträge erfolgt nach den für die Abwicklung der jeweiligen Auftragsart geltenden Regelungen.

Aus Sicherheitsgründen ist die Bank berechtigt, eine Betragsobergrenze für Aufträge im Online-Banking festzusetzen.

Aufträge führt die Bank unter folgenden Bedingungen aus:

- Der Kontoinhaber hat sich mit seinem personalisierten Sicherheitsmerkmal (z. B. NIBCode, PIN, TAN) legitimiert oder den Auftrag mit dem vereinbarten biometrischen Sicherheitsmerkmal autorisiert.
- Die Berechtigung des Kunden für die jeweilige Ausführungsart liegt vor.
- Das Online-Banking Datenformat ist eingehalten.
- Eine vereinbarte Betragsobergrenze oder ein Standardlimit für Aufträge im Online-Banking ist nicht überschritten.
- Die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Ausführungsart maßgeblichen Sonderbedingungen liegen vor.

Liegen die vorstehenden Ausführungsbedingungen vor, führt die Bank den Online-Banking-Auftrag nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Vereinbarungen zum Tagesgeldkonto, Sonderbedingungen für das Wertpapiergeschäft) aus, sofern die Ausführung nicht gegen sonstige Rechtsvorschriften verstößt.

Liegen die Ausführungsbedingungen nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird den Kontoinhaber über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit den Fehlern, die zur Ablehnung geführt haben, berichtigt werden können, mittels Online-Banking eine Information zur Verfügung stellen. Dies gilt nicht, wenn die Angabe von Gründen gegen sonstige Rechtsvorschriften verstößt.

## (g) Sorgfaltspflichten des Kontoinhabers

Der Kontoinhaber wird seine personalisierten Sicherheitsmerkmale (NIBCode, PIN, TAN) geheim halten und nur über die von der Bank gesondert mitgeteilten Online-Banking Zugangskanäle (z. B. Internetadresse) an diese übermitteln. Er wird sein Authentifizierungsinstrument (mobiles Endgerät im SecureGo-Verfahren<sup>2</sup>, mobiles Endgerät im mTAN-Verfahren<sup>3</sup>, NIBCard und Chipkartenlesegerät / TAN-Generator) vor dem Zugriff anderer Personen sicher verwahren.

Der Kontoinhaber weiß, dass jeder Dritte, der im Besitz des Authentifizierungsinstruments ist, in Verbindung mit den dazugehörigen personalisierten Sicherheitsmerkmalen das Online-Banking verfahrensmisbräuchlich nutzen kann.

Der Kontoinhaber wird insbesondere folgendes beachten:

- Die personalisierten Sicherheitsmerkmale PIN und TAN sowie der NIBCode dürfen nicht ungesichert elektronisch gespeichert werden.
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dies nicht ausspionieren können.
- Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf Online-Händlerseiten).
- Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb des Online-Banking Verfahrens weitergegeben werden, so beispielsweise nicht per E-Mail.
- Der NIBCode und die PIN dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Kontoinhaber darf zur Autorisierung eines Auftrages oder der Aufhebung einer Sperre nicht mehr als eine TAN verwenden.
- Beim mTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z.B. Mobilfunktelefon / Smartphone mit SIM-Karte), nicht gleichzeitig für das Online-Banking genutzt werden.<sup>3</sup>

Soweit die Bank dem Kontoinhaber Daten aus seinem Online-Banking Auftrag (z. B. Betrag, IBAN des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät des Kontoinhabers (z. B. Smartphone / Tablet mit SecureGo-App<sup>2</sup>, Mobilfunktelefon / Smartphone mit SIM-Karte, Chipkartenlesegerät / TAN-Generator) zur Bestätigung anzeigt, ist der Kontoinhaber verpflichtet, vor der Autorisierung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen. Der Kontoinhaber muss die Sicherheitshinweise auf der Internetseite der Bank zum Online-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

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

## (h) Anzeige- und Unterrichtungspflichten

Stellt der Kontoinhaber den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung, oder die sonstige nicht autorisierte Nutzung eines Authentifizierungsinstruments oder eines seiner persönlichen Sicherheitsmerkmale oder keine Übereinstimmung der von der Bank dem Kontoinhaber angezeigten Transaktionsdaten mit den von ihm für die Transaktion vorgesehenen Daten fest, muss er die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Kontoinhaber hat folgende Möglichkeiten, eine Sperranzeige gegenüber der Bank abzugeben:

- Online Banking
- 24h über die telefonische Kundenbetreuung (NIBC Hotline)

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

Hat der Kontoinhaber 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.

Der Kontoinhaber hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

## (i) Sperren

### (1) Sperre auf Veranlassung des Kontoinhabers

Die Bank sperrt auf Veranlassung des Kontoinhabers, insbesondere im Fall der Sperranzeige nach (h), seinen Online-Zugang oder sein Authentifizierungsinstrument.

### (2) Sperre auf Veranlassung der Bank

Die Bank darf den Online-Banking Zugang für den Kontoinhaber sperren, wenn sie berechtigt ist, das Vertragsverhältnis aus wichtigem Grund zu kündigen, sachliche Gründe im Zusammenhang mit der Sicherheit des Au-

Authentifizierungsinstrumentes oder des personalisierten Sicherheitsmerkmals dies rechtfertigen oder der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstrumentes besteht. Die Bank wird den Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten.

### **(3) Aufhebung der Sperre**

Die Bank wird die Sperre aufheben oder das personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber unverzüglich.

### **(4) Automatische Sperre des Online-Banking Zugangs bei falscher Eingabe von PIN**

Wird dreimal hintereinander die falsche PIN eingegeben, so sperrt die Bank den Online-Zugang zum Konto. Der Nutzer kann diese Sperre aufheben, indem er neben der gültigen PIN eine TAN eingibt. Die Bank übersendet dem Kontoinhaber auf Anforderung oder nach neunmaliger falscher Eingabe auf dem Postweg eine neue PIN.

### **(5) Automatische Sperre des Online-Banking Zugangs bei falscher Eingabe von smartTAN plus**

Wird dreimal hintereinander die falsche smartTAN plus eingegeben, so sperrt die Bank den Online-Zugang zum Konto. Der Nutzer kann sich mit der Bank in Verbindung setzen, um diese Sperre aufzuheben und die Nutzungsmöglichkeiten des Online-Banking wieder herzustellen.

### **(6) Automatische Sperre des Online-Banking Zugangs bei falscher Eingabe von TAN im SecureGo-Verfahren<sup>2</sup>**

Wird dreimal hintereinander die falsche TAN im SecureGo-Verfahren eingegeben, so sperrt die Bank den Online-Zugang zum Konto. Der Nutzer kann sich mit der Bank in Verbindung setzen, um diese Sperre aufzuheben und die Nutzungsmöglichkeit des Online-Banking wieder herzustellen.

## **(j) Haftung**

### **(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 richtet sich vorrangig nach (j) Absätze (2) bis (4) und nachrangig nach den für die jeweilige Ausführungsart vereinbarten Sonderbedingungen.

### **(2) Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige**

(2.1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstrumentes oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungsinstrumentes, haftet der Kontoinhaber für den Bank hierdurch entstehenden Schaden bis zu einem Betrag in Höhe von 50 EURO, ohne dass es darauf ankommt, ob den Kontoinhaber ein Verschulden trifft.

(2.2) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach dem Absatz (2.1) verpflichtet, wenn

- es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungsinstrumentes vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Authentifizierungsinstrumentes durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder einer sonstigen Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(2.3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Kontoinhaber in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von den vorstehenden Regelungen den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Kontoinhabers kann insbesondere vorliegen, wenn er

- den Verlust oder Diebstahl des Authentifizierungsinstrumentes oder die missbräuchliche Nutzung des Authentifizierungsinstrumentes oder des personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe h),
- das personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe g),
- das personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe g),
- das personalisierte Sicherheitsmerkmal per E-Mail weitergegeben hat (siehe g),
- das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe g),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe g),
- beim mTAN-Verfahren das Gerät, mit dem die TAN empfangen wird (z.B. Mobiltelefon), auch für das Online-Banking nutzt (siehe g).<sup>3</sup>

(2.4) Abweichend von den Absätzen (2.1) und (2.3) ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Bank vom Kontoinhaber eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdienstleistungsgesetz nicht verlangt hat, obwohl die Bank zur starken Kundenauthentifizierung nach § 68 Absatz 4 Zahlungsdienstleistungsgesetz verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, das der Kontoinhaber weiß, z.B. PIN), Besitz (etwas, das der Kontoinhaber besitzt (z.B. TAN-Generator) oder Inhärenz (etwas, das der Teilnehmer ist, z.B. Fingerabdruck).

(2.5) Die Haftung für Schäden, die innerhalb des Zeitraumes, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

(2.6) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz (2.1) und (2.3) verpflichtet, wenn der Kontoinhaber die Sperranzeige nach (h) nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(2.7) Die Absätze (2.3) und (2.4) bis (2.6) finden keine Anwendung, wenn der Kontoinhaber in betrügerischer Absicht gehandelt hat.

### **(3) Haftung der Bank ab der Sperranzeige**

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

### **(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.

## **4. POSTBOX / ELEKTRONISCHES POSTFACH**

Der Kontoinhaber kann im Rahmen seines Online-Banking-Zugangs „elektronische Post“ in einem elektronischen Postfach, der sogenannten Postbox, empfangen und elektronische Nachrichten an die Bank senden. Die Bank wird dem Kontoinhaber alle Informationen, rechtsverbindliche Mitteilungen zur laufenden Geschäftsverbindung (z. B. Änderung der Geschäftsbedingungen gemäß Nr. 1 Abs. (2) der Allgemeinen Geschäftsbedingungen), Kontoauszüge und Rechnungsabschlüsse in der Postbox zur

Verfügung stellen und erfüllt damit ihre Unterrichts- und Informationspflichten aus der Geschäftsverbindung mit dem Kontoinhaber. Sofern die Bank den Kontoinhaber nach den gesetzlichen Bestimmungen über das Einstellen von Informationen, Mitteilungen und Dokumenten in seine Postbox in Kenntnis setzen muss, wird sie ihn hierüber per Post, E-Mail oder SMS informieren. Der Kontoinhaber hat der Bank hierfür seine Anschrift, seine E-Mail-Adresse und seine mobile Telefonnummer anzugeben. Um eine Information des Kontoinhabers gewährleisten zu können, ist es erforderlich, dass der Kontoinhaber der Bank Änderungen seiner Anschrift, seiner E-Mail-Adresse und seiner mobilen Telefonnummer unverzüglich mitteilt. Die Bank garantiert, dass die von ihr in die Postbox eingestellten Dokumente von ihr inhaltlich nicht mehr geändert werden können. Die Bank wird die in die Postbox eingestellten Dokumente aber nach Ablauf der gesetzlichen Aufbewahrungspflichten wieder löschen.

Der Kontoinhaber hat über das Internet und mit Hilfe seines NIBCode und seiner PIN Zugriff auf die Postbox. Der Kontoinhaber kann sich die Mitteilungen in seiner Postbox ansehen und ausdrucken, herunterladen und archivieren. Die Bank entscheidet selbst, welche Kategorie von Dokumenten sie in die Postbox einstellt. Sie kann die Auswahl unter Beachtung der Interessen des Kontoinhabers erweitern oder einschränken. Von derartigen Änderungen wird die Bank den Kontoinhaber informieren.

Der Kontoinhaber verzichtet ausdrücklich darauf, dass die Bank die Dokumente, die sie ihm in die Postbox eingestellt hat, in ausgedruckter Form übersendet. Die Bank ist aber berechtigt, ihre Pflichten nicht durch Einstellen einer Datei in die Postbox, sondern durch postalischen Versand an den Kontoinhaber zu erfüllen, um z.B. gesetzliche Auflagen zu erfüllen oder aus Gründen der Zweckmäßigkeit.

Mitteilungen in der Postbox gehen dem Kontoinhaber in dem Zeitpunkt zu, in dem dieser die Information abgerufen hat, spätestens jedoch drei Tage nach Einstellung in die Postbox.

Der Kontoinhaber ist verpflichtet, die Postbox in regelmäßigen Abständen auf Eingänge hin zu überprüfen. Irgendwelche Einwendungen gegen den Inhalt oder die Richtigkeit der in die Postbox übermittelten Dokumente wird der Kontoinhaber unverzüglich, spätestens jedoch innerhalb von sechs Wochen, der Bank mitteilen; es gelten insbesondere die Ziffern 7.2, 11.4 und 11.5 der Allgemeinen Geschäftsbedingungen der NIBC Bank N.V. Zweigniederlassung Frankfurt am Main.

## **5. EINZAHLUNGEN UND VERFÜGUNGEN**

Einzahlungen sind jederzeit durch Überweisungen vom Referenzkonto der/des Kontoinhaber(s) gemäß Nr. 6 möglich. Bei Einzelkonten sind auch Einzahlungen durch Überweisungen innerhalb des Gebietes des einheitlichen Euro-Zahlungsverkehrsraums („SEPA-Raum“)<sup>1</sup> von einem

anderen auf den Namen des Kontoinhabers lautenden Konto und von einem auf den Namen des Kontoinhabers und einer weiteren Person lautenden Gemeinschaftskonto möglich. Bei Gemeinschaftskonten sind auch Einzahlungen innerhalb des SEPA-Raums von einem anderen auf den Namen beider Kontoinhaber lautenden Gemeinschaftskonto und von einem Einzelkonto möglich, das auf den Namen eines der beiden Kontoinhaber lautet. Bei einem Jugend.Zins.Konto sind auch Einzahlungen durch Überweisungen innerhalb des SEPA-Raums von einem anderen auf den Namen eines oder aller gesetzlichen Vertreter lautenden Konto möglich. Verfügungen sind nur bis zur Höhe des jeweiligen Guthabens zulässig. Auch wenn der Kontoinhaber über das gesamte Guthaben auf dem Tagesgeldkonto verfügt, bleibt das Tagesgeldkonto bestehen, es sei denn, der Kunde wünscht ausdrücklich eine Kontoauflösung. Auszahlungen sind ausschließlich durch Überweisungen auf das vom Kontoinhaber angegebene Referenzkonto bei einer anderen kontoführenden Bank möglich.

## 6. REFERENZKONTO

Der Kontoinhaber hat ein Referenzkonto anzugeben, das bei einer anderen inländischen Bank geführt wird. Dieses Referenzkonto, das ein Girokonto (Zahlungsverkehrskonto) sein muss, muss auf den Namen des Kontoinhabers lauten. Als Referenzkonto für ein Einzelkonto kann ein Gemeinschaftskonto angegeben werden, das auf den Namen des Kontoinhabers und einer weiteren Person lautet. Bei einem Jugend.Zins.Konto darf das Referenzkonto auch auf den Namen des/der gesetzlichen Vertreter/s lauten. Bei Gemeinschaftskonten muss das Referenzkonto auf die beiden Namen der Kontoinhaber lauten. Der Kontoinhaber ist berechtigt, das Referenzkonto einmal innerhalb von 30 Tagen zu ändern. Beim Gemeinschaftskonto ist jeder der beiden Kontoinhaber berechtigt, das Referenzkonto alleine zu ändern.

## 7. ZINSVEREINBARUNG UND ABRECHNUNGSMODALITÄTEN

a) Zinsen für das Guthaben auf dem Tagesgeldkonto werden jeweils zum Ende des Kalenderjahres berechnet und dem Tagesgeldkonto gutgeschrieben. Die Bank erstellt zu diesem Zeitpunkt einen Kontoauszug, der dem Kunden neben dem jährlichen Rechnungsabschluss in elektronischer Form in seinem elektronischen Briefkasten, der sogenannten Postbox, zur Verfügung gestellt wird.

b) Wird das Tagesgeldkonto des Kunden auch als Verrechnungskonto für ein Depot (Einfach.Invest.Depot) des Kunden bei der Bank geführt, werden die Zinsen quartalsweise berechnet und am Ende des Quartals dem Tagesgeldkonto gutgeschrieben bzw. belastet. Die Bank erteilt jeweils am Ende eines Quartals einen Rechnungsabschluss unter Verrechnung von Zinsen und Entgelten. Jeweils am Ende

des Quartals erstellt die Bank einen Kontoauszug, der dem Kunden zusammen mit dem Rechnungsabschluss in elektronischer Form in seinem elektronischen Briefkasten, der sogenannten Postbox, zur Verfügung gestellt wird.

c) Die Bank ist berechtigt, den Zinssatz nach billigem Ermessen (§ 315 BGB) zu ändern. Eine gesonderte Mitteilung hierüber erfolgt nicht. Der Kunde kann den aktuellen Zinssatz jederzeit auf der Webseite von NIBC ([www.nibc.de](http://www.nibc.de)) einsehen. Der angegebene Zinssatz ist ein Jahreszinssatz. Die zeitanteilige Berechnung der Zinsen erfolgt auf der Grundlage von 360 Tagen pro Jahr und 30 Tagen pro Monat unabhängig von der tatsächlichen Anzahl der Tage eines Kalendermonats.

## 8. AUSGLEICH VON KONTOÜBERZIEHUNGEN

(1) Entsteht auf dem Konto ein Sollsaldo (z. B. durch Einzug von Entgelten oder Auslagen im Zusammenhang mit der Abwicklung von Wertpapiergeschäften des Kontoinhabers, sofern das Konto auch als Verrechnungskonto für ein Depot (Einfach.Invest.Depot) dient, Steuernachzahlungen an das Finanzamt oder der Belastung von Überziehungszinsen), so ist die Überziehung unverzüglich, spätestens nach fünf Bankarbeitstagen durch entsprechende Geldeingänge auszugleichen, sofern mit dem Kunden keine anderweitige Vereinbarung getroffen ist.

(2) Die Bank ist berechtigt, auf den Betrag, um den das vorhandene Guthaben überschritten wird (Überziehung), ihren während der Überziehung gültigen „Überziehungszinssatz für Tagesgeldkonten als Verrechnungskonto“ zu berechnen. Die Bank ist berechtigt, den Zinssatz nach billigem Ermessen (§ 315 BGB) zu ändern. Der jeweils gültige Überziehungszinssatz kann dem jeweils aktuellen Preis- und Leistungsverzeichnis mit Ausführungs- und Annahmefristen sowie Geschäftstage im Zahlungsverkehr entnommen werden. Die Bank informiert den Kontoinhaber über Zinsänderungen. Die Information darf auch durch entsprechenden Hinweis in den Kontoauszügen erfolgen.

Die Zinsen für die Überziehung des Tagesgeldkontos als Verrechnungskonto werden vierteljährlich nachträglich in Rechnung gestellt und dem Verrechnungskonto des Kontoinhabers belastet.

(3) Wird der Sollsaldo vom Kontoinhaber nicht vereinbarungsgemäß ausgeglichen, ist die Bank berechtigt, von ihrem Sicherungs- und Verwertungsrecht nach Maßgabe von Nr. 14 bis 17 der „Allgemeinen Geschäftsbedingungen“ der Bank Gebrauch machen. Bei Überziehungen, die im Zusammenhang mit der Abwicklung von Wertpapiergeschäften des Kunden entstanden sind, ist die Bank insbesondere berechtigt, den Sollsaldo mit Ertragsausschüttungen zu verrechnen oder durch Verkauf von Wertpapieren aus dem Depot (Einfach.Invest.Depot) auszugleichen.

## 9. KÜNDIGUNG

Wird das Tagesgeldkonto nicht auch als Verrechnungskonto für ein Einlagenkonto mit einer vereinbarten Laufzeit bzw. Kündigungs- und Verfügungsfrist und/oder ein Depot des Kontoinhabers geführt, kann er jederzeit ohne Einhaltung einer Frist die Kontoverbindung kündigen. Wird das Tagesgeldkonto auch als Verrechnungskonto für ein Einlagenkonto mit einer vereinbarten Laufzeit oder einer Kündigungs- und Verfügungsfrist und/oder ein Depot des Kontoinhabers geführt, gilt die Kündigung des Tagesgeldkontos erst zum Ablauf der vereinbarten Laufzeit oder der Kündigungs- und Verfügungsfrist und nach Umbuchung des Guthabenbetrags von dem Einlagenkonto auf das Tagesgeldkonto und Auflösung des Einlagenkontos und/oder nach Auflösung des Depots. Zum Kündigungszeitpunkt wird die Bank den auf dem Tagesgeldkonto befindlichen Guthabenbetrag auf das Referenzkonto überweisen. Die Bank kann das Tagesgeldkonto jederzeit unter Einhaltung einer angemessenen Frist von mindestens zwei Monaten kündigen. Die Bank hat auf die berechtigten Interessen des Kontoinhabers, insbesondere auf eventuelle Bindungen aus einem Einlagenkonto und einem bei der Bank geführten Depot Rücksicht zu nehmen. Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt für beide Seiten bestehen.

## 10. GEBÜHREN

Die Führung des Tagesgeldkontos ist kostenfrei. Der Kontoinhaber hat jedoch seine eigenen Kosten (z. B. für Ferngespräche, Computer- und Datenverbindungskosten etc.) selbst zu tragen.

## 11. HINWEIS ZUR STEUERPFlicht

Die anfallenden Guthabenzinsen sind als Einkünfte steuerpflichtig. Die Bank ist nach den gesetzlichen Bestimmungen verpflichtet, die Kapitalertragsteuer, die auf die Guthabenzinsen anfällt, einzubehalten und an das jeweilige Finanzamt abzuführen (sogenannte Abgeltungssteuer), wodurch der an den Kunden zu zahlende Betrag gemindert wird. Dies gilt nur, soweit der Kunde der Bank keine Nichtveranlagungsbescheinigung vorgelegt hat, keinen Freistellungsauftrag erteilt hat oder dieser ausgeschöpft ist. Bei Fragen sollte sich der Kontoinhaber an die für ihn zuständige Steuerbehörde oder seinen steuerlichen Berater wenden.

## 12. PFANDRECHT, VERBOT DER ABTRETUNG UND / ODER VERPFÄNDUNG

Der Kontoinhaber und die Bank sind sich darüber einig, dass der Bank ein Pfandrecht an dem Guthaben einschließlich aller Zinsen auf dem Tagesgeldkonto zusteht. Das Pfandrecht dient der Sicherung aller bestehenden, künftigen und bedingten Ansprüche, die der Bank mit sämtlichen ihrer in- und ausländischen Geschäftsstellen aus der bankmäßigen Geschäftsbeziehung gegen den Kontoinhaber zustehen.

Die Abtretung und / oder Verpfändung der Ansprüche des Kontoinhabers von Konten und Depots aus der Geschäftsbeziehung sind ausgeschlossen. Das Abtretungsverbot gilt für sämtliche Ansprüche, insbesondere für solche im Hinblick auf Kontoguthaben, Kredite und Wertpapiere.

## 13. EINLAGENSICHERUNG

Die Bank unterliegt dem niederländischen Einlagensicherungssystem, welches durch die Bankenaufsicht der De Nederlandsche Bank N.V. (DNB) beaufsichtigt und umgesetzt wird. Nähere Informationen hierzu finden Sie unter Nr. 20 der Allgemeinen Geschäftsbedingungen der Bank, dem „Informationsbogen für den Einleger“ und der Internetseite der niederländischen Zentralbank unter [www.dnb.nl](http://www.dnb.nl). Die Bank ist befugt, dem niederländischen Einlagensicherungssystem oder einem von diesem Beauftragten auf Anforderung alle in diesem Zusammenhang erforderlichen Auskünfte zu erteilen und Unterlagen zur Verfügung zu stellen.

## 14. ANWENDBARES RECHT / GERICHTSSTAND

Für diesen Vertrag und die Geschäftsbeziehung zwischen dem Kontoinhaber und der Bank gilt deutsches Recht. Es gibt keine vertragliche Bestimmung des Gerichtsstands.

## 15. VERTRAGSSPRACHE

Maßgebliche Sprache für dieses Vertragsverhältnis ist Deutsch. Der Vertrag und die allgemeinen Geschäftsbedingungen stehen ausschließlich in deutscher Sprache zur Verfügung.

<sup>1</sup> Die zum SEPA-Raum aktuell gehörenden Staaten und Gebiete entnehmen Sie bitte unseren Vereinbarungen für Zahlungen mittels Lastschrift im SEPA-Basislastschriftverfahren (Nr. 2.1.1), die im Formularcenter auf unserer Webseite ([www.nibc.de](http://www.nibc.de)) veröffentlicht sind.

<sup>2</sup> Mit dem Begriff „SecureGo-App“ sind in dieser Vereinbarung sowohl die SecureGo-App als auch die SecureGo plus-App und mit dem Begriff „SecureGo-Verfahren“ sowohl das SecureGo-Verfahren als auch das SecureGo plus-Verfahren gemeint.

<sup>3</sup> Das mobile TAN-Verfahren wird mit Ablauf des 30.06.2023 technisch nicht mehr unterstützt und steht dem Kunden nicht mehr zur Verfügung. Der Kunde kann stattdessen das SecureGo plus-Verfahren oder smartTAN plus-Verfahren nutzen.