VBANK

Die Vermögensbank.

Benutzerantrag für Online-Banking

Konto-/Depot-Nr.: | | | | | | | | | | |

1 Persönliche Angaben

Anrede, Titel: ☐ Frau ☐ Herr ☐ Dr. ☐ Prof.

Vorname: _____ Nachname: _____

Geburtsdatum: _____

2 Zugriffsberechtigung

Der Onlinezugang soll mit nachfolgender Berechtigung eingerichtet werden:

_ Leserecht

3 Dokumentenversand

Die Mitteilungen der Bank (u. a. Wertpapierabrechnungen, Kontoauszüge, Ex-Ante-Kostenbelege, regelmäßige Reportings) sowie gegebenenfalls weitere erforderliche Informationen werden elektronisch übermittelt und stehen in der Postbox zum Abruf zur Verfügung. Der Antragsteller erhält die Zugangsdaten unabhängig von der gewählten Versandart an die Meldeadresse automatisiert zugesandt.

Entgegen oben genannten Vereinbarung wünsche ich die Zustellung von allen Mitteilungen der Bank:

☐ postalisch (gegen Gebühr, sofern keine vertragliche oder gesetzliche Verpflichtung der Bank dazu besteht)

☐ ausdrücklich an meinen bevollmächtigten Finanzdienstleister

4 Stammnummern

Folgende Stammnummern sollen innerhalb des Online-Zuganges ebenfalls freigeschalten werden (nur möglich, wenn Kontoinhaber oder bevollmächtigt):

Kundenstamm-Nr. 1	Kundenstamm-Nr. 2	Kundenstamm-Nr. 3
Kundenstamm-Nr. 4	Kundenstamm-Nr. 5	Kundenstamm-Nr. 6

Unterschrift

Mit meiner Antragstellung bestätige ich, die Weboberfläche sowie den Zugang über elektronische Medien und per Telefax nutzen zu wollen. Die „Bedingungen für den Zugang über elektronische Medien und per Telefax“ habe ich erhalten.

Ort	Datum	X Unterschrift Antragsteller

VBANK

Die Vermögensbank.

Bedingungen für den Zugang über elektronische Medien und per Telefax

1 Leistungsumfang

(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 eventuell 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).

2.1 Personalisierte 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:

- Benutzerkennung
- persönliche Identifikationsnummer (PIN)
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN] bzw. Pushnachrichten, die den Besitz des Teilnehmers nachweisen, wie das mobile Endgerät, oder Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers). Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelementes und/oder den Nachweis des Seinselementes an die Bank übermittelt.

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. Passwort, QR-Code) dem Teilnehmer zur Verfügung gestellt werden:

- Passwort-Brief
- QR-Code-Brief
- Hardwaregerät (Smartphone oder Tablet) bzw. Token zur Erzeugung von einmal verwendbaren Transaktionsnummern (TAN) bzw. zur Erzeugung von Push-Nachrichten

3 Zugang zum Online-Banking

Der Teilnehmer muss seinen Zugang zum Online-Banking (reiner Lesezugriff, aber auch Aufträge, z. B. Überweisungen) für dessen Wirksamkeit alle drei Authentifizierungselemente (Wissenselement, Nachweis des Besitzelements, Nachweis des Seinselements) autorisieren und der Bank mittels Online-Banking übermitteln. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags. Nach Gewährung des Zugangs zum Online-Banking kann der Teilnehmer Informationen abrufen oder, bei entsprechender Berechtigung, 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 (z. B. Überweisungen) zu deren Wirksamkeit alle drei Authentifizierungselemente (Wissenselement, Nachweis des Besitzelements, Nachweis des Seinselements) 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 (z. B. „Bedingungen für den Überweisungsverkehr"). Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Online-Banking ausdrücklich vor.

1057_03_2025

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 (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.

(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 (z. B. 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 (z. B. 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 (z. B. „Bedingungen für den Überweisungsverkehr“, „Sonderbedingungen für Wertpapiergeschäfte“) 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 im Rahmen des vereinbarten Reportings 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 (z. B. 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 Nummer 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 und nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln 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 weitergegeben werden.

_ Das personalisierte Sicherheitsmerkmal (z. B. Passwort, QR-Code) darf nicht zusammen mit dem Authentifizierungsinstrument (z. B. Hardwaregerät [Smartphone oder Tablet] bzw. Token) verwahrt werden.

7.3 Sicherheitshinweise 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 (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapier-Kennnummer) im Kundensystem oder ggf. über ein anderes Gerät des Teilnehmers 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 seines persönlichen Sicherheitsmerkmals 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.

1057_03_2025

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) Der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der personalisierten Sicherheitsmerkmale/Authentifizierungsmerkmale besteht insbesondere dann, wenn

_ 5-mal hintereinander die PIN falsch eingegeben wird.

(3) 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.

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 (z. B. „Bedingungen für den Überweisungsverkehr“, „Sonderbedingungen für Wertpapiergeschäfte“).

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

10.2.1 Haftung des Kontoinhabers bei nicht autorisierten Wertpapiertransaktionen 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 Zahlungsvorgang zu 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 erster Spiegelstrich),

_ das personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1),

_ das personalisierte Sicherheitsmerkmal weitergegeben hat (siehe Nummer 7.2 Absatz 2 dritter Spiegelstrich),

_ das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 vierter 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.

1057_03_2025

(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.

11 Aufträge per Fax

Die Bank kann sich die Ordnungsmäßigkeit eines Auftrags vor dessen Ausführung durch telefonische Nachfrage beim Konto-/Depotinhaber bestätigen lassen. Ist eine solche Autorisierung nicht möglich oder bestehen aus anderen Gründen erhebliche Zweifel an der Ordnungsmäßigkeit des Auftrages, ist die Bank berechtigt, den Auftrag nicht auszuführen. In diesem Fall erhält der Konto-/Depotinhaber eine gesonderte Mitteilung über die Nichtausführung.

12 Elektronische Bereitstellung von Bankpost

Verzichtet der Konto-/Depotinhaber zu Gunsten elektronischer Bereitstellung auf die Zusendung von Bankpost (z. B. Auszüge, Rechnungsabschlüsse, Wertpapiertransaktionsabrechnungen, Mitteilungen), ist die Bank nach Ablauf eines nach pflichtgemäßem Ermessen der Bank zu bestimmenden Zeitraumes berechtigt, bereitgestellte, aber nicht gelesene Unterlagen gegen Erstattung von Auslagen (insbesondere Portokosten) auf dem Postweg zuzusenden, sofern nicht anders mit dem Konto-/Depotinhaber vereinbart.

13 Kontroll- und Mitwirkungspflichten des Kunden

Der Kunde ist verpflichtet, das elektronische Postfach auf den Eingang neuer Dokumente zu kontrollieren. Die Kontrolle ist regelmäßig – mindestens jedoch einmal im Monat – insbesondere jedoch dann vorzunehmen, wenn aufgrund eines zuvor erteilten Auftrages mit der Einstellung neuer Dokumente zu rechnen ist. Der Kunde verpflichtet sich im elektronischen Postfach neu hinterlegte Dokumente regelmäßig abzurufen und neu eingegangene Dokumente auf Richtigkeit und Vollständigkeit zu kontrollieren. Beanstandungen und Einwendungen sind der Bank unverzüglich nach Zugang des entsprechenden Dokuments und aus Beweisgründen schriftlich mitzuteilen. Soweit den Kunden hinsichtlich der bislang papierhaft übersandten Dokumente Verpflichtungen treffen, bestehen diese in gleicher Weise für die durch das elektronische Postfach übermittelten Dokumente.

14 Zugang

Soweit der Kunde die Dokumente nicht bereits vorher abgerufen hat, gelten sie am Tag nach der Bereitstellung als zugegangen.