

Antrag für den Zugang zur norisbank GmbH über elektronische Medien






Zurücksenden per Post: norisbank GmbH, 10910 Berlin

An
norisbank GmbH
10910 Berlin

Persönliche Angaben

Bitte tragen Sie hier die Daten der freizuschaltenden Kundenverbindung ein:

| Fil.-Nr.  | Kunden-Nr.  oder | IBAN 

Kontoinhaber Frau Herr

| Vorname/n 

| Nachname 

Bei Unterzeichnung durch mehrere Kontoinhaber gilt jeweils statt der verwendeten Einzahl die Mehrzahl.

Anmeldung des Kontoinhabers für das Online-Banking der norisbank

Hiermit melde ich mein/e Konto/en unter der o.g. Kundennummer für das Online-Banking der norisbank an. Damit kann ich bzw. der nachfolgend genannte Nutzer den von der Bank angebotenen Umfang des Online-Banking der norisbank nutzen. Für Online-Überweisungen wird ein Verfügungsrahmen von 2.500 Euro pro Tag beantragt, wenn nachstehend kein abweichender Rahmen beantragt wird.

Abweichend beantragter Verfügungsrahmen: _____ Euro

Anmeldung des Nutzers für das Online-Banking der norisbank

Der Zugang soll für
den o.g. Kontoinhaber

oder, falls hiervon abweichend,
folgenden Nutzer

| Vorname/n _____

| Nachname _____

| Geburtsdatum _____

angemeldet werden.

Eine wirksame Anmeldung setzt voraus, dass der Nutzer verfügungsberechtigt ist, z. B. auf Grund einer Bankvollmacht.

Ausstattung mit Zugangsdaten

Sofern der Kontoinhaber/der Nutzer bereits über persönliche Zugangsdaten für das Online-Banking verfügt, gelten diese auch für oben genannte Kundennummer. Andernfalls werden diese an die Adresse des Kontoinhabers/Nutzers gesandt.



BestSign

Für das Online-Banking der norisbank wird neben den Zugangsdaten (ID und Passwort) ein BestSign-Sicherheitsverfahren benötigt. Falls BestSign bereits in einem bestehenden Online-Zugang genutzt wird, kann dies ebenfalls für oben angegebene Kundennummer verwendet werden. **Falls nicht, benötigt o. g. Person die norisbank App auf einem Smartphone oder ein separates BestSign-Gerät.** Die norisbank App wird kostenfrei im Google PlayStore (für Android) und im App Store (für iOS) angeboten. Alle Informationen und Anleitungen zu BestSign sind unter www.norisbank.de/bestsign zu finden.

Damit kann ich bzw. der oben genannte Nutzer den Standardumfang des Online-Banking der norisbank nutzen (z. B. Kontoumsätze einsehen, In- und Auslandsüberweisungen tätigen). Sofern Einschränkungen an o. g. Standardumfang vorgenommen werden sollen, ist bei einem vom Kontoinhaber abweichenden Nutzer das angehängte Formular „Antrag für den Zugang zur Bank über elektronische Medien für einen weiteren Nutzer“ zu verwenden. Einschränkungen für den Kontoinhaber sind separat zu beauftragen.

Es gelten die Bedingungen für den Zugang zur norisbank GmbH über elektronische Medien.

Postfach

Bitte aktivieren Sie für meine Geschäftsverbindung mit Ihnen das digitale Postfach für den Empfang von Bankmitteilungen.

Ich erkläre mich damit einverstanden, dass mir Bankmitteilungen auf einem anderen dauerhaften Datenträger als Papier (digitales Postfach oder E-Mail) übermittelt werden, soweit dies nach den gesetzlichen Vorgaben zulässig ist. Dabei handelt es sich insbesondere um folgende vertragsrelevante Bankerklärungen und vertraglich, gesetzlich und aufsichtsrechtlich geschuldete Informationen: Vorvertragliche Informationen, Vertragsangebote und ggf. Erläuterungen, Bankmitteilungen unter anderem zu Allgemeinen Geschäftsbedingungen sowie ggfs. deren Änderungen, Preisverzeichnis etc., Kontoauszüge, Kontoabrechnungen, Zinsänderungen, Mitteilungen zu eingeräumten Kontoüberziehungen (z. B. Dispo-Kredit, Kreditlinien etc.) und zu geduldeten Kontoüberziehungen (z. B. Sollzinsen, Inanspruchnahmen, Beratungsangebote, Änderungen zur Höhe eines Dispo-Kredites etc.) Informationen, Mitteilungen und Erklärungen zum Inhalt, der Durchführung und der Beendigung von Darlehensverträgen (z. B. Zins- und Tilgungsplan, Saldenmitteilung, Angebot eines neuen gebundenen Sollzinssatzes nach Auslauf der Sollzinsbindung etc.), Mahnungen, Kündigungsandrohungen und Kündigungserklärungen. Liegt eine Mitteilung im digitalen Postfach vor, werde ich über die von mir mitgeteilte E-Mail Adresse darüber per E-Mail informiert.

| E-Mail-Adresse (Pflichtfeld)

Es gelten die Bedingungen zur Nutzung des digitalen Postfachs im Online-Banking.

Anmeldung des Kontoinhabers/o. g. Nutzers für das Telefon-Banking der norisbank

Hiermit melde ich mein /e bestehenden und zukünftigen Konto /Konten unter der genannten Kundennummer für die genannte Person zum Telefon-Banking an.

Sofern die oben genannte Person, z. B. als Bevollmächtigter bereits über persönliche Zugangsdaten verfügt, gelten sie auch für diese Kundennummer. Andernfalls werden dies an die Adresse der oben genannten Person zugesandt. Damit kann ich bzw. der oben genannte Nutzer in dem von der Bank angebotenen Umfang das Telefon-Banking nutzen (z. B. Kontoumsätze einsehen, In- und Auslandsüberweisungen tätigen).

Es gelten die Bedingungen für den Zugang zur norisbank GmbH über elektronische Medien.

Aufzeichnung der Telefonkommunikation

Voraussetzung für die Teilnahme am Telefon-Banking ist die Aufzeichnung der Telefonate. Die Aufzeichnung erfolgt zu Nachweiszwecken sowie aufgrund gesetzlicher Vorgaben. Nach Ablauf entsprechender Aufbewahrungsfristen werden diese Daten gelöscht.

Einbeziehung der Geschäftsbedingungen

Maßgebend für die Geschäftsverbindung sind die **Allgemeinen Geschäftsbedingungen** der Bank und die **Bedingungen für den Zugang zur norisbank GmbH über elektronische Medien**, sowie **Bedingungen zur Nutzung des digitalen Postfachs im Online-Banking**. Deren Wortlaut kann unter www.norisbank.de/bedingungen eingesehen werden. Sie werden auf Wunsch zugesandt.

Datenschutzrechtlicher Hinweis zur Verarbeitung und Nutzung Ihrer personenbezogenen Daten

Die Bank verarbeitet und nutzt die von Ihnen erhobenen personenbezogenen Daten auch für Zwecke der Werbung oder der Markt- oder Meinungsforschung. Der Verarbeitung und Nutzung Ihrer personenbezogenen Daten für die vorgenannten Zwecke können Sie jederzeit widersprechen.



Unterschrift (Bitte unterschreiben Sie an den markierten Stellen)

| Datum _____

X Unterschrift des Kontoinhaber/s _____

| Datum _____

X Unterschrift des Nutzers, sofern dieser nicht Kontoinhaber ist _____

| Datum _____

X Unterschrift des/der Kreditkarteninhaber/s, sofern diese/r nicht Kontoinhaber/in _____

Empfangsbestätigung

Ich habe jeweils ein Exemplar

der Bedingungen für den Zugang zur norisbank über elektronische Medien.

der Bedingungen zur Nutzung des digitalen Postfachs im Online-Banking,

der Allgemeinen Geschäftsbedingungen, der Sonderbedingungen und des Informationsbogens für den Einleger (www.norisbank.de/bedingungen)

erhalten.

| Datum _____

X Unterschrift des/der Kontoinhaber/s _____






Antrag für den Zugang zur norisbank GmbH über elektronische Medien für einen weiteren Nutzer



Kontoinhaber

Bitte tragen Sie hier die Daten der freizuschaltenden Kundenverbindung ein:

| Fil.-Nr.  | Kunden-Nr.  oder | IBAN 

Kontoinhaber Frau Herr

| Vorname/n 

| Nachname 

Bei Unterzeichnung durch mehrere Kontoinhaber gilt jeweils statt der verwendeten Einzahl die Mehrzahl.

Nutzer

Neben dem Kontoinhaber können weitere Nutzer zum Online-Banking der norisbank und/oder Telefon-Banking der norisbank angemeldet werden. Eine wirksame Anmeldung setzt voraus, dass der Nutzer verfügbare ist, z. B. auf Grund einer Bankvollmacht.

Der Verfügungsberechtigte soll den jeweiligen elektronischen Zugang zu meinem/unserem Konto nutzen:

Nutzer Frau Herr

| Vorname

| Nachname

| Geburtsdatum

Anmeldung des Nutzers für das Online-Banking der norisbank

Der Nutzer soll folgende Bankdienstleistungen nutzen:

- Kontoumsätze einsehen
- Digitales Postfach einsehen
- In- und Auslandsüberweisungen tätigen
- Sonstige Aufträge erteilen (z. B. Mitteilungen an die Bank senden)

Ausstattung mit Zugangsdaten

Sofern die oben genannte Person bereits über persönliche Zugangsdaten für das Online-Banking verfügt, gelten diese auch für oben genannte Kundennummer. Andernfalls werden diese an die Adresse der oben genannten Person gesandt.

BestSign

Für das Online-Banking der Deutsche Bank wird neben den Zugangsdaten (ID und Passwort) ein BestSign-Sicherheitsverfahren benötigt. Falls BestSign bereits in einem bestehenden Online-Zugang genutzt wird, kann dies ebenfalls für oben angegebene Kundennummer verwendet werden.

Falls nicht, benötigt o. g. Person die norisbank App auf einem Smartphone oder ein separates BestSign-Gerät. Die norisbank App wird kostenfrei im Google PlayStore (für Android) und im App Store (für iOS) angeboten. Alle Informationen und Anleitungen zu BestSign sind unter www.norisbank.de/bestsign zu finden.

Es gelten die Bedingungen für den Zugang zur norisbank GmbH über elektronische Medien.

Anmeldung des Nutzers für das Telefon-Banking der norisbank

Hiermit melde ich mein /e bestehenden und zukünftigen Konto /Konten, Depot /s unter der genannten Kundennummer für die genannte Person zum Telefon-Banking an.

Sofern die oben genannte Person, z. B. als Bevollmächtigter bereits über persönliche Zugangsdaten verfügt, gelten sie auch für diese Kundennummer. Andernfalls werden dies an die Adresse der oben genannten Person zugesandt. Damit kann die o.g. Person in dem von der Bank angebotenen Umfang das Telefon-Banking nutzen (z. B. Kontoumsätze einsehen, In- und Auslandsüberweisungen tätigen).

Es gelten die Bedingungen für den Zugang zur norisbank GmbH über elektronische Medien.



Aufzeichnung der Telefonkommunikation

Voraussetzung für die Teilnahme am Telefon-Banking ist die Aufzeichnung der Telefonate. Die Aufzeichnung erfolgt zu Nachweiszwecken sowie aufgrund gesetzlicher Vorgaben. Nach Ablauf entsprechender Aufbewahrungsfristen werden diese Daten gelöscht.

Einbeziehung der Geschäftsbedingungen

Maßgebend für die Geschäftsverbindung sind die **Allgemeinen Geschäftsbedingungen der Bank** und die **Bedingungen für den Zugang zur norisbank GmbH über elektronische Medien**, sowie **Bedingungen zur Nutzung des digitalen Postfachs im Online-Banking**. Deren Wortlaut kann unter www.norisbank.de/bedingungen eingesehen werden. Sie werden auf Wunsch zugesandt.

Datenschutzrechtlicher Hinweis zur Verarbeitung und Nutzung Ihrer personenbezogenen Daten

Die Bank verarbeitet und nutzt die von Ihnen erhobenen personenbezogenen Daten auch für Zwecke der Werbung oder der Markt- oder Meinungsforschung. Der Verarbeitung und Nutzung Ihrer personenbezogenen Daten für die vorgenannten Zwecke können Sie jederzeit widersprechen.

Unterschrift (Bitte unterschreiben Sie an den markierten Stellen)

Datum _____	<input checked="" type="checkbox"/> Unterschrift des Kontoinhaber/s _____
Datum _____	<input checked="" type="checkbox"/> Unterschrift des Nutzers, sofern dieser nicht Kontoinhaber ist _____
Datum _____	<input checked="" type="checkbox"/> Unterschrift des/der Kreditkarteninhaber/s, sofern diese/r nicht Kontoinhaber/in _____
Empfangsbestätigung	
Ich habe jeweils ein Exemplar	
der Bedingungen für den Zugang zur norisbank über elektronische Medien,	
der Bedingungen zur Nutzung des digitalen Postfachs im Online-Banking,	
der Allgemeinen Geschäftsbedingungen, der Sonderbedingungen und des Informationsbogens für den Einleger (www.norisbank.de/bedingungen)	
erhalten.	
Datum _____	<input checked="" type="checkbox"/> Unterschrift des/der Kontoinhaber/s _____



Stand Mai 2025

1. Leistungsangebot

- (1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels elektronischer Zugangsmedien, im Einzelnen Online-Banking und Telefon-Banking (jeweils einzeln „Online-Banking“ bzw. „Telefon-Banking“ sowie gemeinsam „Zugangsmedien“ bzw. „elektronische Medien“), in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online- und Telefon-Banking abrufen. Im Rahmen des Online-Bankings sind sie gemäß § 675f Absatz 3 BGB zusätzlich berechtigt, Zahlungsauslösedienste gemäß § 1 Absätze 33 und 34 Zahlungsdienstenaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen sorgfältig ausgewählte sonstige Drittdienste nutzen.
- (2) Kunde und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet.
- (3) Für die Nutzung der Zugangsmedien gelten die mit der Bank gesondert vereinbarten Verfügungsmittele.

2. Voraussetzungen zur Nutzung der elektronischen Medien

- (1) Der Teilnehmer kann Bankgeschäfte über elektronische Medien abwickeln, wenn die Bank ihn authentifiziert hat.
- (2) Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers, oder die berechtigte Verwendung eines bestimmten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).
- (3) Authentifizierungselemente sind
 - Wissensselemente, also etwas, das nur der Teilnehmer weiß (z. B. die persönliche Identifikationsnummer [PIN] oder das persönliche Passwort),
 - Besitzelemente, also etwas, was nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN], die girocard mit TAN-Generator oder das mobile Endgerät), oder
 - Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).
- (4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung das Wissensselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.
- (5) Je nach Authentifizierungsverfahren und -instrument benötigt der Teilnehmer hierfür gegebenenfalls geeignete Hard- und Software. Über das Angebot der bankeigenen Anwendungen hinaus bleibt der Teilnehmer selbst für die Beschaffung, Installation und Pflege dieser Hard- und Software verantwortlich.
- (6) Bei einer Nutzung einer Hard- bzw. Software von Drittanbietern durch den Teilnehmer übernimmt die Bank keine eigene Gewährleistung oder sonstige Verantwortung für eine andauernde Eignung oder Verfügbarkeit im Zusammenhang mit einem Authentifizierungsverfahren.

3. Zugang über elektronische Medien

- (1) Der Teilnehmer erhält Zugang zum Online- und Telefon-Banking der Bank, wenn
 - dieser die Kontonummer oder seinen individuellen Benutzernamen angibt und
 - er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
 - keine Sperre des Zugangs (siehe Nummern 8.1 und 9 dieser Bedingungen) vorliegt.

Nach Gewährung des Zugangs zum Online- und Telefon-Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge¹ erteilt werden.

- (2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z. B. zum Zweck der Änderung der Anschrift des Kunden) fordert die Bank den Teilnehmer auf, sich unter Verwendung eines weiteren Authentifizierungselementes auszuweisen, wenn beim Zugang zum Online-Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kontoinhabers und die Kontonummer sind für den vom Teilnehmer genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Daten (§ 1 Absatz 26 Satz 2 ZAG).

4. Aufträge¹

4.1 Auftragserteilung

- (1) Der Teilnehmer muss einem Auftrag (z. B. Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z. B. Eingabe einer TAN oder Übertragung einer elektronischen Signatur als Nachweis des Besitzelements) zu verwenden. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags.
- (2) Der Teilnehmer kann Telefon-Banking-Aufträge nur nach erfolgreicher Autorisierung mit dem von der Bank bereitgestellten personalisierten Sicherheitsmerkmal erteilen. Die Bank bestätigt den Eingang des Auftrags auf dem vom Teilnehmer für den Auftrag gewählten Zugangsweg. Die zwischen der Bank und dem Kontoinhaber übermittelte Telefonkommunikation wird zu Beweis Zwecken automatisch aufgezeichnet und gespeichert.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines 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- und Telefon-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Online- und Telefon-Banking ausdrücklich vor.

5. Bearbeitung von Aufträgen¹ durch die Bank

- (1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Online- und Telefon-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

¹ Zum Beispiel Überweisung, Dauerauftrag und Lastschrift.

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 (vgl. Nummer 4.1 dieser Bedingungen).

— Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Überweisung) liegt vor.

— Das Online-Banking-Datenformat ist eingehalten.

— Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.

— Im Telefon-Banking wird die Bank Verfügungen über das Konto, die eine Zahlung¹ an einen Dritten (abweichende Kontonummer) enthalten, bis zu einem Betrag von insgesamt unter 50.000 EUR pro Tag ausführen, sofern nicht ein anderer Verfügungshöchstbetrag mit dem Teilnehmer vereinbart ist. Für Überträge (Überweisungen) innerhalb der gleichen Kundennummer oder An- und Verkäufe von Wertpapieren gilt diese Betragsgrenze nicht.

— Die weiteren Ausführungsbedingungen 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- und Telefon-Banking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Online- bzw. Telefon-Banking-Auftrag nicht ausführen und den Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Online- bzw. Telefon-Banking oder postalisch informieren.

6. Information des Kunden über Online- und Telefon-Banking-Verfügungen¹

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

7. Sorgfaltspflichten des Teilnehmers

7.1 Schutz der Authentifizierungsinstrumente

(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online- und Telefon-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummern 3 und 4 dieser Bedingungen).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

a) Wissensselemente, wie z.B. die PIN, sind geheim zu halten. Sie dürfen insbesondere

— nicht außerhalb des Online-Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden,

— nicht ungesichert außerhalb des zugelassenen Authentifizierungsverfahrens elektronisch gespeichert werden (z. B. PIN im Klartext im Computer oder im mobilen Endgerät) und

— nicht auf einem Gerät notiert sein oder als Abschrift zusammen mit einem Gerät, das als Besitzelement (z. B. mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z.B. mobiles Endgerät mit Anwendung für das Online-Banking und Fingerabdrucksensor) dient, aufbewahrt werden.

b) Besitzelemente, wie z. B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

— ist die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,

— ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können.

— ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für das Online-Banking (z. B. Online-Banking-App, Authentifizierungs-App) nicht nutzen können,

— ist die Anwendung für das Online-Banking (z. B. Online-Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf des Mobiltelefons),

— dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online-Bankings mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und

— muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das Online-Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ein Gerät als Besitzelement für das Online-Banking des Teilnehmers aktivieren.

c) Seinselemente, wie z.B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online-Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online-Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Online-Banking das von der Bank ausgegebene Wissensselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 2 darf der Teilnehmer seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst (siehe Nummer 1 Absatz 1 Satz 3 dieser Bedingungen) verwenden. Möchte der Teilnehmer einen sonstigen Drittdienst nutzen (siehe Nummer 1 Absatz 1 Satz 4 dieser Bedingungen), hat er diesen mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

¹ Zum Beispiel Überweisung, Dauerauftrag und Lastschrift.

- (4) Der Aufforderung per elektronischer Nachricht (z. B. E-Mail), eine damit übersandte Verknüpfung zum (vermeintlichen) Online-Banking der Bank anzuwählen und darüber persönliche Zugangsdaten einzugeben, darf nicht gefolgt werden.
- (5) Anfragen außerhalb der bankseitig zur Verfügung gestellten originären Zugangswege, in denen nach vertraulichen Daten wie PIN, Geheimzahl oder Passwort/TAN gefragt wird, dürfen nicht beantwortet werden. Die Nutzung von Zahlungsauslösediensten bzw. Kontoinformationsdiensten bleibt hiervon unberührt.
- (6) Der Teilnehmer hat vor seinem jeweiligen Zugang zum Online-Banking sicherzustellen, dass auf dem verwendeten System handelsübliche Sicherheitsvorkehrungen (wie Anti-Viren-Programm und Firewall) installiert sind und diese ebenso wie die verwendete System- und Anwendungssoftware regelmäßig aktualisiert werden. Beispiele handelsüblicher Sicherheitsvorkehrungen kann der Teilnehmer den Internetseiten der Bank entnehmen.
- (7) Die Softwareanwendungen der Bank sind ausschließlich direkt von der Bank oder von einem von der Bank benannten Anbieter zu beziehen.

7.2 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. Darüber hinaus hat der Kunde in eigener Verantwortung etwaige Sicherheitshinweise der Anbieter der eingesetzten Kundensysteme zu beachten (z. B. Sicherheitsupdates von Systemsoftware mobiler Endgeräte).

7.3 Prüfung durch Abgleich der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Daten (z. B. Betrag, Kontonummer des Zahlungsempfängers) über das gesondert vereinbarte Gerät des Teilnehmers an (z. B. mittels mobilem Endgerät oder Lesegerät). Der Teilnehmer ist verpflichtet, vor der Autorisierung (z. B. Eingabe der TAN) die Übereinstimmung der angezeigten Daten mit den für den Auftrag¹ vorgesehenen Daten zu prüfen. Stimmen die angezeigten Daten nicht überein, ist der Vorgang abzubrechen und die Bank unverzüglich zu informieren.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

- (1) Stellt der Teilnehmer
 - den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. mobiles Endgerät, Signaturkarte) oder
 - die missbräuchliche Verwendung oder sonstige nicht autorisierte Nutzung seines Authentifizierungsinstrumentes oder eines seiner persönlichen Sicherheitsmerkmale fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.
- (2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.

- (3) Hat der Teilnehmer den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge¹

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

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

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

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

9.2 Sperre auf Veranlassung der Bank

- (1) Die Bank darf den Online- und Telefon-Banking-Zugang für einen Teilnehmer sperren oder ein Authentifizierungsinstrument nicht mehr zulassen, wenn
 - sie berechtigt ist, den Online- und Telefon-Banking-Vertrag aus wichtigem Grund zu kündigen,
 - sachliche Gründe im Zusammenhang mit der Sicherheit seiner Authentifizierungselemente dies rechtfertigen,
 - der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht oder
 - ein genutzter Zugangsweg bzw. ein im Zusammenhang mit einem Authentifizierungsverfahren zugelassenes Gerät von der Bank als unsicher eingestuft wird. Als Zugangsweg gelten auch Softwareanwendungen der Bank in allen zur Verfügung stehenden Versionen.
- (2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre postalisch, telefonisch oder online unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich. Der Teilnehmer kann eine von ihm veranlasste Sperrung nur postalisch oder mit telefonisch legitimiertem Auftrag aufheben lassen.

9.4 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Kunden verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters zum Zahlungskonto vorliegen.

¹ Zum Beispiel Überweisung, Dauerauftrag und Lastschrift.

to, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Bank wird den Kunden über eine solche Zugangsverweigerung auf dem vereinbarten Weg unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Bank die Zugangssperre auf. Hierüber unterrichtet sie den Kunden unverzüglich.

10. Haftung

10.1 Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags¹ und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

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

10.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

10.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge¹ vor der Sperranzeige

- (1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.
- (2) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn
 - es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
 - der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines 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 Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Um-

fang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach

- Nummer 7.1 Absatz 2,
- Nummer 7.1 Absatz 3,
- Nummer 7.3 oder
- Nummer 8.1 Absatz 1

dieser Bedingungen verletzt hat.

- (4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdienstenaufsichtsgesetz nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Inhärenz (siehe Nr. 2 Absatz 3 dieser Bedingungen).
- (5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.
- (6) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 dieser Bedingungen nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.
- (7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.
- (8) Ist der Kunde kein Verbraucher, gilt ergänzend Folgendes:
 - Der Kunde haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
 - Die Haftungsbeschränkung in Absatz 2, 1. Punkt findet keine Anwendung.

10.2.2 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-/Telefon-Banking-Verfügungen¹ entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.2.3 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.

¹ Zum Beispiel Überweisung, Dauerauftrag und Lastschrift.

Stand: 02/2025

Präambel

Kunden der norisbank GmbH (im Folgenden „Bank“) haben die Möglichkeit, im Online-Banking ein digitales Postfach (im Folgenden „Postfach“) zu nutzen. Das Postfach nutzt die Bank, um dem Kunden Bankdokumente zukommen zu lassen, die der Kunde dann in digitaler Fassung abrufen, herunterladen und speichern kann. Das Postfach dient der Kommunikation zwischen Bank und Kunden.

1. Allgemeines

- 1.1 Das Postfach ist ein elektronischer Briefkasten, in dem für den Kunden bestimmte persönliche Mitteilungen der Bank (im Folgenden „Bankmitteilungen“) in elektronischer Form verschlüsselt und dauerhaft abrufbar eingestellt werden.
- 1.2 Die Bank behält sich das Recht vor, das Postfach und zugehörige Funktionalitäten teilweise oder insgesamt weiterzuentwickeln, zu ändern oder zu ergänzen.

2. Aktivierung des Postfachs

- 2.1 Die Aktivierung des Postfachs setzt einen hierauf gerichteten Antrag im Zusammenhang mit der Beantragung einer Produkteröffnung voraus.
- 2.2 Die Annahme des Antrags seitens der Bank erfolgt durch die Freischaltung des Postfachs.

3. Voraussetzung und Zugangswege

Der Kunde benötigt zur Nutzung des Postfachs einen Internetzugang, eine gültige und üblicherweise für die Kommunikation mit Dritten verwendete E-Mail-Adresse, einen aktuellen, marktüblichen Internetbrowser und/oder einen Zugang zum jeweiligen Online-Banking oder sonstigen von der Bank zugelassenen Zugang über elektronische Medien (z. B. Mobile Banking App) sowie eine Zugangsberechtigung (z. B. mittels aktivem TAN-Verfahren) bei der Bank.

4. Zugang zum Postfach und Nutzungsrecht

- 4.1 Der Zugang zum Postfach erfolgt über eine Anmeldung im Online-Banking oder sonstigen von der Bank zugelassenen Zugang über elektronische Medien.
- 4.2 Bei der erstmaligen Anmeldung mit einem noch nicht für das Postfach autorisierten Gerät muss die Anmeldung im Postfach mit einer TAN bestätigt werden.
- 4.3 Der Kunde hat mit der TAN-Bestätigung die Möglichkeit, das Gerät als vertrauenswürdig einzustufen, sodass keine wiederholte Eingabe einer TAN notwendig ist. Der Kunde kann sich mit der Anmeldung in seinem Online-Banking oder sonstigen von der Bank zugelassenen Zugang über elektronische Medien dann automatisch im Postfach anmelden.

5. Leistungsangebot und -umfang

- 5.1 Im Postfach werden dem Kunden Bankmitteilungen in elektronischer Form eingestellt, soweit dies nach den gesetzlichen Vorgaben zulässig ist. Dabei handelt es sich insbesondere um folgende vertragsrelevante Bankerklärungen und vertraglich, gesetzlich und aufsichtsrechtlich geschuldete Informationen:
 - Vorvertragliche Informationen, Vertragsangebote und ggf. Erläuterungen,
 - Bankmitteilungen unter anderem zu Allgemeinen Geschäftsbedingungen sowie ggfs. deren Änderungen, Preisverzeichnis etc.,

- Kontoauszüge, Kontoabrechnungen, Zinsänderungen, Mitteilungen zu eingeräumten Kontoüberziehungen (z. B. Dispo-Kredit, Kreditlinien etc.) und zu geduldeten Kontoüberziehungen (z. B. Sollzinsen, Inanspruchnahmen, Beratungsangebote, Änderungen zur Höhe eines Dispo-Kredites etc.),

- Informationen, Mitteilungen und Erklärungen zum Inhalt, der Durchführung und der Beendigung von Darlehensverträgen (z. B. Zins- und Tilgungsplan, Saldenmitteilung, Angebot eines neuen gebundenen Sollzinssatzes nach Auslauf der Sollzinsbindung etc.),

- Mahnungen, Kündigungsandrohungen und Kündigungserklärungen.

- 5.2 Der Kunde kann die Bankmitteilungen dauerhaft online abrufen, herunterladen, speichern oder löschen. Das Löschen einer Mitteilung erfolgt durch den Kunden und ist endgültig.
- 5.3 Die Nutzung des Postfachs ist ausschließlich dem Kunden selbst und den von ihm hierzu berechtigten Personen vorbehalten.
- 5.4 Über den Eingang von Bankmitteilungen wird der Kunde mindestens einmal täglich an die von ihm mitgeteilte E-Mail-Adresse benachrichtigt.

6. Einstellung von Bankmitteilungen

- 6.1 Die Bank kommt ihrer Verpflichtung zur Übermittlung, Unterbringung oder Zurverfügungstellung von Bankmitteilungen auf einem dauerhaften Datenträger durch deren Einstellung in das Postfach nach. Hiervon bleiben etwaige Aufbewahrungspflichten der Bank (vgl. Nr. 7.3) unberührt.
- 6.2 Mit der Einrichtung des Postfachs ist der Kunde nach Maßgabe dieser Bedingungen ausdrücklich damit einverstanden, dass kein postalischer Versand der in das Postfach einzustellenden Bankmitteilungen stattfindet. Hiervon umfasst sind Bankmitteilungen sowohl für aktuelle als auch für zukünftig vom Kunden gewählte Bankleistungen, insbesondere auch diejenigen, die der Textform unterliegen. Die Bestimmung unter Nr. 1.2 bleibt unberührt.
- 6.3 Die Bankmitteilungen gehen dem Kunden spätestens einen Tag nach dem Zeitpunkt zu, in dem die Bank die Mitteilungen in das Postfach eingestellt und den Kunden über den Eingang von Bankmitteilungen per E-Mail informiert hat.
- 6.4 Kann die E-Mail-Benachrichtigung nicht zugestellt werden (z. B. wenn die E-Mail Adresse nicht mehr gültig ist), kann die Bank den Kunden kontaktieren. Die Bankmitteilungen können papierhaft zur Verfügung gestellt werden. Die Bank stellt dem Kunden hierfür kein Entgelt, sondern nur ihren Aufwendersersatz (insbesondere Porto) in Rechnung.

7. Speicherung der Bankmitteilungen

- 7.1 Die Bank speichert die eingestellten Bankmitteilungen während der Gesamtdauer der Nutzung des Online-Bankings durch den Kunden im Rahmen einer bestehenden Konto- oder Depotverbindung.
- 7.2 Die Bank stellt die Unveränderbarkeit der in das Postfach eingestellten und dort gespeicherten Bankmitteilungen im Rahmen einer bestehenden Konto- oder Depotverbindung sicher.
- 7.3 Die Bank ist innerhalb der gesetzlichen Aufbewahrungsfristen jederzeit in der Lage, dem Kunden auf dessen Anforderung eine papierhafte Ausfertigung dieser Bankmitteilungen zur Verfügung zu stellen. Ein hierfür ggf. anfallendes Entgelt ergibt sich aus dem Preis- und Leistungsverzeichnis der Bank.

8. Gewährleistung und Haftung

- 8.1 Das Postfach ist üblicherweise entsprechend der Online-Banking Funktionalität und vorbehaltlich üblicher Wartungsfenster ständig verfügbar. Für Störungen, insbesondere für vorübergehende, technisch bedingte Zugangsbeschränkungen zum Postfach, haftet die Bank nur bei Vorsatz und grober Fahrlässigkeit und stellt die Postfach Funktionalität lediglich in der jeweils aktuellen Form bereit. Soweit aus technischen Gründen ausnahmsweise Wartungsarbeiten mit Auswirkungen auf die Postfach Funktionalität erforderlich werden, wird die Bank den Kunden nach Möglichkeit rechtzeitig im Online-Banking oder auf einem anderen Weg (z. B. per E-Mail) darüber informieren.
- 8.2 Für die Anbindung an das Internet und zugehöriger Netzverbindung auf Kundenseite trägt der Kunde selbst Sorge. Im Falle länger anhaltender Störungen kann die Bank für Bankmitteilungen andere Kommunikationswege (z. B. Banking-Terminals der Deutschen Bank, postalischer Versand) nutzen.

9. Folgen der Beendigung der Geschäftsbeziehung

- 9.1 Bei Beendigung der Geschäftsbeziehung, Schließung des Online-Banking Zugangs oder sonstigen von der Bank zugelassenen Zugangs über elektronische Medien werden die zu diesem Zeitpunkt im Postfach eingestellten Bankmitteilungen – sofern noch nicht vom Kunden gelöscht – für einen Zeitraum von vier Jahren weiterhin über einen Download-Link zur Verfügung gestellt. Die Frist beginnt einen Tag nach Beendigung der Geschäftsbeziehung, des Online-Bankings oder sonstigen von der Bank zugelassenen Zugangs über elektronische Medien.
- 9.2 Der Link wird dem Kunden per E-Mail zugesendet. Ein entsprechendes Passwort, welches den Zugriff des Kunden auf den Link legitimiert, wird dem Kunden auf postalischem Weg zur Verfügung gestellt.

10. Datenschutz

Die Bank verarbeitet die personenbezogenen Daten des Kunden im Rahmen der geltenden Datenschutzgesetze ausschließlich zu den oben unter Nr. 1 genannten Zwecken. Der Kunde bzw. dessen Vertretungsberechtigter trägt dafür Sorge, dass im Rahmen einer Bevollmächtigung persönliche Mitteilungen und darin enthaltene personenbezogene Daten betreffend seine Person durch den Bevollmächtigten legitim zur Kenntnis genommen werden dürfen. Hinsichtlich weiterführender datenschutzrechtlicher Informationen wird verwiesen auf die geltenden Datenschutzhinweise des Online-Banking der Bank.

11. Ergänzende Geltung der Allgemeinen Geschäftsbedingungen

Ergänzend gelten die Allgemeinen Geschäftsbedingungen und Sonderbedingungen der Bank, insbesondere die Bedingungen für den Zugang zur Bank über elektronische Medien, die unter www.norisbank.de/bedingungen eingesehen werden können und dem Kunden auf Wunsch zur Verfügung gestellt werden.