Antrag für den Zugang zur norisbank GmbH über elektronische Medien

norisbank

Zurücksenden per Post: norisbank GmbH, 10910 Berlin
Interessentenservice: 030-310 66 000; **Internet:** www.norisbank.de

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

Name, Vorname/n

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

Anmeldung des Kontoinhabers für das noris Onlinebanking

Hiermit melde ich mein/e Konto/en und Depot/s unter der o.g. Kundennummer für das noris Onlinebanking an.
Damit kann ich bzw. der oben genannte Nutzer den Standardfunktionsumfang des noris Onlinebanking nutzen (z.B. Kontoumsätze einsehen, Überweisungen tätigen).
Für Online-Überweisungen wird ein Verfügungsrahmen von 2.500 Euro pro Tag beantragt, wenn nachstehend kein abweichender Rahmen beantragt wird.

Abweichend beantragter Verfügungsrahmen: Euro

Der Zugang zu meinen Konten und Depots über das noris Onlinebanking soll erfolgen über: (Bitte wählen Sie eines oder mehrere der nachstehenden Verfahren aus.)

☐ **mobileTAN-Verfahren**[1]
(für die Nutzung des noris Onlinebanking im Internet bzw. HBCI Plus). Für die Teilnahme übersenden Sie mir eine Online-PIN.
Die Gebühren gem. Preis- und Leistungsverzeichnis der Bank für die per SMS versandten mobileTAN sind vom oben genannten Konto abzubuchen.

Mobilfunknummer
(ausschließlich deutsche Mobilfunknummern sind zulässig)

☐ **iTAN-Verfahren**[1]
(für die Nutzung des noris Onlinebanking im Internet bzw. HBCI Plus). Für die Teilnahme übersenden Sie mir eine Online-PIN und einen TAN-Block.

Zusätzlich zum mobileTAN- oder iTAN-Verfahren:

☐ **photoTAN-Verfahren**[1]
(für die Nutzung des noris Onlinebanking im Internet bzw. HBCI Plus)
Es wird ein Smartphone (iOS, Android, Windows Phone) benötigt. Für die Teilnahme übersenden Sie mir einen Aktivierungsbrief.

☐ Ich möchte kein Smartphone nutzen. Bitte übersenden Sie mir zusätzlich ein photoTAN-Lesegerät zum Preis von 14,90 Euro inkl. Versandkosten

Die Kosten hierfür sind vom oben genannten Konto abzubuchen.
Ich ermächtige Sie zum Einzug des fälligen Rechnungsbetrages für das photoTAN-Lesegerät von meinem persönlichen Konto bei der norisbank GmbH.

Anmeldung zur Anzeige der Umsätze von Kreditkarten im Internet

Auftrag: Der Kontoinhaber soll die Einzelumsätze folgender Kreditkarten im Rahmen des noris Onlinebanking angezeigt bekommen. Die Umsätze werden unter der oben genannten Kundennummer angezeigt.

Karteninhaber | Kartennummer

Karteninhaber | Kartennummer

[1] Die Zusendung der Authentifizierungs-Instrumente erfolgt an die Adresse des Kontoinhabers, ggf. zur Weitergabe an o.g. Nutzer.

035 18000 91 160120 NB DE

Nutzung des Online-Banking Postfachs

☐ Hiermit melde ich mein/e Konto/en und Kreditkarte/n unter der o. g. Kundennummer für das noris Onlinebanking Postfach an.
Damit werden mir bestimmte persönliche Mitteilungen der Bank (z. B. Kontoauszüge, Rechnungsabschlüsse, Kreditkartenabrechnungen etc.) in elektronischer Form online bereitgestellt.
Details zu Umfang und Art der Mitteilungen erhalte ich unter www.norisbank.de/postfach.

Anmeldung des Kontoinhabers für das noris Telefonbanking

Hiermit melde ich mein/e Konto/en und Depot/s unter der o. g. Kundennummer für das noris Telefonbanking an. Bitte übersenden Sie mir eine Telefon-PIN.

Aufzeichnung der Telefonkommunikation

Ich bin damit einverstanden, dass die zwischen der Bank und dem Kontoinhaber übermittelte Telefonkommunikation zu Beweiszwecken automatisch aufgezeichnet und gespeichert wird.
Das Einverständnis wird mit der Antragsunterzeichnung erteilt.

Bedingungen

Maßgebend für die Geschäftsverbindung sind die Allgemeinen Geschäftsbedingungen der Bank und die Bedingungen für den Zugang zur norisbank GmbH über elektronische Medien, die Sonderbedingungen für die Nutzung des photoTAN-Verfahrens sowie die Sonderbedingungen zur Nutzung des Online-Banking Postfachs.
Auf Wunsch kann ich alle genannten Bedingungen auch unter der Internetadresse www.norisbank.de einsehen oder ferner zugesandt bekommen.

Besondere Hinweise zur sofortigen Vertragsausführung

☐ Ich erkläre mich ausdrücklich damit einverstanden, dass die Bank nach Annahme meines Vertragsantrages auf Abschluss des Vertrages, aber noch vor Ablauf der Widerrufsfrist mit der Ausführung dieses Vertrages beginnt.

Datenschutzrechtlicher Hinweis

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 an den markierten Stellen unterschreiben)

Datum	X Unterschrift des/der Kontoinhaber/s
Datum	X Unterschrift des/der Karteninhaber/s, sofern diese/r nicht Kontoinhaber/in

Empfangsbestätigung
Ich habe jeweils ein Exemplar

☐ der „Informationen zum Online- und Telefonbanking“ inklusive der Widerrufsbelehrung,
☐ des „Antrages für den Zugang zur norisbank GmbH über elektronische Medien“,
☐ der „Allgemeinen Geschäftsbedingungen” und der „Bedingungen für den Zugang zur norisbank GmbH über elektronische Medien“,
☐ der „Sonderbedingungen für die Nutzung des photoTAN-Verfahrens“,
☐ der „Sonderbedingungen zur Nutzung des Online-Banking Postfachs“

erhalten.

Datum	X Unterschrift des/der Kontoinhaber/s
Datum	X Unterschrift des/der Karteninhaber/s, sofern diese/r nicht Kontoinhaber/in

035 18000 91 160120 NB DE

Informationen zum Online- und Telefonbanking

Interessentenservice: 030 - 310 66 000
Internet: www.norisbank.de

norisbank

Vorvertragliche Informationen zum Onlinebanking und Telefonbanking der norisbank

Sehr geehrte Kundin, sehr geehrter Kunde,
bevor Sie im Fernabsatz (per Internet, Telefon oder Briefverkehr) mit uns Verträge abschließen, möchten wir Ihnen gemäß den gesetzlichen Bestimmungen (Artikel 246b EGBGB) einige allgemeine Informationen zur Bank, zur angebotenen Bankdienstleistung und zum Vertragsabschluss im Fernabsatz geben.

A1. Allgemeine Informationen zur Bank

Name und Anschrift der Bank
norisbank GmbH
Reuterstraße 122
53129 Bonn

Telefon
Interessentenservice: Interessentenservice: 030 - 310 66 000
24h-Kundenservice: Interessentenservice: 030 - 310 66 005
E-Mail: service@norisbank.de

Gesetzliche Vertretungsberechtigte der Bank
Thomas große Darrelmann (Vorsitzender), Marco Lindgens

Eintragung der Hauptniederlassung im Handelsregister
Handelsregister des Amtsgerichts Bonn: HRB 21185

Umsatzsteueridentifikationsnummer
DE226545047

Hauptgeschäftstätigkeit der Bank
Gegenstand des Unternehmens ist der Betrieb von Bankgeschäften aller Art mit Ausnahme von Investment-, Pfandbrief- und E-Geldgeschäften und das Betreiben von Anlagevermittlung, Anlageberatung, Abschlussvermittlung und Eigenhandel.

Zuständige Aufsichtsbehörden
Europäische Zentralbank (EZB), Sonnemannstraße 22, 60314 Frankfurt am Main und Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Graurheindorfer Straße 108, 53117 Bonn und Marie-Curie-Straße 24–28, 60439 Frankfurt am Main (Internet: www.bafin.de)

A2. Allgemeine Informationen zum Vertrag

Vertragssprache
Maßgebliche Sprache für dieses Vertragsverhältnis und die Kommunikation mit dem Kunden während der Laufzeit des Vertrages ist Deutsch.

Rechtsordnung und Gerichtsstand
Für den Vertragsschluss und die gesamte Geschäftsverbindung zwischen dem Kunden und der Bank gilt deutsches Recht (Nr. 6 Abs. 1 der Allgemeinen Geschäftsbedingungen der Bank). Es gibt keine vertragliche Gerichtsstandsklausel.

Außergerichtliche Streitschlichtung
Für die Beilegung von Streitigkeiten mit der Bank besteht für Privatkunden die Möglichkeit, den Ombudsmann der privaten Banken anzurufen. Näheres regelt die „Verfahrensordnung für die Schlichtung von Kundenbeschwerden im deutschen Bankgewerbe", die auf Wunsch zur Verfügung gestellt wird. Die Beschwerde ist in Textform (z.B. mittels Brief, Telefax oder E-Mail) an die Kundenbeschwerdestelle beim Bundesverband deutscher Banken e.V., Postfach 040307, 10062 Berlin, Fax: (030) 1663-3169, E-Mail: ombudsmann@bdb.de, zu richten.

Hinweis zum Bestehen einer freiwilligen Einlagensicherung
Die Bank ist dem Einlagensicherungsfonds des Bundesverbandes deutscher Banken e.V. angeschlossen (vgl. Nr. 20 der Allgemeinen Geschäftsbedingungen der Bank).

Zustandekommen des Vertrages
Der Kunde gibt gegenüber der Bank ein ihn bindendes Angebot auf Abschluss des Kontovertrages sowie der Teilnahmevereinbarung am noris Online- und Telefonbanking ab, indem er den ausgefüllten und unterzeichneten oder im Online-Banking mittels PIN/TAN bestätigten Antrag auf Eröffnung eines Kontos an die Bank übermittelt und dieser ihr zugeht. Der Kontovertrag kommt zustande, wenn die Bank dem Kunden nach der gegebenenfalls erforderlichen Legitimationsprüfung die Annahme des Vertrages erklärt. Voraussetzung für die Annahme des Vertrages ist, dass der Bank alle erforderlichen Unterlagen – einschließlich der Empfangsbestätigung dieser Information – vorliegen.

Hinweise zur sofortigen Vertragsausführung
Die Bank wird sofort nach Annahme des Kontovertrages und noch vor Ablauf der Widerrufsfrist mit der Ausführung dieses Vertrages und der auf dessen Grundlage abgeschlossenen weiteren Verträge beginnen, wenn der Kunde hierzu seine ausdrückliche Zustimmung erteilt. Die ausdrückliche Zustimmung holt die Bank bei Vertragsunterzeichnung ein.

B. Informationen zum noris Onlinebanking und noris Telefonbanking

Wesentliche Leistungsmerkmale des noris Onlinebanking
Durch den Abschluss der Teilnahmevereinbarung zum noris Onlinebanking ist der Kunde grundsätzlich zur Abwicklung seiner Bankgeschäfte per Internet (nachfolgend auch noris Onlinebanking genannt) berechtigt.
Der Umfang der Bankgeschäfte, die der Kunde per noris Onlinebanking abwickeln kann, richtet sich im Übrigen nach den zwischen Kunde und Bank getroffenen einzelnen Produktvereinbarungen (z.B. einem mit ihm geschlossenen Kontovertrag).

Folgende Dienstleistungen sind vom noris Onlinebanking erfasst:
- Inlandsüberweisungen
- Auslandsüberweisungen
- Zahlungsverkehrs- und Sparprodukte abschließen
- Daueraufträge einrichten, ändern und löschen
- Onlinelimitänderungen
- Adressdatenaktualisierung
- Abruf von Kontodaten
- Abruf von Kreditkartendaten

Für die Online-Bankgeschäfte des Kunden gibt es die Sicherheitssysteme mit persönlicher Identifikationsnummer (PIN) und Transaktionsnummern (TAN) der Bank, das sogenannte PIN-/TAN-Verfahren. Die 5-stellige PIN kann durch eine individuelle Wunsch-PIN ersetzt werden. Für die Autorisierung von Transaktionen kann wahlweise das photoTAN-Verfahren (mit kostenloser Smartphone-App für Apple iOS, Google Android und Microsoft Windows Phone oder einem optional bestellbaren Lesegerät), das mobileTAN-Verfahren (die TAN wird auf Anforderung per SMS an die hinterlegte Mobilfunknummer versandt) oder das iTAN-Verfahren (es wird eine Liste mit indizierten TAN bereitgestellt) genutzt werden. Im Internet wird bei der Übertragung zusätzlich zum PIN-/TAN-Verfahren eine SSL-Verschlüsselung eingesetzt, die die Daten des Kunden vor dem Zugriff Dritter schützt.

Wesentliche Leistungsmerkmale des noris Telefonbanking
Bei Vereinbarung des noris Telefonbanking kann der Kunde eine Reihe seiner Bankgeschäfte an 7 Tagen in der Woche und 24 Stunden am Tag am Telefon erledigen, z.B.
- generelle Informationen zum Produkt- und Serviceangebot abrufen,
- Zahlungsverkehr und Wertpapiergeschäfte abwickeln und
- Zahlungsverkehrs-, Spar- und Anlageprodukte abschließen.

Zur Abwicklung der telefonischen Bankgeschäfte über das noris Telefonbanking erhält der Kunde eine 5-stellige Telefon-PIN, die durch eine individuelle Wunsch-PIN ersetzt werden kann.

Preise
Die Teilnahme am noris Onlinebanking und noris Telefonbanking ist kostenlos. Der Preis für den Versand einer angeforderten mobileTAN per SMS ergibt sich aus Kapitel A4 des Preis- und Leistungsverzeichnisses. Das jeweils aktuelle Preis- und Leistungsverzeichnis kann der Kunde auf den Internetseiten der Bank unter www.norisbank.de einsehen. Auf Wunsch wird die Bank dieses dem Kunden zusenden. Ein photoTAN-Lesegerät kostet 14,90 Euro.

Hinweis auf vom Kunden zu zahlende Steuern und Kosten
- Steuern: keine.
- Die Kosten für die ihm seitens des Internet-Providers in Rechnung gestellten Verbindungen sowie sonstige eigene Kosten (z.B. für Ferngespräche, Porti) hat der Kunde selber zu tragen.

Zusätzliche Telekommunikationskosten
Es fallen keine zusätzlichen Telekommunikationskosten an. Bei der Nutzung des noris Telefonbanking entstehen dem Kunden pro Minute die Kosten eines Inlandsgesprächs.

Leistungsvorbehalt
Keiner.

035 18000 92 160927 NB DE

B. Informationen zum noris Onlinebanking und noris Telefonbanking (Fortsetzung)

Zahlung und Erfüllung des Vertrages
Zahlung: entfällt
Erfüllung: Die Bank erfüllt ihre Verpflichtung zur Erreichbarkeit dadurch, dass sie zu den für das jeweilige Angebot dem Kunden mitgeteilten Zeiten grundsätzlich erreichbar ist. Ein Anspruch darauf, jederzeit online und telefonisch erreichbar zu sein, besteht hingegen nicht. Im Übrigen gelten für die Erfüllung der Vereinbarungen über den Zugang zur Bank über Telefon und Online Service durch Bank und Kunden die Bedingungen für den Zugang zur norisbank GmbH über elektronische Medien.

Vertragliche Kündigungsregeln
Die Teilnahme am noris Onlinebanking oder noris Telefonbanking kann der Kunde formlos kündigen (Nr. 11 der Bedingungen für den Zugang zur norisbank GmbH über elektronische Medien).
Des Weiteren gelten die in Nr. 18 und 19 der Allgemeinen Geschäftsbedingungen für den Kunden und die Bank festgelegten Kündigungsregeln.

Mindestlaufzeit des Vertrages
Eine Mindestlaufzeit besteht nicht.

Sonstige Rechte und Pflichten von Bank und Kunde
Die Grundregeln für die gesamte Geschäftsverbindung zwischen Bank und Kunden sind in den Allgemeinen Geschäftsbedingungen der Bank beschrieben.
Die Grundregeln für die Teilnahme am noris Onlinebanking und/oder noris Telefonbanking zwischen Bank und Kunde sind in den Bedingungen für den Zugang zur norisbank GmbH über elektronische Medien aufgeführt. Vorgenannte Bedingungen stehen in deutscher Sprache zur Verfügung.

C. Widerrufsbelehrung

Widerrufsbelehrung bei im Fernabsatz geschlossenen Verträgen von Finanzdienstleistungen

Widerrufsrecht
Sie können Ihre Vertragserklärung innerhalb von 14 Tagen ohne Angabe von Gründen mittels einer eindeutigen Erklärung widerrufen. Die Frist beginnt nach Erhalt dieser Belehrung auf einem dauerhaften Datenträger, jedoch nicht vor Vertragsschluss und auch nicht vor Erfüllung unserer Informationspflichten gemäß Artikel 246b § 2 Absatz 1 in Verbindung mit Artikel 246b § 1 Absatz 1 EGBGB. Zur Wahrung der Widerrufsfrist genügt die rechtzeitige Absendung des Widerrufs, wenn die Erklärung auf einem dauerhaften Datenträger (z.B. Brief, Telefax, E-Mail) erfolgt. Der Widerruf ist zu richten an:

norisbank GmbH
Reuterstraße 122
53129 Bonn
Fax: 030 - 310 66 012
E-Mail: widerruf.fernabsatz@norisbank.de

Widerrufsfolgen
Im Falle eines wirksamen Widerrufs sind die beiderseits empfangenen Leistungen zurückzugewähren. Sie sind zur Zahlung von Wertersatz für die bis zum Widerruf erbrachte Dienstleistung verpflichtet, wenn Sie vor Abgabe Ihrer Vertragserklärung auf diese Rechtsfolge hingewiesen wurden und ausdrücklich zugestimmt haben, dass wir vor dem Ende der Widerrufsfrist mit der Ausführung der Gegenleistung beginnen. Besteht eine Verpflichtung zur Zahlung von Wertersatz, kann dies dazu führen, dass Sie die vertraglichen Zahlungsverpflichtungen für den Zeitraum bis zum Widerruf dennoch erfüllen müssen. Ihr Widerrufsrecht erlischt vorzeitig, wenn der Vertrag von beiden Seiten auf Ihren ausdrücklichen Wunsch vollständig erfüllt ist, bevor Sie Ihr Widerrufsrecht ausgeübt haben. Verpflichtungen zur Erstattung von Zahlungen müssen innerhalb von 30 Tagen erfüllt werden. Die Frist beginnt für Sie mit der Absendung Ihrer Widerrufserklärung, für uns mit deren Empfang.

Besondere Hinweise
Bei Widerruf dieses Vertrags sind Sie auch an einen mit diesem Vertrag zusammenhängenden Vertrag nicht mehr gebunden, wenn der zusammenhängende Vertrag eine Leistung betrifft, die von uns oder einem Dritten auf der Grundlage einer Vereinbarung zwischen uns und dem Dritten erbracht wird.

Ende der Widerrufsbelehrung

Gültigkeitsdauer dieser Informationen
Diese Informationen (Stand: 09/16) sind bis auf Weiteres gültig und stehen nur in deutscher Sprache zur Verfügung.

Mit freundlichen Grüßen
Ihre norisbank GmbH

035 18000 92 160927 NB DE

Bedingungen für den Zugang zur norisbank GmbH (nachstehend Bank) über elektronische Medien

norisbank

Interessentenservice: 030 - 310 66 000
Internet: www.norisbank.de

Stand: August 2015

1. Leistungsangebot

(1) Der Kontoinhaber kann Bankgeschäfte mittels Online- und Telefon-Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Online- und Telefon-Banking abrufen. Darüber hinaus kann der Kontoinhaber das Zugangsmedium Telefax nutzen.

(2) Kontoinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer" bezeichnet.

(3) Für die Nutzung der Zugangsmedien gelten die mit der Bank gesondert vereinbarten Verfügungslimite.

2. Voraussetzungen zur Nutzung der elektronischen Medien

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften über elektronische Medien 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).

Dieser Prozess wird als Authentifizierungsverfahren bezeichnet.

2.1 Personalisierte Sicherheitsmerkmale
Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:
- die persönliche Identifikationsnummer (PIN) oder das persönliche Passwort,
- einmal verwendbare Transaktionsnummern (TAN),
- der Nutzungscode für die elektronische Signatur,
- der Aktivierungscode für ein Authentifizierungsinstrument oder
- ein von einem von der Bank zugelassenen Authentifizierungsinstrument geprüftes biometrisches Merkmal wie der eigene Fingerabdruck (Fingerprint).

2.2 Authentifizierungsinstrumente
Die TAN beziehungsweise die elektronische Signatur können dem Teilnehmer auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:
- auf einer Liste mit einmal verwendbaren TAN (iTAN),
- mittels eines mobilen Endgerätes (z.B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN), auf einer Chipkarte mit Signaturfunktion (z.B. HBCI) oder
- auf einem sonstigen Authentifizierungsinstrument u.a. über eine Softwareanwendung bzw. „App" der Bank auf elektronischen Geräten wie Smartphone, Tablet oder Lesegerät z.B. für das photoTAN-Verfahren oder über ein für eine elektronische Signatur ausreichend geeignetes Lesegerät, auf dem sich Signaturschlüssel befinden.

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. 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.

Sofern die Bank für einzelne hier aufgeführte Leistungen ein Entgelt verlangt, ist der jeweilige Preis im Preis- und Leistungsverzeichnis der Bank bzw. der jeweiligen Teilnahmevereinbarung ausgewiesen. Für Änderungen und Preise gilt Ziffer 12 der Allgemeinen Geschäftsbedingungen der Bank, wenn keine besondere Vereinbarung zwischen Bank und Kunde getroffen wurde.

3. Zugang über elektronische Medien

Der Teilnehmer erhält Zugang zu Online- und Telefon-Banking, wenn
- dieser die Kontonummer oder seinen individuellen Benutzernamen und seine PIN oder seinen Token oder sein Passwort oder seine elektronische Signatur der Bank übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.

Nach Gewährung des Zugangs zum Online- und Telefon-Banking kann der Teilnehmer Informationen abrufen und Aufträge erteilen.

4. Online- und Telefon-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung
Der Teilnehmer muss Online-Banking-Aufträge (z.B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten personalisierten Sicherheitsmerkmal (z.B. TAN oder elektronische Signatur) autorisieren und der Bank mittels Online-Banking übermitteln.

Der Teilnehmer kann Telefon-Banking-Aufträge nur nach erfolgreicher Autorisierung mit dem vereinbarten personalisierten Sicherheitsmerkmal erteilen. Die Bank bestätigt den Eingang des Auftrags auf dem vom Teilnehmer für den Auftrag gewählten Zugangsweg.

4.2 Widerruf von Aufträgen
Die Widerrufbarkeit eines Online- und Telefon-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- und Telefon-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Online- und Telefon-Banking ausdrücklich vor.

5. Bearbeitung von Online- und Telefon-Banking-Aufträgen durch die Bank

(1) Die Bearbeitung der Online- und Telefon-Banking-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 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 sich mit seinem personalisierten Sicherheitsmerkmal (z.B. PIN) legitimiert.
- 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 Zahlung 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 innerhalb der gleichen Kundennummer oder An- und Verkäufe von Wertpapieren gelten diese Betragsgrenze nicht.
- Die 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- 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.

(4) Bearbeitung von Telefaxaufträgen durch die Bank: Bei Verfügungen einschließlich der Einrichtung oder Änderung von Daueraufträgen genügt zur Legitimation die Unterschrift auf dem Fax. Die Bank kann sich vor Ausführung eines Auftrages telefonisch vom Teilnehmer die Ordnungsmäßigkeit bestätigen lassen. Soweit eine solche Autorisierung nicht möglich ist oder aus anderen Gründen erhebliche Zweifel an der Echtheit des Auftrages bestehen, wird die Bank den Auftrag nicht ausführen. In diesem Fall erhält der Teilnehmer eine Mitteilung über die Nichtausführung.

035 18000 93 150723 NB DE

6. Information des Kontoinhabers über Online- und Telefon-Banking-Verfügungen

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

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum Online- und Telefon-Banking
Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online- und Telefon-Banking nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle (z.B. Internetadresse) und den Telefon-Banking-Zugangskanal (Telefonnummern) herzustellen.

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- und Telefon-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 dem dazugehörigen personalisierten Sicherheitsmerkmal das Online- und Telefon-Banking-Verfahren missbräuchlich nutzen.

(2) Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:
- Das personalisierte Sicherheitsmerkmal darf nicht außerhalb des zugelassenen Authentifizierungsverfahrens elektronisch gespeichert werden (z.B. im Kundensystem oder auf einem Endgerät).
- Das Authentifizierungsinstrument (z.B. die Softwareanwendung der Bank oder das zugelassene Lesegerät) darf sich ausschließlich in der alleinigen Verfügungsgewalt des Teilnehmers befinden. Ein Zugriff auf personalisierte Sicherheitsmerkmale durch unberechtigte Dritte über das Authentifizierungsinstrument ist durch angemessene Sicherheitsmaßnahmen des Teilnehmers (z.B. Passwortschutz bei Smartphone) zu unterbinden.
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das personalisierte Sicherheitsmerkmal darf nur innerhalb der von der Bank zugelassenen Authentifizierungsverfahren eingegeben werden.
- Sollte der Teilnehmer im Rahmen eines Authentifizierungsverfahrens Systeme oder Verfahren eines Dritten verwenden, so übernimmt die Bank keine Verantwortung für die Auswahl, Sicherheit oder Überwachung dieser Systeme oder Verfahren. Der Teilnehmer bleibt bei einer Nutzung dieser Dritt-Systeme oder -Verfahren für die Einhaltung seiner Pflichten aus diesen Bedingungen verantwortlich.
- Das personalisierte Sicherheitsmerkmal darf nicht an unberechtigte Dritte (z.B. per E-Mail oder Telefon) weitergegeben werden.
- Die PIN, das Passwort und der Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung z.B. eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung eines Authentifizierungsinstruments nicht mehr als eine TAN verwenden oder ein sonstiges personalisiertes Sicherheitsmerkmal einsetzen.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z.B. Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.
- 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.
- Anfragen außerhalb der bankseitig zur Verfügung gestellten originären Zugangswege, in denen nach vertraulichen Daten wie PIN, Geheimzahl oder Passwort/Online-TAN gefragt wird, dürfen nicht beantwortet werden.
- Auf einer Login-Seite (Startseite) zum (vermeintlichen) Online-Banking der Bank darf keine TAN eingegeben werden.
- 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.
- Die Softwareanwendungen der Bank sind ausschließlich direkt von der Bank oder von einem von der Bank benannten Anbieter zu beziehen.

7.3 Sicherheit des Kundensystems
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).

7.4 Kontrolle durch Abgleich 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) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z.B. Mobiltelefon oder Lesegerät) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Autorisierung (z.B. Eingabe der TAN) die Übereinstimmung der angezeigten Daten mit den für die Transaktion 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, den Diebstahl oder die missbräuchliche Verwendung des Authentifizierungsinstruments oder des zugehörigen Gerätes (z.B. Smartphone mit installierter Banksoftwareanwendung zur Authentifizierung) 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.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge
Der Kontoinhaber 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 vom Teilnehmer bezeichneten Banking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument.

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 des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals dies rechtfertigen,
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments 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 Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre postalisch, telefonisch oder online 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 Kontoinhaber unverzüglich. Der Teilnehmer kann eine von ihm veranlasste Sperrung nur postalisch oder mit telefonisch legitimiertem Auftrag aufheben lassen.

035 18000 93 150723 NB DE

10. Haftung

10.1 Haftung der Bank bei einer nicht autorisierten Online- und Telefon-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online- und Telefon-Banking-Verfügung

Die Haftung der Bank bei einer nicht autorisierten Online- und Telefon-Banking-Verfügung und einer nicht oder fehlerhaft 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 Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigem Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verloren gegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 Euro nach Absatz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 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 und der Schaden dadurch eingetreten ist.

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

- den Verlust, Diebstahl oder die missbräuchliche Verwendung des Authentifizierungsinstruments, des zugehörigen Gerätes (z.B. Smartphone mit installierter Banksoftwareanwendung zur Authentifizierung) oder des personalisierten Sicherheitsmerkmals nicht unverzüglich der Bank anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1 Absatz 1),
- das personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2 Absatz 2, 1. Punkt),
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1, 2. Punkt),
- das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2, 4. Punkt),
- das personalisierte Sicherheitsmerkmal außerhalb des Online- und Telefon-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2, 6. Punkt),
- das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2, 7. Punkt),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2, 8. Punkt),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z.B. Mobiltelefon), auch für das Online-Banking nutzt (siehe Nummer 7.2 Absatz 2, 9. Punkt),
- die Softwareanwendungen der Bank nicht direkt von der Bank oder von einem von der Bank benannten Anbieter bezieht (siehe Nummer 7.2 Absatz 2, 14. Punkt),
- die auf seinem Authentifizierungsinstrument angezeigten Auftragsdaten nicht prüft (siehe Nummer 7.4),
- bei Abweichen der Daten auf dem Authentifizierungsinstrument von den für die Transaktion vorgesehenen Daten den Vorgang nicht abbricht und die Bank nicht unverzüglich informiert (siehe Nummer 7.4).

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

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-Verfügungen 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.

035 18000 93 150723 NB DE

Sonderbedingungen zur Nutzung des Online-Banking Postfachs

norisbank

24h-Kundenservice: 030 - 310 66 005
Internet: www.norisbank.de

Sonderbedingungen zur Nutzung des Online-Banking Postfachs

1. Auftrag zur Einrichtung des Postfachs / Leistungsumfang

Die Bank richtet dem am Online-Banking der Bank teilnehmenden Kunden auf seinen Wunsch ein Postfach – als seinen elektronischen Briefkasten – ein, in dem sie für ihn bestimmte persönliche Mitteilungen der Bank (z.B. Kontoauszüge, Rechnungsabschlüsse, Kreditkartenabrechnungen etc.) in elektronischer Form online bereitstellt. Welche Mitteilungen die Bank dort konkret einstellt, teilt sie dem Kunden vor erstmaliger Nutzung des Postfachs gesondert mit. Der Kunde kann sich die Unterlagen online ansehen, diese herunterladen, ausdrucken und archivieren. Deren Nutzung ist ausschließlich dem Kunden selbst und den von ihm hierzu bevollmächtigten Personen vorbehalten.

Auf Wunsch des Kunden benachrichtigt die Bank ihn von einer in dem Postfach eingegangenen Mitteilung nach seiner Wahl durch E-Mail oder über SMS. Bei Nutzung der SMS fallen Kosten an, die die Bank an den Kunden weitergibt. Deren Höhe ergibt sich aus dem „Preis- und Leistungsverzeichnis" der Bank.

2. Zugang

Die Mitteilungen der Bank gehen dem Kunden spätestens in dem Zeitpunkt zu, in dem dieser die Informationen aus dem Postfach abgerufen hat.

3. Verzicht auf papierhafte Zustellung

Mit der Einrichtung des Postfachs verzichtet der Kunde nach Maßgabe dieser Bedingungen ausdrücklich auf den postalischen Versand der in das Postfach einzustellenden Mitteilungen. Die Bank kommt ihrer Verpflichtung zur Übermittlung, Unterrichtung oder zu einem anderweitigen Zurverfügungstellen der betreffenden Mitteilungen durch deren Einstellung in das Postfach nach.

Die Bank ist jedoch berechtigt, ihrem Kunden die in das Postfach bereits eingestellten Mitteilungen ergänzend auf dem Postweg oder in sonstiger Weise zuzusenden, sofern die gesetzlichen Vorgaben dies erforderlich machen, oder die Bank dies auch unter Berücksichtigung des Kundeninteresses für zweckmäßig hält. Hiervon wird die Bank insbesondere dann Gebrauch machen, wenn der Kunde seine in das Postfach eingestellten Bankmitteilungen längere Zeit nicht abgerufen hat. Die Bank stellt dem Kunden hierfür kein Entgelt in Rechnung, nur der hierfür entstehende Aufwand (Porto) wird in Rechnung gestellt.

4. Zusendung von Kontoauszügen und sonstigen Mitteilungen der Bank auf Verlangen des Kunden

Auf Verlangen des Kunden wird die Bank dem Kunden die in das Postfach eingestellten Mitteilungen zusätzlich auf dem postalischen Weg zusenden. Das hierfür anfallende Entgelt ergibt sich aus dem „Preis- und Leistungsverzeichnis" der Bank.

5. Mitwirkungspflichten des Kunden

Der Kunde verpflichtet sich, das Postfach regelmäßig auf neu hinterlegte Mitteilungen durchzusehen, ggf. diese zeitnah abzurufen und unverzüglich auf Richtigkeit und Vollständigkeit hin zu überprüfen sowie etwaige Einwendungen unverzüglich zu erheben.

6. Unveränderbarkeit der Daten

Die Bank stellt die Unveränderbarkeit der in das Postfach eingestellten Dokumente sicher, sofern diese innerhalb des Postfachs gespeichert oder aufbewahrt werden.

7. Speicherung der Dokumente

Die Bank speichert die eingestellten Mitteilungen während der Gesamtdauer der Nutzung des digitalen Postfachs durch den Kunden im Rahmen einer bestehenden Konto- oder Depotverbindung. Die Bank ist innerhalb der gesetzlichen Aufbewahrungsfristen jederzeit in der Lage, dem Kunden auf dessen Anforderung eine papierhafte Ausfertigung dieser Mitteilungen zur Verfügung zu stellen.

8. Kündigung durch den Kunden

Der Kunde kann die Nutzung des digitalen Postfachs ohne Angabe von Gründen jederzeit kündigen. Eine Kündigung ist auch online über die Deaktivierung des Postfachs („Button-Lösung") möglich. Die Bank wird dem Kunden die für das digitale Postfach vorgesehenen Mitteilungen nach Wirksamwerden der Kündigung wieder auf dem vor Einrichtung des digitalen Postfachs vereinbarten Wege zukommen lassen. Im Anschluss an die Kündigung des digitalen Postfachs kann der Kunde aber weiterhin im Rahmen einer bestehenden Konto- und Depotverbindung auf die bereits eingestellten Mitteilungen zugreifen. Bei Beendigung der Konto- und Depotbeziehung werden noch nicht vom Kunden abgerufene wichtige Mitteilungen mittels Brief zur Verfügung gestellt.

9. Anerkennung durch Finanzbehörden

Die im Postfach bereitgestellten Bankmitteilungen, wie z.B. der elektronische Kontoauszug oder Rechnungsabschluss, erfüllen nach Auffassung der Finanzverwaltung weder die Anforderungen der steuerlichen Aufbewahrungspflicht nach § 147 AO noch die einer Rechnung im Sinne des Umsatzsteuergesetzes. Sie werden daher nur im Privatkundenbereich und damit nur für den Kontoinhaber anerkannt, der nicht buchführungs- und aufzeichnungspflichtig i. S. d. §§ 145 ff. AO ist. Die Bank gewährleistet nicht, dass die Finanzbehörden die im Posteingang gespeicherten Informationen anerkennen. Der Kunde sollte sich darüber vorher bei dem für ihn zuständigen Finanzamt informieren.

Ergänzend gelten die Allgemeinen Geschäftsbedingungen und Sonderbedingungen der Bank, die unter https://www.norisbank.de/service/formulare.html eingesehen werden können und dem Kunden auf Wunsch auch auf dem Postweg zugesandt werden.

Sonderbedingungen zur Nutzung des photoTAN-Verfahrens

norisbank

24h-Kundenservice: 030 - 310 66 005
Internet: www.norisbank.de

Sonderbedingungen für die Nutzung des photoTAN-Verfahrens

Die photoTAN ist ein Sicherheitsverfahren im Online-Banking. Hierbei kann ein Kontoinhaber oder ein Bevollmächtigter (im Folgenden einheitlich als „Teilnehmer" bezeichnet), der sich für das photoTAN-Verfahren registriert hat, die für die Erteilung eines Auftrages erforderliche Transaktionsnummer (TAN) mittels der photoTAN-App bzw. des -Lesegerätes durch Abfotografieren einer farbigen photoTAN-Grafik generieren. Eine photoTAN kann nur einmalig und für den konkret erteilten Auftrag verwendet werden.

Für die Nutzung des photoTAN-Verfahrens gelten die Allgemeinen Geschäftsbedingungen der Bank, die Bedingungen für den Zugang zur Bank über elektronische Medien und für den Electronic Broking Service sowie diese Sonderbedingungen für die Nutzung des photoTAN-Verfahrens.

1. Personalisiertes Sicherheitsmerkmal

Bei dem personalisierten Sicherheitsmerkmal handelt es sich um den Aktivierungscode, der dem Teilnehmer in Form einer Aktivierungsgrafik in einem Aktivierungsbrief zur Verfügung gestellt wird, damit er nach seiner Registrierung das photoTAN-Verfahren aktivieren kann.

2. Authentifizierungsinstrumente

Die photoTAN kann dem Teilnehmer über die photoTAN-App auf einem Smartphone oder über ein von der Bank zur Verfügung gestelltes photoTAN-Lesegerät übermittelt werden (Authentifizierungsinstrumente).

3. Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

Zum Schutz des personalisierten Sicherheitsmerkmals sowie der Authentifizierungsinstrumente ist der Teilnehmer verpflichtet, diese geheim zu halten und vor dem Zugriff anderer Personen sicher zu verwahren.

Die photoTAN-App ist ausschließlich direkt von der Bank oder von einem von der Bank genannten Anbieter zu beziehen.

4. Vergleich der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank wird dem Teilnehmer die Daten aus seinem Auftrag zur Bestätigung im Online-Banking anzeigen und eine Autorisierung durch Eingabe der TAN verlangen. Der Teilnehmer ist verpflichtet, vor der Autorisierung (Eingabe der TAN) die Übereinstimmung der im Online-Banking angezeigten Daten mit den in seinem Authentifizierungsinstrument dargestellten Daten (z. B. Betrag, IBAN des Zahlungsempfängers, Wertpapierkennnummer) zu prüfen. Eine Autorisierung des Auftrags durch den Teilnehmer darf nur erfolgen, wenn die Daten im Online-Banking und im Authentifizierungsinstrument übereinstimmen.

5. Sperranzeige

Stellt der Teilnehmer den Verlust oder den Diebstahl eines Authentifizierungsinstruments (z.B. Smartphone mit installierter photoTAN-App, Lesegerät) oder des personalisierten Sicherheitsmerkmals, 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).

6. Sperre auf Veranlassung der Bank

Die Bank darf die Zulassung eines Authentifizierungsinstruments zurückziehen und dieses für das photoTAN-Verfahren sperren, wenn

- Anzeichen für eine missbräuchliche Nutzung des Authentifizierungsinstruments vorliegen,
- das Authentifizierungsinstrument abhandengekommen ist,
- sonstige Sicherheitserfordernisse die Sperre gebieten.

7. Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach den Bedingungen für den Zugang zur Bank über elektronische Medien vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn

- er den Verlust oder Diebstahl des Authentifizierungsinstruments oder des zugehörigen Gerätes (z.B. Smartphone mit installierter photoTAN-App, Lesegerät) oder des Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er davon Kenntnis erlangt hat,
- die photoTAN-App der Bank nicht direkt von der Bank oder einem von der Bank benannten Anbieter bezieht, oder
- die auf seinem Authentifizierungsinstrument angezeigten Auftragsdaten nicht prüft oder trotz fehlender Übereinstimmung der Daten die entsprechende Transaktion freigibt.