

Anpassung unserer Allgemeinen Geschäftsbedingungen (AGB) – was sich für Sie ändert

Sehr geehrte Damen und Herren,

unsere Allgemeinen Geschäftsbedingungen (AGB) ändern sich zum 14.09.2019. Was heißt das für Sie?

Noch mehr Sicherheit bei der Authentifizierung

Die neuen Vorgaben der zweiten EU-Zahlungsdiensterichtlinie (PSD2) gelten europaweit ab dem 14.09.2019. Wir als Bank sind verpflichtet, für Ihr Girokonto eine „starke Kundenauthentifizierung“ zu verlangen.

Was ändert sich durch die starke Kundenauthentifizierung? Für jeden Zahlungsauftrag und jeden Log-in ins Internetbanking müssen zwei voneinander unabhängige Sicherheitsmerkmale verwendet werden. Das Merkmal für die Freigabe wird dynamisch für den jeweiligen Vorgang generiert. Die iTAN ist für die starke Kundenauthentifizierung nicht geeignet und darf nicht mehr für Girokonten genutzt werden.

Das neue Standardverfahren für Freigaben und Zahlungen ist unsere Banking to go App, denn diese passen wir permanent an die aktuellen Anforderungen an. Alternativ können Sie auch die mTAN nutzen – und für alle ohne Handy kommt rechtzeitig zum 14.09.2019 der photoTAN-Generator dazu.

Ihre VISA Card wird zur Debitkarte

Die Kartenumsätze werden am Tag des Eingangs bei der ING auf dem Girokonto gebucht. Die VISA Card auszutauschen ist nicht nötig – ihre Funktionen bleiben dieselben.

Digitale VISA Card und girocard

Wir möchten auf künftige Entwicklungen gut vorbereitet sein und nehmen die Regelungen für digitale Karten in unsere Bedingungen mit auf.

Was ändert sich noch?

Schauen Sie bitte in die beigegefügtten Bedingungen. Dort finden Sie die wesentlichen Änderungen.

Wichtig für Sie:

Wenn Sie uns bis zum 13.09.2019 keinen Widerspruch senden, gehen wir davon aus, dass Sie den Änderungen zustimmen. Sie gelten dann als genehmigt. Wenn Sie mit den AGB-Änderungen nicht einverstanden sind, haben Sie das Recht, Ihr Girokonto fristlos und kostenfrei zu kündigen.

Und: Wenn Sie den geänderten Vereinbarungen zum Internetbanking inklusive Post-Box widersprechen, müssen wir leider Ihren Zugang zum Internetbanking ab 14.09.2019 sperren.

Mit freundlichen Grüßen

Ihre ING



Matthias Bayer
Leiter Service



Christine Gaida
Stellvertretende Leiterin Service

Anpassung unserer Allgemeinen Geschäftsbedingungen

Was sich für Sie ändert

Die Anpassungen gelten ab 14.09.2019

Vereinbarungen zum Internetbanking inklusive Post-Box

1. Einleitung

Die ING und der Kunde vereinbaren, dass die Konto- und Depotführung sowie die Abwicklung von Bank- und Wertpapiergeschäften per Internetbanking inklusive Post-Box erfolgen.

Die Nutzung der Banking to go App wird als das Standardverfahren zur Authentifizierung und Autorisierung vereinbart.

Unter Internetbanking sind die Banking- und Brokerage-Funktionen auf der ING-Website (inkl. Mobile Banking), die Banking to go App sowie alle Funktionen und Applikationen zu verstehen, welche die ING dem Kunden zur Verfügung stellt.

2. Teilnahme

(1) Der Kunde kann Bank- und Wertpapiergeschäfte mittels Internetbanking in dem angebotenen Umfang abwickeln. Zudem kann er Informationen der ING mittels Internetbanking abrufen. Des Weiteren ist er gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösdienste und Kontoinformationsdienste gem. § 1 Absatz 33 und 34 Zahlungsdienstleistungsgesetz (ZAG) zu nutzen. Darüber hinaus kann der Kunde von ihm ausgewählte sonstige Drittdienste nutzen.

(2) Die ING hat das Recht, den Umfang der über das Internetbanking abwickelbaren Geschäftsvorgänge sowie die Art und Weise der Nutzung des Internetbanking unter Berücksichtigung der berechtigten Belange des Kunden jederzeit zu verändern oder von weiteren Auflagen abhängig zu machen. Die ING wird den Kunden über derartige Änderungen rechtzeitig in geeigneter Form unterrichten.

3. Nutzungsvoraussetzungen

(1) Der Kunde kann das Internetbanking nutzen, wenn die Bank ihn authentifiziert hat.

(2) Authentifizierung ist das Verfahren, mit dessen Hilfe die ING die Identität des Kunden oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Kunden überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Kunde sich gegenüber der ING als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 4 dieser Vereinbarungen) sowie Aufträge erteilen (siehe Nummer 5 dieser Vereinbarungen).

(3) Authentifizierungselemente sind

- › Wissensselemente, also etwas, das nur der Kunde weiß (z.B. die persönliche Geheimzahl (PIN))
- › Besitzelemente, also etwas, das nur der Kunde besitzt (z.B. mobiles Endgerät, das für die Nutzung der Banking to go App durch den Kunden registriert ist oder ein Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern (TAN), die den Besitz des Kunden nachweisen, wie den TAN-Generator), oder
- › Seinsselemente, also etwas, das der Kunde ist (Inhärenz, z.B. Fingerabdruck als biometrisches Merkmal des Kunden).

(4) Die Authentifizierung des Kunden erfolgt, indem der Kunde gemäß den Anforderungen der ING das Wissensselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinsselements an die ING übermittelt.

4. Zugang zum Internetbanking (Login)

(1) Der Kunde erhält Zugang zum Internetbanking der ING, wenn

- › er seine Zugangsdaten (z.B. Zugangsnummer, PIN, DiBa Key) angibt und
- › er sich unter Verwendung des oder der von der ING angeforderten Authentifizierungselemente ausweist und
- › keine Sperre des Zugangs vorliegt.

Nach Gewährung des Zugangs zum Internetbanking kann der Kunde auf Informationen zugreifen oder nach Nummer 5 dieser Vereinbarungen Aufträge erteilen.

(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 ING den Kunden auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Online-Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kunden und die Kontonummer sind für den vom Kunden genutzten Zahlungsauslösdienst und Kontoinformationsdienst keine sensiblen Zahlungsdaten (§ 1 Absatz 26 Satz 2 ZAG).

(3) Die von der ING dem Kunden erteilten Wissensselemente muss der Kunde in nur ihm bekannte Wissensselemente umwandeln. Erst dann stehen die Dienste des Internetbanking dem Kunden zur Verfügung. Er kann jederzeit seine Wissensselemente ändern und seine Authentifizierungselemente sperren bzw. löschen und neue anfordern bzw. registrieren. Bei einer Änderung der Authentifizierungselemente werden die bisherigen ungültig. Eine Sperre kann durch ein vom Kunden unterzeichnetes Schreiben (im Original, nicht per Telefax), per Telebanking oder über das Internetbanking veranlasst werden. In Notfällen steht die Telefonnummer des

Rund-um-die-Uhr-Sperrdienstes zur Verfügung, die über die Internetseite der ING zu erfahren ist.

(4) Falls der Zugriff auf das Internetbanking über Kommunikationsmittel erfolgt, die anderen Betreibern unterstehen, obliegt es dem Kunden, die dafür notwendigen Vorkehrungen zu treffen und sicherzustellen, dass alle gesetzlichen und technischen Vorschriften eingehalten werden.

5. Auftragserteilung

(1) Der Kunde muss einem per Internetbanking erteilten Auftrag (z.B. einer Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat der Kunde hierzu Authentifizierungselemente (z.B. bei Nutzung der Banking to go App die Eingabe der mobilePIN oder die Verwendung des Fingerabdrucks) zu verwenden. Die ING bestätigt mittels Internetbanking den Eingang des Auftrags.

(2) 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 Internetbanking erfolgen, es sei denn, das Internetbanking sieht eine Widerrufsmöglichkeit ausdrücklich vor.

6. Banking to go App als Standardverfahren

(1) Die ING und der Kunde vereinbaren die Nutzung der Banking to go App als das Standardverfahren zur Authentifizierung und Autorisierung.

(2) Die ING stellt die Banking to go App zur Installation auf hierzu geeigneten mobilen Endgeräten (z.B. Smartphone, Tablet) zur Verfügung. Über die Nutzung der Banking to go App werden Besitz, Wissens- und/oder Seinsselemente (je nach persönlicher Einstellung) als Authentifizierungselemente zur Authentifizierung im Rahmen des Zugangs zum Internetbanking und zur Autorisierung von Aufträgen im Internetbanking kombiniert.

(3) Von der ING als Alternative zur Banking to go App angebotene weitere Verfahren zur Authentifizierung und Autorisierung (z.B. TAN-Übermittlung per SMS [mTAN] oder mittels TAN-Generator) sind Sonderleistungen, für die gegebenenfalls Entgelte nach Maßgabe des Preis- und Leistungsverzeichnisses anfallen.

7. Auftragsbearbeitung

(1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung) im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem im Preis- und Leistungsverzeichnis angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag der ING gemäß Preis- und Leistungsverzeichnis, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.

(2) Die ING wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- › Der Kunde hat den Auftrag autorisiert (vgl. Nummer 5 Absatz 1 dieser Vereinbarungen).
- › Die Berechtigung des Kunden für die jeweilige Auftragsart (zum Beispiel Wertpapierorder) liegt vor.
- › Das Internetbanking-Datenformat ist eingehalten.
- › Das Internetbanking-Verfügungslimit ist nicht überschritten.
- › Zur Ausführung von Aufträgen zum Kauf oder Verkauf von Wertpapieren oder zur Ausübung von Bezugsrechten reicht das Guthaben, ein für Wertpapiergeschäfte nutzbarer Kredit oder der Depotbestand des Kunden aus.
- › 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 vorstehenden Ausführungsbedingungen vor, führt die ING die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 nicht vor, wird die ING den Auftrag nicht ausführen. Sie wird dem Kunden mittels Internetbanking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtet werden können.

8. Information des Kunden über Internetbanking-Verfügungen

(1) Die ING unterrichtet den Kunden über die mittels Internetbanking getätigten Verfügungen in der für Kontoinformationen vereinbarten Art und Weise.

(2) Der Kunde hat die ihm im Internetbanking mitgeteilten Umsatzinformationen und Ausführungsdaten auf ihre Vollständigkeit und Richtigkeit zu überprüfen.

(3) Der Kunde ist verpflichtet, sich nach Erteilung von Zahlungsaufträgen oder Aufträgen sonstiger Art von der Ausführung des Auftrags durch die ING unverzüglich zu vergewissern. Nicht autorisierte oder fehlerhaft ausgeführte Aufträge hat der Kunde

der ING unverzüglich anzuzeigen. Dabei zu beachtende Fristen richten sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen.

9. Sorgfaltspflichten des Kunden

9.1 Schutz der Authentifizierungselemente

(1) Der Kunde hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 3 Absatz 3 dieser Vereinbarungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Internetbanking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummer 4 und 5 dieser Vereinbarungen).

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

(a) Wissensselemente, wie z.B. die PIN oder die mobilePIN, sind geheim zu halten; sie dürfen insbesondere

- › nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden,
- › nicht außerhalb des Internetbanking in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden,
- › nicht ungesichert elektronisch gespeichert (z.B. Speicherung der PIN im Klartext im Computer oder mobilen Endgerät) werden und
- › nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z.B. TAN-Generator, mobiles Endgerät) oder zur Prüfung des Seinelements (z.B. mobiles Endgerät mit Banking to go App und Fingerabdrucksensor) dient.

(b) Besitzelemente, z.B. der TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

- › sind der TAN-Generator oder das mobile Endgerät 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. Smartphone, Tablet) befindlichen Anwendungen für das Internetbanking (z.B. Banking to go App) nicht nutzen können,
- › ist die Anwendung für das Internetbanking (z.B. Banking to go App) auf dem mobilen Endgerät des Kunden zu deaktivieren, bevor der Kunde den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf oder Entsorgung des Mobiltelefons),
- › dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb des Internetbanking mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden und
- › hat der Kunde von der ING einen Code zur Aktivierung des Besitzelements erhalten, muss er diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Internetbanking des Kunden aktivieren.

(c) Seinelemente, wie z.B. der Fingerabdruck des Kunden, dürfen auf einem mobilen Endgerät des Kunden für das Internetbanking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinelemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Internetbanking genutzt wird, Seinelemente anderer Personen gespeichert, ist für das Internetbanking das von der Bank ausgegebene Wissensselement (z.B. mobilePIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinelement (z.B. Fingerabdruck).

(3) Beim mTAN-Verfahren darf das mobile Endgerät, mit dem die mTAN empfangen wird (z.B. Mobiltelefon), nicht gleichzeitig für das Internetbanking genutzt werden.

(4) Die für das mTAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Kunde diese Telefonnummer für das mTAN-Verfahren nicht mehr nutzt.

(5) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 4 darf der Kunde seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden (siehe Nummer 2 Absatz 1 Satz 3 und 4 dieser Vereinbarungen). Sonstige Drittdienste hat der Kunde mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

9.2 Sicherheitshinweise der ING

Der Kunde muss die Sicherheitshinweise zum Internetbanking auf der Internetseite der ING, insbesondere auch die Maßnahmen zum Schutz der von ihm eingesetzten Hard- und Software (Kundensystem), beachten.

9.3 Prüfung der Auftragsdaten mit von der ING angezeigten Daten

Die ING zeigt dem Kunden die von ihr von dem Kunden empfangenen Auftragsdaten (z.B. Betrag, IBAN des Zahlungsempfängers, Wertpapierkennnummer) an. Der Kunde ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

9.4 Allgemeine Sorgfaltspflichten des Kunden

Der Kunde hat die Verfahrensanleitungen, insbesondere die ihm während des Online-Kontakts angezeigte Benutzerführung, zu beachten und alle von ihm eingegeben oder die von einer Anwendung ermittelten und ausgelesenen Daten (z.B. Fotoüberweisung) auf Vollständigkeit und Richtigkeit zu überprüfen. Aufträge jeder Art müssen ihren Inhalt zweifelsfrei erkennen lassen. Nicht eindeutig formulierte Aufträge und insbesondere nicht oder nicht richtig ausgefüllte Felder können Rückfragen und Missverständnisse zur Folge haben, die zu Verzögerungen der Ausführung führen können. Die ING überprüft nicht die formale und inhaltliche Richtigkeit der erteilten Aufträge.

10. Anzeige und Unterrichtungspflichten

10.1 Sperranzeige

(1) Stellt der Kunde

- › den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z.B. mobiles Endgerät oder TAN-Generator) oder
 - › die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements
- fest, muss der Kunde die ING hierüber unverzüglich unterrichten (Sperranzeige). Der Kunde kann eine solche Sperranzeige jederzeit über die hierfür angebotenen Kommunikationskanäle abgeben.

(2) Der Kunde hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.

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

10.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

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

11. Nutzungssperre

11.1 Sperre auf Veranlassung des Kunden

Die ING sperrt auf Veranlassung des Kunden, insbesondere im Fall der Sperranzeige nach Nummer 10 Absatz 1 dieser Vereinbarungen,

- › den Internetbanking-Zugang für den Kunden oder
- › sein Authentifizierungselement zur Nutzung des Internetbanking.

11.2 Sperre auf Veranlassung der ING

(1) Die ING darf den Zugang zum Internetbanking für einen Kunden sperren, wenn

- › sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente dies rechtfertigen oder
- › der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselementes besteht oder
- › sie berechtigt ist, den Internetbanking-Vertrag aus wichtigem Grund zu kündigen.

(2) Die ING darf den Zugang zum Internetbanking für einen Kunden sperren, wenn der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der Authentifizierungselemente besteht, insbesondere dann, wenn

- › 3-mal hintereinander die PIN oder ein anderes Wissensselement falsch eingegeben wurde oder
- › 3-mal hintereinander eine falsche TAN eingegeben wurde.

(3) Die ING wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die ING hierdurch gegen gesetzliche Pflichten verstoßen würde.

11.3 Aufhebung der Sperre

Die ING wird eine Sperre aufheben oder soweit möglich die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

11.4 Zugangssperre für Zahlungsauslösdienste und Kontoinformationsdienste

Die ING kann Kontoinformationsdienstleistern oder Zahlungsauslösdienstleistern 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 Zahlungsauslösdienstleisters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die ING 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 ING hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die ING die Zugangssperre auf. Hierüber unterrichtet sie den Kunden unverzüglich.

12. E-Mail-Adresse

Zur Nutzung der digitalen Services der ING, einschließlich des Internetbanking, ist es erforderlich, dass der Kunde der ING eine E-Mail-Adresse zur Verfügung stellt. Der Kunde stellt sicher, dass die im Internetbanking hinterlegte E-Mail-Adresse immer auf dem aktuellen Stand ist. Änderungen sind vom Kunden unverzüglich im Internetbanking vorzunehmen.

13. Nutzung der Post-Box

(1) Inhalt

In der Post-Box werden dem Kunden persönliche Dokumente und Informationen zum Konto/Depot online zur Verfügung gestellt. Das heißt, der Kunde kann sich die Unterlagen online ansehen, herunterladen, ausdrucken und archivieren. Die Dokumentenauswahl kann von der ING jederzeit erweitert oder verringert werden. Die ING wird den Kunden hierüber informieren.

(2) Benachrichtigung

Die ING informiert den Kunden über die Einstellung von Dokumenten per E-Mail. Die Benachrichtigung erfolgt zeitnah, in der Regel am Tag der Einstellung. Eine Benachrichtigung bezieht sich auf sämtliche seit der letzten Benachrichtigung eingestellten Dokumente.

(3) Verzicht auf papierhafte Postzustellung

Die Post-Box wird mit dem Abschluss des Kontovertrags/Depotvertrags eingerichtet. Mit der Einrichtung der Post-Box verzichtet der Kunde auf den postalischen Versand der eingestellten Dokumente. Dies gilt auch für termin- und fristgebundene Nachrichten. Die ING ist weiter berechtigt, die hinterlegten Dokumente weiterhin postalisch oder auf andere Weise dem Kunden zuzusenden, wenn dies gesetzliche Vorgaben erforderlich machen oder es aufgrund anderer Umstände (z.B. des vorübergehenden Ausfalls der Post-Box) zweckmäßig ist.

(4) Mitwirkungspflichten des Kunden

Der Kunde verpflichtet sich, die Post-Box regelmäßig – mindestens einmal monatlich – auf neu hinterlegte Dokumente zu prüfen. Er kontrolliert die in der Post-Box hinterlegten Dokumente auf Richtigkeit und Vollständigkeit. Beanstandungen sind der ING unverzüglich, spätestens jedoch 6 Wochen nach Zugang und aus Beweisgründen in Textform mitzuteilen.

(5) Unveränderbarkeit der Daten/Haftung

Die ING garantiert die Unveränderbarkeit der Daten in der Post-Box, sofern die Daten innerhalb der Post-Box gespeichert oder aufbewahrt werden. Werden Dokumente außerhalb der Post-Box gespeichert, aufbewahrt oder in veränderter Form in Umlauf gebracht, übernimmt die ING hierfür keine Haftung.

(6) Historie

In der Post-Box und dem Archiv werden Dokumente in der Regel 3 Jahre zur Verfügung gestellt. Der Kunde wird im Internetbanking über den Zeitpunkt der automatischen Löschung in Kenntnis gesetzt. Nach Ablauf dieser Fristen erhält der Kunde keine gesonderte Nachricht.

14. Haftung

14.1 Haftung der ING bei Ausführung eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der ING bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

14.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

14.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge 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 hierdurch entstehenden Schaden nach den gesetzlichen Regelungen (§ 675v Absatz 1 BGB) bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Kunden ein Verschulden trifft. Die ING verzichtet auf eine Inanspruchnahme des Kunden nach diesen gesetzlichen Bestimmungen.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Kunde in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Vereinbarungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von Absatz 1 den hierdurch entstandenen Schaden in vollem Umfang, sofern nicht die Voraussetzungen des Absatzes 4 vorliegen. Grobe Fahrlässigkeit des Kunden kann insbesondere vorliegen, wenn er

› Nummer 9.1 Absatz 2

› Nummer 9.1 Absatz 4

› Nummer 9.3 oder

› Nummer 10.1 Absatz 1

dieser Vereinbarungen verletzt hat.

(3) Abweichend von Absatz 2 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die ING vom Kunden eine starke Kundenauthentifizierung nach § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Inhärenz (siehe Nummer 3 Absatz 3 dieser Vereinbarungen).

(4) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

(5) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 2 verpflichtet, wenn er die Sperranzeige nach Nummer 10 Abs. 1 dieser Vereinbarungen nicht abgeben konnte, weil die ING nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(6) Die Absätze 1 und 3 bis 5 finden keine Anwendung, wenn der Kunde in betrügerischer Absicht gehandelt hat.

(7) Die ING übernimmt zugunsten des Kunden den vollen Schaden aus nicht autorisierten Zahlungsvorgängen, der durch grob fahrlässiges Handeln entstanden ist, wenn der Kunde

› nicht autorisierte Zahlungsvorgänge unverzüglich angezeigt hat und

› wegen der missbräuchlichen Verwendung seiner Authentifizierungselemente Strafanzeige gestellt hat und dies der ING nachweist.

14.2.2 Haftung ab der Sperranzeige

Sobald die ING eine Sperranzeige eines Kunden erhalten hat, übernimmt sie alle danach durch nicht autorisierte Internetbanking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Kunde in betrügerischer Absicht gehandelt hat.

14.2.3 Haftungsausschluss

(1) Für Störungen des elektronischen Vertriebswegs, insbesondere für die nicht ordnungsgemäße Datenübermittlung sowie dafür, dass der Zugang zu einem Konto beziehungsweise Depot des Kunden über das Internetbanking vorübergehend nicht möglich ist, haftet die ING nur bei grobem Verschulden.

(2) 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.

Auszug aus den Bedingungen für die girocard [Debitkarte]

II. 1. Ausgabe der Karte

Die Karte kann als physische Karte oder als digitale Karte zur Speicherung auf einem mobilen Endgerät ausgegeben werden. Diese Vereinbarungen gelten für beide Kartenformen gleichermaßen, es sei denn, es ist ausdrücklich etwas anderes geregelt. Für die digitale Karte gelten ergänzend gesondert mit der ING vereinbarte Nutzungsbedingungen für die digitale Karte. ...

II. 7(3) Geheimhaltung der persönlichen Geheimzahl (PIN)

Der Karteninhaber hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der persönlichen Geheimzahl (PIN) erlangt. Die PIN darf insbesondere nicht auf der Karte vermerkt, bei einer digitalen Karte nicht im mobilen Endgerät oder in einem anderen Kommunikationsgerät gespeichert oder in anderer Weise zusammen mit dieser aufbewahrt werden. ...

(4) Unterrichtungs- und Anzeigepflichten

(4.1) Stellt der Karteninhaber den Verlust oder Diebstahl seiner Karte, des mobilen Endgeräts mit digitaler Karte, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von Karte oder PIN fest, so ist die ING unverzüglich telefonisch zu benachrichtigen (Sperranzeige). ...

II. 15. Haftung des Kontoinhabers für nicht autorisierte Kartenverfügungen

(1) Haftung des Kontoinhabers bis zur Sperranzeige. ...

(1.4) ... Grobe Fahrlässigkeit des Karteninhabers kann insbesondere dann vorliegen, wenn
er die persönliche Geheimzahl der digitalen Karte im mobilen Endgerät oder in einem anderen Endgerät gespeichert hat, ...

(1.6) Abweichend von den Absätzen (1.1) und (1.2) ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Bank vom Karteninhaber eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz (ZAG) nicht verlangt hat (z.B. bei Kleinbetragszahlungen gemäß Abschnitt I. Nummer 3. Absatz (3) dieser Bedingungen) oder der Zahlungsempfänger oder sein Zahlungsdienstleister diese nicht akzeptiert hat, obwohl die Bank zur starken Kundenauthentifizierung nach § 55 ZAG verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen (das ist die PIN), Besitz (das ist die Karte) oder Sein (etwas, das der Karteninhaber ist, zum Beispiel Fingerabdruck).

Auszug aus den Bedingungen für die VISA Card [Debitkarte] in Verbindung mit dem Girokonto

(bisher: „Bedingungen für die Kreditkarte [VISA Card] in Verbindung mit dem Girokonto“). Zahlungsverkehrsbezogene Anwendungen

1. Verwendungsmöglichkeiten

(1) Zu Zahlungsverkehrszwecken

Die von der ING ausgegebene VISA Card ist eine Debitkarte (im Folgenden „Karte“ genannt).

...

Die Karte kann als physische Karte oder als digitale Karte zur Speicherung auf einem Telekommunikations-, Digital- oder IT-Gerät (mobiles Endgerät) ausgegeben werden. Diese Sonderbedingungen gelten für beide Kartenformen gleichermaßen, es sei denn, es ist ausdrücklich etwas anderes geregelt. Für die digitale Karte gelten ergänzend die gesondert mit der Bank vereinbarten Nutzungsbedingungen für die digitale Karte. ...

I. 3. Autorisierung von Kartenzahlungen durch den Karteninhaber

(1) Bei Nutzung der Karte ist entweder
ein Beleg zu unterschreiben, auf den das Vertragsunternehmen die Kartendaten übertragen hat, oder
an Geldautomaten und automatisierten Kassen die PIN einzugeben.

Beim Karteneinsatz an automatisierten Kassen kann von der Eingabe der PIN abgesehen werden:

- › Zur Bezahlung von Verkehrsnutzungsentgelten oder Parkgebühren an unbeaufsichtigten automatisierten Kassen
- › Zur kontaktlosen Bezahlung von Kleinbeträgen. Hierbei ist die Karte mit Kontaktfunktion an ein Kartenlesegerät zu halten. Es gelten die von der Bank festgelegten Betrags- und Nutzungsgrenzen.

Bei Online-Bezahlvorgängen erfolgt die Authentifizierung des Karteninhabers, indem er auf Anforderung die gesondert vereinbarten Authentifizierungselemente einsetzt. Authentifizierungselemente sind

- › Wissensselemente (etwas, das der Karteninhaber weiß, zum Beispiel PIN),
- › Besitzelemente (etwas, das der Karteninhaber besitzt, zum Beispiel mobiles Endgerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN] als Besitznachweis) oder
- › Seinselemente (etwas, das der Karteninhaber ist, zum Beispiel Fingerabdruck)...

(2) Mit dem Einsatz der Karte erteilt der Karteninhaber die Zustimmung (Autorisierung) zur Ausführung des Zahlungsvorgangs. Soweit dafür zusätzlich die Unterschrift, eine PIN oder ein sonstiges Authentifizierungselement gefordert wird, wird die Zustimmung erst mit deren Einsatz erteilt.

5. Ablehnung von Kartenzahlungen durch die ING

Die ING ist berechtigt, die Kartenzahlung abzulehnen, wenn

- › sich der Karteninhaber nicht gemäß Ziffer 3 mit seiner PIN oder seinem sonstigen Authentifizierungselement legitimiert hat, ...

6. Verrechnung der Verfügungen – Unter- richtung – Ausführungsfrist

...

(2) Die Kartenumsätze werden werden am Tag des Eingangs bei der ING auf dem Girokonto gebucht. ...

8. Sorgfalts- und Mitwirkungspflichten des Karteninhabers

...

(3) Geheimhaltung der PIN

Der Karteninhaber hat Sorge dafür zu tragen, dass keine andere Person Kenntnis von der persönlichen Geheimzahl (PIN) erlangt. Insbesondere darf die PIN Dritten nicht mitgeteilt und auch nicht auf der Karte vermerkt, bei einer digitalen Karte nicht im mobilen Endgerät oder in einem anderen Kommunikationsgerät gespeichert oder in anderer Weise zusammen mit dieser aufbewahrt werden. (...) Sofern der Karteninhaber eine digitale Karte nutzt und der Zugriff auf das mobile Endgerät oder ein anderes Kommunikationsgerät durch ein vom Karteninhaber wählbares Legitimationsmedium abgesichert werden kann, so darf der Karteninhaber zur Absicherung des Zugriffs nicht dieselbe PIN verwenden, die für die Nutzung der Debitkarte erforderlich ist.

(4) Schutz der Authentifizierungselemente für Online-Bezahlvorgänge

Der Karteninhaber hat alle zumutbaren Vorkehrungen zu treffen, um seine mit der Bank vereinbarten Authentifizierungselemente für Online-Bezahlvorgänge (siehe Nummer 3 letzter Unterabsatz dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass die Authentifizierungselemente für Online-Bezahlvorgänge missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt werden.

Zum Schutz der einzelnen Authentifizierungselemente für Online-Bezahlvorgänge hat der Karteninhaber vor allem Folgendes zu beachten:

(a) Wissensselemente, wie z.B. das Online-Passwort, sind geheim zu halten; sie dürfen insbesondere

- › nicht mündlich (zum Beispiel telefonisch oder persönlich) mitgeteilt werden,
- › nicht außerhalb von Online-Bezahlvorgängen in Textform (z.B. per E-Mail oder Messenger-Dienst) weitergegeben werden,
- › nicht ungesichert elektronisch gespeichert (zum Beispiel Speicherung des Online-Passworts im Klartext im mobilen Endgerät) werden und
- › nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (zum Beispiel mobiles Endgerät) oder zur Prüfung des Seinselements (z.B. mobiles Endgerät mit Anwendung für Kreditkartenzahlung und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie zum Beispiel ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

- › ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Karteninhabers (zum Beispiel Mobiltelefon) nicht zugreifen können,
- › ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z.B. Mobiltelefon) befindliche Anwendung für Kreditkartenzahlungen (zum Beispiel Karten-App, Authentifizierungs-App) nicht nutzen können,
- › ist die Anwendung für Online-Bezahlvorgänge (zum Beispiel Karten-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 oder Entsorgung des Mobiltelefons) und
- › dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb der Online-Bezahlvorgänge mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden.

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

(5) Kontrollpflichten bei Online-Bezahlvorgängen

Sollten bei Online-Bezahlvorgängen an den Karteninhaber Angaben zum Zahlungsvorgang (zum Beispiel der Name des Vertragsunternehmens und der Verfügungsbetrag) mitgeteilt werden, sind diese Daten vom Karteninhaber auf Richtigkeit zu prüfen.

(6) Unterrichts- und Anzeigepflichten des Karteninhabers

(4.1) Stellt der Karteninhaber den Verlust oder Diebstahl seiner Karte, des mobilen Endgeräts mit digitaler Karte, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von Karte, PIN oder für Online-Bezahlvorgänge vereinbarter Authentifizierungselemente fest, so ist die ING unverzüglich zu unterrichten, um die Karte sperren zu lassen. ...

(4.2) Hat der Karteninhaber den Verdacht, dass eine andere Person unberechtigt in den Besitz seiner Karte gelangt ist, eine missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von Karte, PIN oder für Online-Bezahlvorgänge vereinbarter Authentifizierungselemente vorliegt, muss er ebenfalls unverzüglich eine Sperranzeige abgeben. ...

12. Haftung des Karteninhabers für nicht autorisierte Kartenverfügungen

(1) Haftung des Karteninhabers bis zur Sperranzeige

(1.1) Verliert der Karteninhaber seine Karte, PIN oder ein personalisiertes Sicherheitsmerkmal, werden sie ihm gestohlen, kommen sie ihm sonst abhanden oder werden die Karte oder die für Online-Bezahlvorgänge vereinbarte Authentifizierungselemente sonst missbräuchlich verwendet und kommt es dadurch zu nicht autorisierten Kartenverfügungen in Form der

› Bargeldauszahlung oder
› Verwendung der Karte zum Bezahlen bei einem Vertragsunternehmen, so haftet der Karteninhaber für dadurch bis zum Zeitpunkt der Sperranzeige entstandene Schäden nur, wenn er die nicht autorisierte Kartenverfügung in betrügerischer Absicht ermöglicht oder vorsätzlich oder grob fahrlässig seine Sorgfaltspflichten nach diesen Bedingungen verletzt hat.

(1.2) Der Karteninhaber haftet nicht nach Absatz 1, wenn

› es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung der Karte oder des mobilen

Endgeräts mit der digitalen Karte oder die für Online-Bezahlvorgänge vereinbarte Authentifizierungselemente vor dem nicht autorisierten Zahlungsvorgang zu bemerken. ...

(1.4) ... Grobe Fahrlässigkeit des Karteninhabers kann insbesondere dann vorliegen, wenn

...

› die PIN oder das vereinbarte Wissensselement für Online-Bezahlvorgänge (z.B. Online-Passwort) auf der Karte vermerkt oder zusammen mit der Karte verwahrt war,

› er die PIN der digitalen Karte im mobilen Endgerät oder in einem anderen Endgerät gespeichert hat,

› die PIN oder das vereinbarte Wissensselement für Online-Bezahlvorgänge (z.B. Online-Passwort) einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde. ...

(1.7) Abweichend von den Absätzen (1.1), (1.3) und (1.4) ist der Karteninhaber nicht zum Schadensersatz verpflichtet, wenn die Bank vom Karteninhaber eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz (ZAG) nicht verlangt hat oder der Zahlungsempfänger oder sein Zahlungsdienstleister diese nicht akzeptiert hat, obwohl die Bank zur starken Kundenauthentifizierung nach § 55 ZAG verpflichtet war. ...

(2) Haftung des Karteninhabers ab Sperranzeige

Sobald der Verlust oder Diebstahl der Karte, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von Karte, PIN oder für Online-Bezahlvorgänge vereinbarte Authentifizierungselemente gegenüber der ING angezeigt wurde, übernimmt die ING alle danach durch Verfügungen in Form der

› Bargeldauszahlung oder

› Verwendung der Karte zum Bezahlen bei einem Vertragsunternehmen entstehenden Schäden. Handelt der Karteninhaber in betrügerischer Absicht, trägt der Kontoinhaber auch die nach der Sperranzeige entstehenden Schäden.

Auszug Preis- und Leistungsverzeichnis Girokonto & Girokonto Student

1. Internetbanking

Nutzung des Internetbanking

kostenlos

Authentifizierung und Autorisierung

Für den Login und zur Erteilung von Aufträgen im Internetbanking verfügbare Verfahren:

Banking to go App

(unabhängig davon nutzbar, welches Gerät für den Zugriff auf das Internetbanking genutzt wird, z.B. Desktop PC, Laptop, Smartphone, Tablet)

kostenlos

mTAN

kostenlos

photoTAN-Generator

(nur nutzbar, wenn und solange ein Girokonto/Basiskonto geführt wird)

32,00 Euro (Kaufpreis)

iTAN

(zur Authentifizierung/Autorisierung nur dann nutzbar, wenn und solange kein Girokonto/Basiskonto geführt wird)

kostenlos

2. Wesentliche kostenlose Leistungen beim Girokonto und Girokonto Student

Kontoführung per Internetbanking mit Authentifizierung per Banking to go App

kostenlos

Monatlicher Kontoauszug per Post-Box, wenn Umsatz vorhanden

Vierteljährlicher Rechnungsabschluss per Post-Box

Sämtliche Buchungsposten

Beauftragen und Ändern von SEPA-Überweisungen, Daueraufträgen und Terminüberweisungen (online und mobil)

SEPA-Lastschriften in Euro

Einreichung inländischer Schecks in Euro

VISA Card [Debitkarte] und girocard [Debitkarte] einschließlich Partnerkarte

Kontoauszug

Bereitstellung des monatlichen Kontoauszugs in der Post-Box, wenn Umsatz vorhanden

ING-DiBa AG
Theodor-Heuss-Allee 2
60486 Frankfurt am Main

Telefon: 069/50502010
E-Mail: info@ing.de
Internet: www.ing.de

ING 
Die Bank und Du