

# VOLKSWAGEN BANK

GMBH

## Bedingungen für die konto-/depotbezogene Nutzung des online banking (online banking - Bedingungen) (Stand 31.10.2009)

### 1. Leistungsangebot

(1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels online banking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels online banking abrufen.

(2) Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet und erhalten jeweils eigene Identifikations- und Legitimationsmedien. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.

(3) Verfügungen mittels Überweisung sind auf EUR 350.000,00 pro Transaktion begrenzt. Überträge zu Lasten des Plus Konto Business sind auf EUR 350.00,00 pro Tag begrenzt. Bei Beträgen größer als EUR 350.000,00 zu Lasten des Plus Konto Business kann ausschließlich per Telefax (0531) 212 4060 verfügt werden. Andere Verfügungsllimite können jedoch vereinbart werden.

### 2. Voraussetzungen zur Nutzung des online banking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels online banking die mit der Bank vereinbarten und von dieser zur Verfügung gestellten personalisierten Sicherheitsmerkmale (z.B. Kundennummer und Einmalkennwort) und Authentifizierungsinstrumente (z.B. BANKEY), um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4).

Der Teilnehmer ist verpflichtet, bei der ersten Anmeldung sein Einmalkennwort sofort zu ändern und sich ein neues, persönliches Kennwort zu vergeben. Das Kennwort sollte in regelmäßigen Abständen geändert werden. Das alte Kennwort verliert bei Änderung seine Gültigkeit.

Im Rahmen der Bankeyzuordnung überträgt der Teilnehmer die Seriennummer an die Bank und ordnet somit den betreffenden Bankey dem Teilnehmer definitiv zu.

#### 2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- Kundennummer und persönliches Kennwort
- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN),
- der Nutzungscode für die elektronische Signatur.

#### 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,
- mittels eines TAN-Generators der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist,
- mittels eines mobilen Endgerätes (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
- auf einer Chipkarte mit Signaturfunktion oder
- auf einem sonstigen Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden.

Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

### 3. Zugang zum online banking

Der Teilnehmer erhält Zugang zum online banking, wenn

- dieser die Kontonummer oder seine individuelle Kundenkennung (Kundennummer und seine PIN oder sein persönliches Kennwort) oder elektronische Signatur 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 banking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen. In den von der Bank angegebenen Fällen hat der Teilnehmer jeweils eine Bankey-generierte TAN einzugeben.

### 4. Online banking - Aufträge

#### 4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss online banking - Aufträge (z. B. Überweisungen) in den von der Bank im Einzelnen angegebenen Fällen zu deren Wirksamkeit mit dem vereinbarten personalisierten Sicherheitsmerkmal (TAN oder elektronische Signatur) autorisieren und der Bank mittels online banking übermitteln. Die Bank bestätigt mittels online banking den Eingang des Auftrags.

#### 4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines online banking - Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des online banking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im online banking ausdrücklich vor.

# VOLKSWAGEN BANK

## GMBH

### 5. Bearbeitung von online banking - Aufträgen durch die Bank

(1) Die Bearbeitung der online banking - Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der online banking - Seite der Bank oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der online banking - Seite der Bank angegebenen oder im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

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

- Der Teilnehmer hat sich mit seinem personalisierten Sicherheitsmerkmal legitimiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das online banking - Datenformat ist eingehalten.
- Das gesondert vereinbarte online banking - Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die online banking - Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den online 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 banking eine Information zur Verfügung stellen.

### 6. Information des Kontoinhabers über online banking - Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels online banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

Umsatzinformationen werden auch zwischen den Rechnungsabschlüssen im business banking online zur Verfügung gestellt.

### 7. Sorgfaltspflichten des Teilnehmers

#### 7.1 Technische Verbindung zum online banking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum online banking nur über die von der Bank gesondert mitgeteilten online banking - Zugangskanäle (z. B. Internet-Adresse) herzustellen. Ein Zugriff auf das online banking über andere Zugänge als dem Teilnehmer durch die Bank mitgeteilten direkten Zugang geschieht auf das Risiko des Teilnehmers. Wenn der Teilnehmer die Internet-Adresse der Bank nicht direkt eingibt, also z.B. über Links auf die Seiten des online banking zugreift, besteht die Gefahr, dass die Identifizierungs- und Authentifizierungsdaten des Teilnehmers Dritten zugänglich werden.

#### 7.2 Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer hat

- seine personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der Bank gesondert mitgeteilten online banking - Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des personalisierten Sicherheitsmerkmals und/oder Authentifizierungsinstruments ist, kann das online banking - Verfahren im Rahmen des vereinbarten Leistungsangebotes missbräuchlich nutzen.

(2) Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

- Das personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert (z. B. im Kundensystem oder auf der Festplatte des PC) oder notiert werden.
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf online - Händlerseiten).
- Das personalisierte Sicherheitsmerkmal darf nicht außerhalb des online banking - Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die PIN 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 einer neuen TAN-Liste nicht mehr als eine TAN verwenden.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht gleichzeitig für das online banking genutzt werden.
- die Identifikations- und Legitimationsmedien sind nach Beendigung der online banking Nutzung aus dem Lesegerät zu entnehmen, soweit ein solches verwandt wird, und sicher zu verwahren.

#### 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. Der Teilnehmer hat dafür Sorge zu tragen, dass die von ihm verwendeten Systeme und Anwendungen (z.B. der PC und die dazugehörige Software) eine einwandfreie Abwicklung gewährleisten. Insbesondere ist dabei die regelmäßige Überprüfung mit aktuellen Verfahren/Werkzeugen auf Viren durchzuführen und der PC/die internetfähigen Endgeräte des Teilnehmers so zu schützen, dass kein unbefugter Zugang eines Dritten zu den Systemen des Teilnehmers möglich ist.

# VOLKSWAGEN BANK

## GMBH

### 7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem online banking - Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z. B. Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

## 8. Anzeige- und Unterrichtungspflichten

### 8.1 Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines Persönlichen Sicherheitsmerkmals

fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit über die folgenden Kontaktdaten mitteilen:

- Betrugsverdacht Hotline (0531)212 16 12
- [betrug@volkswagenbank.de](mailto:betrug@volkswagenbank.de)

Weiterhin kann der Teilnehmer im online - Dialog eine selbständige Sperre seines Persönlichen Sicherheitsmerkmals und seines Authentifizierungsinstruments vornehmen.

(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 online banking - Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument.

### 9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den online banking - Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den online banking - Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.
- sich der Teilnehmer dreimal mit einem falschen persönlichen Sicherheitsmerkmal anmeldet.

Bei Transaktionen, die die Eingabe eines von einem Authentifizierungsinstrument zur Verfügung gestellten Sicherheitsmerkmals (z.B. Bankey-generierten TAN) erfordern, sperrt die Bank das Authentifizierungsinstrument (z.B. den Bankey) und den online banking - Zugang, wenn dreimal hintereinander Transaktionen mit falschem Sicherheitsmerkmal übermittelt werden.

(2) Die Bank wird dem Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre eine Information über diese Sperre durch Anzeige im online - Dialog zur Verfügung stellen.

### 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.

### 9.4 Automatische Sperre eines chip-basierten Authentifizierungsinstruments

(1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur falsch eingegeben wird.

(2) Ein TAN-Generator, der die Eingabe eines eigenen Nutzungscode erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.

(3) Ein TAN-Generator sperrt sich selbst, wenn dreimal in Folge eine falsche TAN eingegeben wird.

# VOLKSWAGEN BANK

## GMBH

(4) Die in Absätzen 1, 2 und 3 genannten Authentifizierungsinstrumente können dann nicht mehr für das online banking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des online banking wiederherzustellen.

### 10. Haftung

#### 10.1 Haftung der Bank bei einer nicht autorisierten online banking - Verfügung und einer nicht oder fehlerhaft ausgeführten online banking - Verfügung

Die Haftung der Bank bei einer nicht autorisierten online banking - Verfügung und einer nicht oder fehlerhaft ausgeführten online banking - Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

#### 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 oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1 Absatz 1),
- das personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2 Absatz 2 1. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1 2. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2 3. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal außerhalb des online banking - Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2 4. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 5. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2 6. Spiegelstrich),
- 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 7. Spiegelstrich).

(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 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.