

Kontovollmacht

der Volkswagen Bank GmbH – nachfolgend Bank genannt.

Bitte angeben, sofern vorhanden

Ihre Plus Konto Business IBAN

Hinweis: Der Vollmachtnehmer erhält automatisch ein kostenpflichtiges PhotoTAN Lesegerät.

1. Persönliche Angaben des Kontoinhabers

Firma* _____

Straße* _____ Hausnummer* _____

PLZ* _____ Ort* _____

2. Angaben zum Bevollmächtigten

Bitte beachten Sie, dass bei gemeinschaftlicher Verfügungsberechtigung mindestens eine zweite Vollmacht erteilt bzw. bestehen muss.

 Frau Herr

Name, Vorname* _____

Geburtsdatum* _____ Art der Verfügungsberechtigung* Einzel GemeinschaftlichPrivatanschrift:*
Straße _____ Hausnummer* _____

PLZ* _____ Ort* _____

E-Mail (geschäftlich)* _____

Telefon (geschäftlich)* _____ Steuer-ID _____

Mit der Unterschrift werden gleichzeitig auch die beigefügten Bedingungen für die konto-/depotbezogene Nutzung des Online-Banking (Online-Banking-Bedingungen) und die allgemeinen Geschäftsbedingungen der Bank anerkannt.

Mit meiner/ unseren Unterschriften bestätige/n ich/wir den Erhalt der Anlage „Datenschutzinformationen“.

Datum*_____
Unterschrift des Vollmachtnehmers*

01.06.039.00 12/25

3. Umfang der Vollmacht für bevollmächtigte Personen

Der Kontoinhaber bevollmächtigt hiermit den unter Punkt 2. genannten Vollmachtnehmer, ihn im Geschäftsverkehr mit der Bank bei allen in unmittelbarem Zusammenhang mit der Kontoführung stehenden Geschäften entsprechend dem Feld „Art der Verfügungsberechtigung“ zu vertreten. Die Vollmacht gilt in Bezug auf sämtliche Anlageprodukte/Anlagekonten für Firmenkunden der Volkswagen Bank GmbH. Die Vollmacht kann jederzeit durch schriftliche Erklärung gegenüber der Bank widerrufen werden.

Diese Vollmacht berechtigt insbesondere dazu,

- Verfügungen über das jeweilige Guthaben vorzunehmen.
- Rechnungsabschlüsse, Kontoauszüge, Ertragnisaufstellungen und sonstige Abrechnungen, Mitteilungen sowie Kündigungen entgegenzunehmen und anzuerkennen.
- weitere Spar- und Einlagenprodukte (Kapitalkonto Business, Festgeld Business, Sparbrief Business) für den Vollmachtgeber zu eröffnen.

Die Erteilung von Untervollmachten ist nicht zulässig.

4. Kontobedingungen

Der Kontozugang, Verfügungen etc. erfolgen ausschließlich online zu den beigefügten „Bedingungen für die konto-/depotbezogene Nutzung des Online-Banking (Online-Banking-Bedingungen)“.

Personen, die Kontoinhaber bzw. Vertretungsberechtigte sind oder eine Kontovollmacht haben, nutzen das business banking online entsprechend den vereinbarten Vertretungsbefugnissen.

Der Kontoinhaber hat gemäß Ziffer 11. Absatz 1 der allgemeinen Geschäftsbedingungen der Bank das Erlöschen oder die Änderung einer der Bank bekannt gegebenen Vertretungsberechtigung unverzüglich mitzuteilen. Diese Mitteilungspflicht besteht auch dann, wenn die Vertretungsberechtigung in einem öffentlichen Register eingetragen ist und ihr Erlöschen oder ihre Änderung in dieses Register eingetragen wird.

5. Unterschrift/-en des/der Vertretungsberechtigten gemäß amtlichem Register_____
Name/-n in Druckbuchstaben*_____
Datum*_____
Firmenstempel, Unterschrift/-en*

Anlage Datenschutzinformationen der Volkswagen Bank GmbH für den Vollmachtnehmer (Seite 1/2)

Datenschutzinformationen der Volkswagen Bank GmbH

Im Rahmen dieser Geschäftsbeziehung verarbeitet der Verantwortliche personenbezogene Daten von Ihnen und speichert sie für die Dauer, die zur Erfüllung der festgelegten Zwecke und gesetzlicher Verpflichtungen erforderlich ist. Im Folgenden informieren wir Sie darüber, um welche Daten es sich dabei handelt, auf welche Weise sie verarbeitet werden und welche Rechte Ihnen diesbezüglich zustehen. Daten, die als Pflichtangaben gekennzeichnet sind, sind entweder gesetzlich oder vertraglich vorgeschrieben oder für den Vertragsschluss erforderlich. Die Nichtbereitstellung der abgefragten Daten kann für Sie rechtliche oder wirtschaftliche Nachteile haben. So kann es z. B. zu einer Ablehnung des Vertragsschlusses oder zu schlechteren Vertragskonditionen kommen.

Verantwortlicher

Volkswagen Bank GmbH
Gifhornstraße 57
38112 Braunschweig
betroffenenrechte@volkswagenbank.de

Allgemeines zur Datenverarbeitung

Der Verantwortliche verarbeitet Ihre Daten aus dieser Geschäftsbeziehung (z. B. aus dem Antrag und der Vertragsabwicklung) (im Folgenden: „Ihre Daten“). Hierbei werden Ihre Daten zum Zweck der Antragsprüfung, Vorgangsanlage, Vertragsabwicklung, Kundenberatung und Auswertung verarbeitet. Ihre Daten werden mit Auftragsverarbeitern und anderen Auftragnehmern (z. B. aus den Branchen: Logistik, Telekommunikation, Forderungsmanagement, Marketing, Druck, Markt- und Meinungsforschung) ausgetauscht. Zudem tauscht der Verantwortliche Ihre Daten mit den Gesellschaften der Volkswagen Finanzdienstleistungsgruppe (z. B. Unternehmen aus den Branchen: Bank, Leasing, Versicherung, Mobilität und Tank-/Servicekarten – im Folgenden: „VW Finanzdienstleistungsgruppe“) aus; für diese Verarbeitung besteht zum Teil eine gemeinsame Verantwortlichkeit (nähere Informationen hierzu sind abrufbar unter www.volkswagenbank.de/datenschutzinformationen). Ebenso erfolgt ein Austausch mit öffentlichen Stellen, öffentlich zugänglichen Quellen und ggf. mit Versicherern, Kreditinstituten, Zahlungsdienstleistern und Kooperationspartnern. Die Verarbeitung sowie der Austausch Ihrer Daten zu den oben genannten Zwecken findet insbesondere statt, soweit

- dies für die Erfüllung eines Vertrages, den Sie geschlossen haben, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist (Art. 6 Abs. 1 S. 1 lit. b Datenschutz-Grundverordnung, DSGVO); Die Datenverarbeitung ist insbesondere erforderlich, um die Vollständigkeit und Richtigkeit der Daten sowie deren Digitalisierung zu gewährleisten und um den Vertrag durchzuführen;
- dies zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist (Art. 6 Abs. 1 S. 1 lit. c DSGVO). Die Datenverarbeitung ist insbesondere erforderlich für die Gewährleistung der Vollständigkeit und Richtigkeit von Steuerdaten nach der Abgabenordnung, Gewerbeordnung und nach dem Handelsgesetzbuch. Darüber hinaus ist die Datenverarbeitung erforderlich für die Sicherung des Wirtschaftsverkehrs oder Kapitalmarktes (z. B. nach dem Kreditwesengesetz);
- dies zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist (Art. 6 Abs. 1 S. 1 lit. f DSGVO). Die Datenverarbeitung ist insbesondere erforderlich, um informierte Entscheidungen der Beteiligten auch in Ihrem Interesse zu gewährleisten und zu optimieren und um eine dauerhaft hohe Qualität und Einheitlichkeit der Kundenberatung durch den Verantwortlichen und die VW Finanzdienstleistungsgruppe zu gewährleisten. Darüber hinaus ist die Datenverarbeitung erforderlich zum Schutz von Vermögenswerten des Verantwortlichen, der VW Finanzdienstleistungsgruppe oder ihrer Kunden sowie zur Erfüllung konzerninterner Verwaltungs- und Abrechnungszwecke. Weiter ist die Datenverarbeitung erforderlich, um die Interessen und Präferenzen der Kunden zu analysieren und zu bewerten und daraus allgemeine Auswertungen für interne Zwecke zu erstellen (z. B. zum betriebswirtschaftlichen Monitoring und zur Optimierung der Produkte);
- dies von Ihrer freiwillig erteilten Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO) umfasst ist;
- dies von Ihrer freiwillig erteilten Einwilligung (Art. 9 Abs. 2 lit. a DSGVO) oder einer sonstigen Rechtsgrundlage (Art. 9 Abs. 2 lit. b bis j DSGVO) umfasst ist, wenn Ihre Daten auch besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO (z. B. Gesundheitsdaten) enthalten.

Drittlandübermittlung

Der Verantwortliche kann Ihre Daten auch an ein Land außerhalb des Europäischen Wirtschaftsraumes (EWR) übermitteln. Diese Übermittlung erfolgt hierbei unter Einhaltung der besonderen Voraussetzungen der Art. 44 – 49 DSGVO, wobei das angemessene Schutzniveau insbesondere entweder durch einen Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO, abgeschlossene EU-Standardvertragsklauseln gemäß Art. 46 Abs. 2 lit. c und d DSGVO oder verbindliche interne Datenschutzvorschriften gemäß Art. 47 DSGVO gewährleistet wird. Die EU-Standardvertragsklauseln können Sie auf der Website der Europäischen Kommission abrufen und einsehen oder direkt beim Verantwortlichen erfragen und in Kopie erhalten.

Allgemeine Speicherfristen

Sollten Sie sich zu Produkten/Dienstleistungen des Verantwortlichen informiert, aber keinen Vertrag angebahnt haben, werden Ihre Daten längstens für 6 Monate nach dem letzten Kontakt zwischen Ihnen und dem Verantwortlichen gespeichert.

Im Übrigen beginnt die Speicherfrist am Ende des Kalenderjahres des letzten Ereignisses im Rahmen dieser Geschäftsbeziehung:

- Wenn es zu einer Vertragsanbahnung, aber zu keinem Vertragsschluss gekommen ist, werden Ihre Daten längstens für 3 Jahre gespeichert.
- Wenn es zu einem Vertragsschluss gekommen ist, werden Ihre Daten, insbesondere steuerrechtlich relevante Daten, bis zum Ablauf der gesetzlichen Aufbewahrungsfristen, längstens für 10 Jahre nach Beendigung des Vertrages, gespeichert. Die allgemeine Speicherdauer von Ihren Daten kann ausnahmsweise bis zu 30 Jahre betragen, soweit dies zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Auf abweichende Speicherfristen bei einzelnen Datenverarbeitungen weisen wir Sie innerhalb dieser Datenschutzinformationen am Ende des jeweiligen Abschnitts hin. Die Speicherfristen können sich ausnahmsweise verlängern, wenn die weitere Speicherung rechtlich zulässig (z. B. zum Schutz von Vermögenswerten oder zur Wahrung und ggf. Durchsetzung unserer Rechte) oder erforderlich ist (z. B. Aufbewahrungsfrist für Werbeinwilligungen oder im Rahmen von Betriebsprüfungen).

Betrugsprophylaxe

Der Verantwortliche verarbeitet Ihre Daten zur Betrugsprophylaxe und tauscht Ihre Daten mit Auskunfteien, den Gesellschaften der VW Finanzdienstleistungsgruppe und ggf. Datenbankanbietern aus, soweit

- dies zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist (Art. 6 Abs. 1 S. 1 lit. c DSGVO). Die Datenverarbeitung ist insbesondere erforderlich zur Verhinderung von Geldwäsche, Terrorismusfinanzierung oder sonstiger strafbarer Handlungen, die zu einer Gefährdung des Vermögens des Verantwortlichen oder seiner Kunden führen können (z. B. nach dem Kreditwesengesetz, Geldwäschegesetz);
- dies zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist (Art. 6 Abs. 1 S. 1 lit. f DSGVO). Die Datenverarbeitung ist insbesondere erforderlich, um das Vermögen des Verantwortlichen, der VW Finanzdienstleistungsgruppe oder ihrer Kunden zu schützen und zukünftige strafbare Handlungen zu verhindern.

Es gelten neben den „Allgemeinen Speicherfristen“ folgende Speicherfristen:

Ihre Daten, die

- aufgrund eines bestätigten Betrugs oder Betrugsversuches gekennzeichnet worden sind, werden dauerhaft im Rahmen der oben genannten Rechtsgrundlagen gespeichert;
- aufgrund eines nicht bestätigten Betrugsverdachts gekennzeichnet worden sind, werden längstens für 3 Jahre gespeichert.

Automatisierte Entscheidungen

Der Verantwortliche verarbeitet Ihre Daten für automatisierte Entscheidungen im Einzelfall. Diese Entscheidungsform kann insbesondere zu Zwecken der Antrags-, Bonitätsprüfung und Betrugsprophylaxe angewendet werden. Die Entscheidungen betreffen dabei gesetzliche (z. B. Geschäftsfähigkeit) und geschäftspolitische Vorgaben (z. B. negative Eigenerfahrungen) sowie anerkannte mathematisch-statistische Verfahren (z. B. Bonitätsscoring). Fällt die Entscheidung nachteilig für Sie aus, haben Sie das Recht, die getroffene Entscheidung durch Einschaltung einer Person überprüfen zu lassen. Die Verarbeitung Ihrer Daten zu den oben genannten Zwecken findet insbesondere statt, soweit

- dies für die Erfüllung eines Vertrages, den Sie geschlossen haben, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist (Art. 6 Abs. 1 S. 1 lit. b DSGVO). Die Datenverarbeitung ist insbesondere erforderlich für die schnellstmögliche und digitale Bewertung und Bearbeitung Ihres Antrages, zur Optimierung der angebotenen Produkte und Prozesse und zum Schutz von Vermögenswerten des Verantwortlichen, der VW Finanzdienstleistungsgruppe und ihrer Kunden;
- dies von Ihrer freiwillig erteilten Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO) umfasst ist.

Kundenprofile

Der Verantwortliche bildet auf Grundlage Ihrer Daten und weiterer werberelevanter Daten (z. B. Nutzungsdaten, Daten zu Ihren Präferenzen) Ihr individuelles Kundenprofil und ordnet dieses bestimmten Kundensegmenten zu. Diese Ergebnisse nutzt der Verantwortliche für die zielgruppenspezifische Steuerung von Art, Inhalt und Häufigkeit von Werbemaßnahmen. Dies kann insbesondere dazu führen, dass Sie im Unterschied zu anderen Kunden bestimmte Werbung erhalten oder nicht erhalten. Dies geschieht, soweit

- dies zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist (Art. 6 Abs. 1 S. 1 lit. f DSGVO). Die Datenverarbeitung ist insbesondere erforderlich, um anhand einfacher Auswertungen von Nutzungsdaten und offensichtlicher Präferenzen Angebote besser auf Sie zuschneiden zu können und unerwünschte oder unpassende Angebote zu vermeiden (eingeschränkte Auswertungen);
- dies von Ihrer freiwillig erteilten Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO) umfasst ist (umfangreiche Auswertungen).

Anlage Datenschutzinformationen der Volkswagen Bank GmbH für den Vollmachtnehmer (Seite 2/2)

Individuelle Werbemaßnahmen

Der Verantwortliche verarbeitet Ihre Daten für Direktwerbung, sowohl für eigene Angebote als auch für Angebote der VW Finanzdienstleistungsgruppe, Ihres Handelspartners und des Herstellers, des Importeurs oder der Vertriebsgesellschaft Ihres Fahrzeuges oder von sonstigen berechtigten Dritten (z. B. Unternehmen aus den Branchen: Bank, Leasing, Versicherung und Mobilität), und tauscht dazu mit den vorgenannten Empfängern Ihre Daten aus. Daneben nutzt der Verantwortliche Online-Marketingdienste, um bestimmten Zielgruppen bei ihrer Nutzung von Online-Diensten interessengerechte Werbeeinhalte anzuzeigen. Dazu übermittelt der Verantwortliche Ihre Daten (z. B. E-Mailadresse) in verschlüsselter Form (Hash-Wert) an die Online-Marketingdienste. Diese gleichen den Hash-Wert der übermittelten Daten mit den Hashwerten ihrer eigenen Nutzerdaten zur Identifikation ab. Dies geschieht jeweils, soweit

- dies zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist (Art. 6 Abs. 1 S. 1 lit. f DSGVO). Die Datenverarbeitung ist insbesondere erforderlich, um Ihnen auf Sie zugeschnittene Angebote zeitnah und zuverlässig zukommen lassen zu können und Ihnen auf Sie zugeschnittene Online-Werbung anzuzeigen;
- dies von Ihrer freiwillig erteilten Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO) umfasst ist.

Ein Austausch mit sonstigen Empfängern erfolgt nur, soweit dies von Ihrer freiwillig erteilten Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO) umfasst ist.

Testdatenmanagement

Der Verantwortliche sowie die VW Finanzdienstleistungsgruppe verarbeiten Ihre Daten im Rahmen der Erhaltung und Einführung von IT-Systemen und Dienstleistungen, soweit dies zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten und der betroffenen Personen erforderlich ist (Art. 6 Abs. 1 S. 1 lit. f DSGVO). Die Datenverarbeitung ist insbesondere erforderlich, um die Sicherheit, Funktionsfähigkeit und Zuverlässigkeit neuer und bestehender IT-Systeme und Dienstleistungen zu gewährleisten und vor Störungen und widerrechtlichen Eingriffen zu schützen, die die Verfügbarkeit, Authentizität, Vollständigkeit oder Vertraulichkeit von Daten beeinträchtigen können. Die Verarbeitung dieser Daten ist auch erforderlich, um eine dauerhaft hohe Qualität und Einheitlichkeit der angebotenen Produkte/Dienstleistungen zu gewährleisten und sie stetig zu optimieren.

Es gilt neben den „Allgemeinen Speicherfristen“ folgende Speicherfrist: Für die Tests wird eine Kopie der hierfür erforderlichen Daten erstellt. Diese Kopie wird längstens für 1 Jahr gespeichert.

Betroffenenrechte

Sie haben das Recht:

- gemäß Art. 15 DSGVO Auskunft über Ihre von dem Verantwortlichen verarbeiteten personenbezogenen Daten zu verlangen;
- gemäß Art. 16 DSGVO unverzüglich die Berichtigung unrichtiger oder Vervollständigung Ihrer beim Verantwortlichen gespeicherten personenbezogenen Daten zu verlangen;
- gemäß Art. 17 DSGVO die Löschung Ihrer beim Verantwortlichen gespeicherten personenbezogenen Daten zu verlangen, sofern die gesetzlichen Voraussetzungen vorliegen;
- gemäß Art. 18 DSGVO die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, sofern die gesetzlichen Voraussetzungen vorliegen;
- gemäß Art. 20 DSGVO Ihre personenbezogenen Daten, die Sie dem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen;
- gemäß Art. 7 Abs. 3 DSGVO Ihre einmal erteilte Einwilligung jederzeit gegenüber dem Verantwortlichen zu widerrufen;
- gemäß Art. 77 DSGVO sich bei einer Aufsichtsbehörde zu beschweren. In der Regel können Sie sich hierfür an die Aufsichtsbehörde Ihres üblichen Aufenthaltsortes oder unseres Unternehmenssitzes wenden.

Möchten Sie von Ihren Betroffenenrechten Gebrauch machen, dann genügt eine E-Mail an: betroffenenrechte@volkswagenbank.de

Darüberhinausgehender Kontakt zum Datenschutzbeauftragten (neben der unter „Verantwortlicher“ genannten Anschrift): dsb@volkswagenbank.de

Widerspruchsrecht

Sie haben das Recht, Widerspruch gegen die Verarbeitung Ihrer personenbezogenen Daten einzulegen, soweit dafür Gründe vorliegen, die sich aus Ihrer besonderen Situation ergeben (Art. 21 Abs. 1 DSGVO). Weiter haben Sie das Recht, ohne Begründung Widerspruch gegen Direktwerbung und ein damit in Verbindung stehendes Werbef profiling einzulegen (Art. 21 Abs. 2 DSGVO).

Möchten Sie von Ihrem Widerspruchsrecht Gebrauch machen, genügt eine E-Mail an betroffenenrechte@volkswagenbank.de

VOLKSWAGEN BANK

GMBH

Bedingungen für die konto-/depotbezogene Nutzung des online banking (online banking - Bedingungen) Stand 14.09.2019

1. Leistungsangebot

(1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels Online Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online Banking abrufen. Des Weiteren sind sie gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absätze 33 und 34 Zahlungsdiensteaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.

(2) Kunde und Bevollmächtigte werden einheitlich als „Teilnehmer“, Konto und Depot einheitlich als „Konto“ bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

(3) Verfügungen mittels Überweisungen und Buchungen sind auf EUR 350.000,00 pro Transaktion begrenzt. Abweichende Verfügungsmitel können jedoch gemäß den Produktsonderbedingungen oder individuell vereinbart werden.

2. Voraussetzungen zur Nutzung des Online Banking

(1) Der Teilnehmer kann das Online Banking nutzen, wenn die Bank ihn authentifiziert hat.

(2) Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechnete Verwendung eines vereinbarten Zahlungsinstrumentes, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).

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.

(3) Authentifizierungselemente sind

- Wissensselemente, also etwas, das nur der Teilnehmer weiß (z.B. persönliche Identifikationsnummer [PIN]),
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z.B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN], die den Besitz des Teilnehmers nachweisen, wie die girocard mit TAN-Generator oder das mobile Endgerät), oder
- Seinsselemente, also etwas, das der Teilnehmer ist (Inhärenz, z.B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

(4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissensselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinsselements an die Bank übermittelt.

3. Zugang zum Online Banking

(1) Der Teilnehmer erhält Zugang zum Online Banking der Bank, wenn

- er seine individuelle Teilnehmerkennung (z.B. Kontonummer, Anmeldenname) angibt und
 - er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
 - keine Sperre des Zugangs (siehe Nummern 8.1 und 9 dieser Bedingungen) vorliegt.
- Nach Gewährung des Zugangs zum Online Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge erteilt werden.

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

4. Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss einem Auftrag (zum Beispiel Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (zum Beispiel Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden.

Die Bank bestätigt mittels Online Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Online Banking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Online Banking ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

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

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

- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1 dieser Bedingungen).

VOLKSWAGEN BANK

GMBH

- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (zum Beispiel Wertpapierorder) liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten (vgl. Nummer 1 Absatz 3 dieser Bedingungen).
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.
- Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird dem Teilnehmer hierüber mittels Online Banking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6. Information des Kunden über Online-Banking-Verfügungen

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

7. Sorgfaltspflichten des Teilnehmers

7.1 Schutz der Authentifizierungselemente

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

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

- a) Wissensselemente, wie z.B. die PIN, sind geheim zu halten; sie dürfen insbesondere
 - nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden,
 - nicht außerhalb des Online Banking in Textform (z.B. per E-Mail, Messenger-Dienst) weiter gegeben werden,
 - nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
 - nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z.B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinelements (z.B. mobiles Endgerät mit Anwendung für das Online Banking und Fingerabdrucksensor) dient.
- b) Besitzelemente, wie z.B. die girocard mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
 - sind die girocard mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
 - ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z.B. Mobiltelefon) nicht zugreifen können,
 - ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z.B. Mobiltelefon) befindliche Anwendung für das Online Banking (z.B. Online-Banking-App, Authentifizierungs-App) nicht nutzen können,
 - ist die Anwendung für das Online Banking (z.B. Online-Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf oder Entsorgung des Mobiltelefons),
 - dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb des Online Banking mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weiter gegeben werden und
 - muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z.B. Mobiltelefon mit Anwendung für das Online Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online Banking des Teilnehmers aktivieren.
- c) Seinelemente, wie z.B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinelemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online Banking genutzt wird, Seinelemente anderer Personen gespeichert, ist für das Online Banking das von der Bank ausgegebene Wissensselement (z.B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinelement.

(3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (zum Beispiel Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.

(4) Die für das mobile-TAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Online Banking nicht mehr nutzt.

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

7.2 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise auf der Online-Banking-Seite der Bank, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (zum Beispiel mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z.B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte)

VOLKSWAGEN BANK

GMBH

oder

• die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements 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: 0531212 16 12
- betrug@volkswagenbank.de

Weiterhin kann der Teilnehmer im online-Dialog eine selbstständige Sperre vornehmen.

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

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

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

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

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

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

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

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 der Authentifizierungselemente des Teilnehmers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

(2) Die Bank 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 Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

9.3 Aufhebung der Sperre

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

9.4 Automatische Sperre eines chip-basierten Besitzelements

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

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

(3) Die in Absätzen 1 und 2 genannten Besitzelemente 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.

9.5 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Kunden verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Bank wird den Kunden über eine solche Zugangsverweigerung auf dem vereinbarten Weg unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Bank die Zugangssperre auf. Hierüber unterrichtet sie den Kunden unverzüglich.

10. Haftung

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

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

10.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

10.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn

VOLKSWAGEN BANK

GMBH

- Es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- Der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach

- Nummer 7.1 Absatz 2,
 - Nummer 7.1 Absatz 4,
 - Nummer 7.3 oder
 - Nummer 8.1 Absatz 1
- dieser Bedingungen verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung im Sinne des § 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 Sein (siehe Nummer 2 Absatz 3 dieser Bedingungen).

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

(6) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 dieser Bedingungen nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(8) Ist der Kunde kein Verbraucher, gilt ergänzend Folgendes:

- Der Kunde haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

10.2.2 Haftung des Kunden bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten (z.B. Wertpapiertransaktionen) vor der Sperranzeige

Beruhend nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten (z.B. Wertpapiertransaktionen) vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung ab der Sperranzeige

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

10.2.4 Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.