

# PSD PrivatKredit PSD AutoKredit PSD WohnKredit

PSD Bank Nürnberg eG  
90328 Nürnberg

PSD Personennummer \_\_\_\_\_  
PSD Personennummer \_\_\_\_\_  
PSD Personennummer \_\_\_\_\_



MH: \_\_\_\_\_ B: \_\_\_\_\_ I: \_\_\_\_\_ A: \_\_\_\_\_ IQ: \_\_\_\_\_ VK: \_\_\_\_\_  
Vertriebsdokumentation (**wird von der Bank ausgefüllt**)

**1. Kreditnehmer**  Frau  Herr

\_\_\_\_\_  
Vorname, Name

\_\_\_\_\_  
Straße, Hausnummer

\_\_\_\_\_  
PLZ, Ort

\_\_\_\_\_  
Geburtsdatum

\_\_\_\_\_  
Geburtsort

\_\_\_\_\_  
Staatsangehörigkeit

\_\_\_\_\_  
Geburtsname

**2. Kreditnehmer**  Frau  Herr

\_\_\_\_\_  
Vorname, Name

\_\_\_\_\_  
Straße, Hausnummer

\_\_\_\_\_  
PLZ, Ort

\_\_\_\_\_  
Geburtsdatum

\_\_\_\_\_  
Geburtsort

\_\_\_\_\_  
Staatsangehörigkeit

\_\_\_\_\_  
Geburtsname

**Weitere Angaben zum 1. Kreditnehmer**

\_\_\_\_\_  
Steuer-Identifikationsnummer

Angestellte/r  Schüler/in  
 Beamter/Beamtin  Student/in  
 Arbeiter/in  Auszubildende/r  
 Rentner  Hausfrau/Hausmann  
 Pensionär  \_\_\_\_\_  
 Öffentlicher Dienst

\_\_\_\_\_  
Beruf

\_\_\_\_\_  
beschäftigt seit

\_\_\_\_\_  
Name und Anschrift des Arbeitgebers

\_\_\_\_\_  
E-Mail

\_\_\_\_\_  
Telefon privat

\_\_\_\_\_  
Telefon geschäftlich

\_\_\_\_\_  
Mobil

**Weitere Angaben zum 2. Kreditnehmer**

\_\_\_\_\_  
Steuer-Identifikationsnummer

Angestellte/r  Schüler/in  
 Beamter/Beamtin  Student/in  
 Arbeiter/in  Auszubildende/r  
 Rentner  Hausfrau/Hausmann  
 Pensionär  \_\_\_\_\_  
 Öffentlicher Dienst

\_\_\_\_\_  
Beruf

\_\_\_\_\_  
beschäftigt seit

\_\_\_\_\_  
Name und Anschrift des Arbeitgebers

\_\_\_\_\_  
E-Mail

\_\_\_\_\_  
Telefon privat

\_\_\_\_\_  
Telefon geschäftlich

\_\_\_\_\_  
Mobil

**Familienstand**

ledig  verheiratet  verwitwet  
 geschieden  getrennt lebend  eingetragene Lebenspartnerschaft

**Güterstand**

Zugewinnngemeinschaft (gesetzlich)  
 Gütertrennung  Gütergemeinschaft

**Familienstand**

ledig  verheiratet  verwitwet  
 geschieden  getrennt lebend  eingetragene Lebenspartnerschaft

**Güterstand**

Zugewinnngemeinschaft (gesetzlich)  
 Gütertrennung  Gütergemeinschaft

**Wohnstatus**

Eigentum  Miete  bei Eltern

**Wohnstatus**

Eigentum  Miete  bei Eltern

Anzahl Personen im Haushalt \_\_\_\_\_ Anzahl der unterhaltsberechtigten Kinder \_\_\_\_\_ Alter der Kinder \_\_\_\_\_

Anzahl Personen im Haushalt \_\_\_\_\_ Anzahl der unterhaltsberechtigten Kinder \_\_\_\_\_ Alter der Kinder \_\_\_\_\_

**Erster und zweiter Kontoinhaber sind miteinander verheiratet:**  ja  nein

Die Kundenzeitschrift ‚Geld & Gewinn‘ und der PSD Newsletter erhalten Sie bei vorliegender E-Mailadresse elektronisch zugestellt.

**Geldwäschegesetz**  
Angaben zum wirtschaftlich Berechtigten gemäß Geldwäschegesetz: Ich versichere/wir versichern, dass ich/wir im eigenen wirtschaftlichen Interesse und nicht auf fremde Veranlassung (insbesondere nicht als Treuhänder) handle/handeln.



**PSD PrivatKredit** (Mindestbetrag 2.500 Euro, Maximalbetrag 30.000 Euro)

Ich/Wir beantrage(n) einen PSD PrivatKredit über \_\_\_\_\_ EUR  
mit einer monatlichen Teilzahlung von \_\_\_\_\_ EUR  
oder einer Laufzeit von \_\_\_\_\_ Monaten (max. 84 Monate)  
Verwendungszweck \_\_\_\_\_

**PSD AutoKredit** (Mindestbetrag 5.000 Euro, Maximalbetrag 30.000 Euro)

Ich/Wir beantrage(n) einen PSD AutoKredit über \_\_\_\_\_ EUR  
mit einer monatlichen Teilzahlung von \_\_\_\_\_ EUR  
oder einer Laufzeit von \_\_\_\_\_ Monaten (max. 84 Monate)  
Verwendungszweck zum Autokauf, ein Nachweis z.B. Kaufvertrag ist erforderlich.

**PSD WohnKredit** (Mindestbetrag 5.000 Euro, Maximalbetrag 50.000 Euro)

Ich/Wir beantrage(n) einen PSD Wohnkredit über \_\_\_\_\_ EUR  
mit einer monatlichen Teilzahlung von \_\_\_\_\_ EUR  
oder einer Laufzeit von \_\_\_\_\_ Monaten (max. 120 Monate)  
Verwendungszweck \_\_\_\_\_  
für meine/unsere Immobilie (mind. 50%-iger Miteigentumsanteil).  
Als Nachweis ist ein Grundbuchauszug (max. 6 Monate alt) erforderlich.

**Vereinbarung für PSD OnlineBanking mit Nutzung des elektronischen Postfachs**

Zwischen dem Kunden und der PSD Bank Nürnberg wird vereinbart, dass der Nutzer mittels PSD OnlineBanking Zugang zu allen gegenwärtigen und zukünftigen Konten und Depots in dem von der Bank angebotenen Umfang hat, bei denen der Inhaber dieser Kontoverbindung Kontoinhaber, Mitkontoinhaber oder Bevollmächtigter ist. Dokumente und Mitteilungen, wie z.B. Kontoauszüge, werden dem Kontoinhaber ausschließlich im elektronischen Postfach vom PSD OnlineBanking zur Verfügung gestellt.

**Der Zugang wird für das SecureGo TAN-Verfahren freigeschaltet.**

**Laden Sie sich hierzu bitte als erstes die SecureGo-App herunter und führen Sie die Registrierung durch.**

1. Nutzer \_\_\_\_\_  
Vorname, Name Personennummer

Auf Wunsch können Sie auch das Smart-TAN-Verfahren nutzen:

Sm@rt-TAN mittels TAN-Generator und girocard (Debitkarte)

2. Nutzer \_\_\_\_\_  
Vorname, Name Personennummer

Auf Wunsch können Sie auch das Smart-TAN-Verfahren nutzen:

Sm@rt-TAN mittels TAN-Generator und girocard (Debitkarte)

Sollte der Nutzer ein Bevollmächtigter sein, muss eine Vollmacht zu Lebzeiten und über den Tod hinaus vorliegen oder auf besonderem Formular erteilt werden. Besteht bereits ein Zugang, so wird dieser um die Verfügungsberechtigung erweitert.

Das Verfügungslimit beträgt 12.500,00 Euro pro Tag. Eine Änderung des Verfügungslimits ist nur in Textform oder im PSD OnlineBanking mit Eingabe einer TAN durch den Kontoinhaber, bei Gemeinschaftskonten mit Einzelverfügungsbefugnis durch einen Kontoinhaber möglich.

**Referenzkonto**

Für künftig erteilte Aufträge wird ein Referenzkonto hinterlegt. Die verbindliche Referenzbankverbindung des Kontoinhabers für den unbaren Zahlungsverkehr ist die im nachfolgenden SEPA-Lastschriftmandat angegebene Bankverbindung. Bis auf Widerruf bevollmächtige ich die PSD Bank, die Beträge für künftig erteilte Aufträge vom Referenzkonto einzuziehen bzw. dem Referenzkonto gutzuschreiben. Überweisungen von Spar-/Tagesgeld-Konten sind nur auf das angegebene Referenzkonto möglich. Die Frist für die Vorabinformation (Prenotification) beträgt 1 Tag vor Kontobelastung.

Falls das Referenzkonto keine Deckung aufweist, besteht keine Einlöschungspflicht. Die ggf. durch Rückbelastung entstehenden Fremdkosten und die Bearbeitungsgebühr der PSD Bank Nürnberg eG sind vom Kunden zu tragen.

Eine Änderung der Referenzbankverbindung ist ausschließlich schriftlich mit dem Antrag ‚PSD Änderung Bankverbindung‘ durch den/die Girokontoinhaber möglich.

\_\_\_\_\_  
Name des Kontoinhabers

\_\_\_\_\_  
IBAN (Voraussetzung: das Referenzkonto ist für den Zahlungsverkehr geeignet)

\_\_\_\_\_  
BIC (außerhalb des Europäischen Wirtschaftsraums)

## 1. Kontoinhaber: Selbstauskunft Auslandssteuer (nur wenn zutreffend, bitte ankreuzen)

Ich bin Staatsangehöriger der USA.

Ich bin in den USA steuerlich ansässig.<sup>1</sup>

\_\_\_\_\_  
US-Steuer-Identifikationsnummer (TIN / SSN)

Ich bin steuerlich im Ausland ansässig<sup>1</sup> in

\_\_\_\_\_  
Land (außer Deutschland und USA)

\_\_\_\_\_  
Steuer-Identifikationsnummer aus diesem Land

Diese Selbstauskunft ersetzt alle vorausgegangenen Selbstauskünfte des Kontoinhabers/Treugebers.

Über wesentliche Änderungen informiert der Kontoinhaber/Treugeber das Kreditinstitut binnen 30 Tagen.

<sup>1</sup> Die steuerliche Ansässigkeit ergibt sich aus dem nationalen Steuerrecht. In Zweifelsfällen wird empfohlen, die Angaben zur/zu steuerlichen Ansässigkeit(en) mit Ihrem Steuerberater abzustimmen.

## 2. Kontoinhaber: Selbstauskunft Auslandssteuer (nur wenn zutreffend, bitte ankreuzen)

Ich bin Staatsangehöriger der USA.

Ich bin in den USA steuerlich ansässig.<sup>1</sup>

\_\_\_\_\_  
US-Steuer-Identifikationsnummer (TIN / SSN)

Ich bin steuerlich im Ausland ansässig<sup>1</sup> in

\_\_\_\_\_  
Land (außer Deutschland und USA)

\_\_\_\_\_  
Steuer-Identifikationsnummer aus diesem Land

Diese Selbstauskunft ersetzt alle vorausgegangenen Selbstauskünfte des Kontoinhabers/Treugebers.

Über wesentliche Änderungen informiert der Kontoinhaber/Treugeber das Kreditinstitut binnen 30 Tagen.

<sup>1</sup> Die steuerliche Ansässigkeit ergibt sich aus dem nationalen Steuerrecht. In Zweifelsfällen wird empfohlen, die Angaben zur/zu steuerlichen Ansässigkeit(en) mit Ihrem Steuerberater abzustimmen.

## Sperrnachricht

Die Sperrnachricht nach Nr. 7.1 „Sonderbedingungen für PSD OnlineBanking“ kann der Nutzer unter der Telefonnummer

**116 116** mitteilen.

## Wichtiger Hinweis:

Besteht das PSD OnlineBanking seit mindestens 21 Monaten, wird aber in den letzten 18 Monaten nicht benutzt, dann erfolgt aus Sicherheitsgründen eine Sperrung.

## Bedingungen

Für den gesamten Geschäftsverkehr gelten ergänzend die Allgemeinen Geschäftsbedingungen der Bank und deren Sonderbedingungen für den Überweisungsverkehr, für Echtzeit-Überweisungen, den Lastschriftverkehr, den Scheckverkehr, die girocard (Debitkarte), das PSD OnlineBanking, PSD ServiceDirekt (TelefonBanking), die Nutzung des elektronischen Postfachs, den Sparverkehr, das PSD TagesGeld, den PSD SparBrief, das PSD WachstumsSparen, den PSD SparPlan Fix, für Wertpapiergeschäfte, die Allgemeinen Kredit- und Darlehensbedingungen und die Bedingungen für das Gemeinschaftskonto mit Einzelverfügungsbefugnis (Oder-Konto). Der Wortlaut dieser Bedingungen kann in den Geschäftsräumen der Bank oder unter [www.psd-nuernberg.de](http://www.psd-nuernberg.de) eingesehen werden; auf Verlangen werden diese Bedingungen auch ausgehändigt oder zugesandt.

## SEPA-Lastschriftmandat (Bitte zwingend vollständig ausfüllen und unterschreiben!)

DE02PSD0000002067

Gläubiger-Identifikationsnummer (CI Creditor Identifier)

wird nachgereicht

Mandatsreferenz (wird von der Bank ausgefüllt)

Ich/Wir ermächtige(n) die PSD Bank Nürnberg eG, Zahlungen von meinem/unserem Konto mittels Lastschrift einzuziehen. Zugleich weise(n) ich/wir mein/unser Kreditinstitut an, die von der PSD Bank Nürnberg eG auf mein/unser Konto gezogenen Lastschriften einzulösen.

Hinweis: Ich kann/Wir können innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrags verlangen. Es gelten dabei die mit meinem/unserem Kreditinstitut vereinbarten Bedingungen. Die Frist für die Vorabinformation (Pre-Notification) beträgt 1 Tag vor Kontobelastung.



Kontoinhaber (Vorname, Name)



Anschrift (Straße, Hausnummer, PLZ, Ort; bitte angeben, wenn Kontoinhaber nicht gleichzeitig Zahlungsempfänger/Darlehensnehmer ist)



Kreditinstitut



BIC (außerhalb des Europäischen Wirtschaftsraums)



IBAN



Ort, Datum (Angabe immer erforderlich)



Unterschrift der/ des Girokontoinhaber/s/gesetzlichen Vertreters für das SEPA-Lastschriftmandat (immer erforderlich)

## Girokonto für monatliche Teilzahlungen

\_\_\_\_\_  
IBAN

\_\_\_\_\_  
BIC (außerhalb des Europäischen Wirtschaftsraums)

\_\_\_\_\_  
Bankinstitut

\_\_\_\_\_  
Kontoinhaber

\_\_\_\_\_  
Unterschrift des Kontoinhabers, sofern nicht Auftraggeber

Der Einzug soll jeweils zum 1.  oder 15.  oder zum  jeden Monats erfolgen.

## Girokonto für Darlehensauszahlung

\_\_\_\_\_  
IBAN

\_\_\_\_\_  
BIC (außerhalb des Europäischen Wirtschaftsraums)

\_\_\_\_\_  
Kontoinhaber

## Restschuldversicherung

Vermittler \_\_\_\_\_

Zur Absicherung des Kredits beantrage/n ich/wir gleichzeitig eine Restschuldversicherung für den

1. Kreditnehmer **und/oder:**  für den Todesfall  zusätzlich auch für Arbeitsunfähigkeit  zusätzlich auch für Arbeitslosigkeit  
 2. Kreditnehmer:  für den Todesfall  zusätzlich auch für Arbeitsunfähigkeit  zusätzlich auch für Arbeitslosigkeit  
 Ich/Wir wünsche(n) keine Darlehensabsicherung und trage(n) die Risiken selbst.

## Selbstauskunft

Angaben

1. Kreditnehmer

2. Kreditnehmer

### monatliche Einkünfte

Nettolohn/-gehalt/-rente  EUR  EUR  
sonstige monatliche Einkünfte  EUR  EUR  
(Nachweise der letzten 2 Monate bitte beifügen)

### monatliche Ausgaben

Miete / Wohnkosten (kalt/warm)  /  EUR  /  EUR  
Versicherungsbeiträge (Kranken-/private Versicherungen)  EUR  EUR  
Unterhaltsverpflichtungen  EUR  EUR  
sonstige Ausgaben (Bausparen etc.)  EUR  EUR

### Vermögen

Sparguthaben/ Wertpapierdepot/ Immobilie .  EUR  EUR  
etc.

### Bürgschaften

Meine Bezüge sind abgetreten/verpfändet  Ja  Nein  Ja  Nein

### 1.Kreditnehmer<sup>1</sup>

Verbindlichkeiten aus Baufinanzierungen (PSD Bank und fremde Banken)

Gläubiger	Restschuld	monatl. Aufwand	wird umgeschuldet
<input type="text"/>	<input type="text"/> EUR	<input type="text"/> EUR	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> EUR	<input type="text"/> EUR	<input type="checkbox"/>

Verbindlichkeiten (Restvaluta) aus anderen Krediten und Leasing (PSD Bank und fremde Banken)

Gläubiger	Restschuld	monatl. Aufwand	wird umgeschuldet
<input type="text"/>	<input type="text"/> EUR	<input type="text"/> EUR	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> EUR	<input type="text"/> EUR	<input type="checkbox"/>

### 2.Kreditnehmer<sup>1</sup>

Verbindlichkeiten aus Baufinanzierungen (PSD Bank und fremde Banken)

Gläubiger	Restschuld	monatl. Aufwand	wird umgeschuldet
<input type="text"/>	<input type="text"/> EUR	<input type="text"/> EUR	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> EUR	<input type="text"/> EUR	<input type="checkbox"/>

Verbindlichkeiten (Restvaluta) aus anderen Krediten und Leasing (PSD Bank und fremde Banken)

Gläubiger	Restschuld	monatl. Aufwand	wird umgeschuldet
<input type="text"/>	<input type="text"/> EUR	<input type="text"/> EUR	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> EUR	<input type="text"/> EUR	<input type="checkbox"/>

<sup>1</sup> gemeinsame Kredite sind beim 1. Kreditnehmer aufzuführen.

## Steuer-Identifikationsnummer

Liegt die Steuer-Identifikationsnummer bei Vertragsabschluss nicht vor, beauftrage ich die Bank mit der Abfrage der Steuer-ID beim Bundeszentralamt für Steuern (BZSt).

### Einwilligungserklärung zu Anrufen und elektronischer Post

Von Ihrer PSD Bank können Sie selbstverständlich erwarten, dass wir mit Ihnen aktiv in Kontakt bleiben. Dabei arbeiten wir im Interesse einer umfassenden Beratung auch mit Verbund- und Kooperationspartnern – im Folgenden Kooperationspartner genannt – zusammen. Zur Kontaktaufnahme mit Ihnen benötigen wir Ihre Einwilligung. Die Erklärungen sind freiwillig und ohne Einfluss auf das Vertragsverhältnis mit der Bank. Kooperationspartner der PSD Bank sind zurzeit:

- Bausparkasse Schwäbisch Hall AG, Crailsheimer Str. 52, 74523 Schwäbisch Hall
- DZ Bank AG Deutsche Zentral-Genossenschaftsbank, Platz der Republik, 60265 Frankfurt/Main
- R+V Allgemeine Versicherung AG, Raiffeisenplatz 1, 65189 Wiesbaden
- R+V Lebensversicherung AG, Raiffeisenplatz 1, 65189 Wiesbaden
- Union Asset Management Holding AG, Weißfrauenstraße 7, 60311 Frankfurt/Main
- Union Investment Service Bank AG, Weißfrauenstraße 7, 60311 Frankfurt/Main

### Einwilligungserklärung zu Anrufen und elektronischer Post der PSD Bank zu eigenen Produkten und Produkten von Kooperationspartnern

Ich/wir willige(n) ein, durch die PSD Bank oder ein von ihr beauftragtes Unternehmen zu Finanz- und Versicherungsprodukten (z. B. Einlage-, Anlage-, Kredit-, Versicherungs- und Bausparprodukte) der PSD Bank oder ihrer Kooperationspartner angerufen und per elektronischer Post kontaktiert zu werden.

 Ja Nein

### Einwilligungserklärung zu Anrufen und elektronischer Post von Kooperationspartnern der PSD Bank zu deren Produkten

Ich/wir willige(n) ein, durch Kooperationspartner der PSD Bank oder ein von einem Kooperationspartner beauftragtes Unternehmen zu Angeboten des jeweiligen Kooperationspartners angerufen und per elektronischer Post kontaktiert zu werden.

 Ja Nein

Diese Einwilligungserklärungen sind **freiwillig** und können jederzeit – ohne Einfluss auf das Vertragsverhältnis – widerrufen werden.

### Einwilligungserklärung für die Datenübermittlung zwischen der Bank und Ihren Kooperationspartnern

Ihre PSD Bank arbeitet im Interesse einer umfassenden Beratung mit Verbund- und Kooperationspartnern – im Folgenden Kooperationspartner genannt – zusammen. Kooperationspartner der PSD Bank sind zurzeit:

- Bausparkasse Schwäbisch Hall AG, Crailsheimer Str. 52, 74523 Schwäbisch Hall
- DZ Bank AG Deutsche Zentral-Genossenschaftsbank, Platz der Republik, 60265 Frankfurt/Main
- R+V Allgemeine Versicherung AG, Raiffeisenplatz 1, 65189 Wiesbaden
- R+V Lebensversicherung AG, Raiffeisenplatz 1, 65189 Wiesbaden
- Union Asset Management Holding AG, Weißfrauenstraße 7, 60311 Frankfurt/Main
- Union Investment Service Bank AG, Weißfrauenstraße 7, 60311 Frankfurt/Main

Damit mich/uns auch die Kooperationspartner und deren Außendienstmitarbeiter in allen Fragen zu Finanzdienstleistungen (z. B. Einlage-, Anlage-, Kredit-, Versicherungs- und Bausparprodukte) der PSD Bank oder ihrer Kooperationspartner umfassend beraten können, bin ich/sind wir damit einverstanden, dass die PSD Bank ihren Kooperationspartnern bzw. deren Außendienstmitarbeitern die für die Aufnahme und Durchführung der Beratung erforderlichen Angaben zur dortigen Datenverarbeitung und Nutzung übermittelt.

Übermittelt werden dürfen (einzelne Datenkategorien können gestrichen werden):

- Personalien (Name, Anschrift, Geburtsdatum, Familienstand, Beruf oder vergleichbare Daten)
- Kontokorrent (Saldo/Limit oder vergleichbare Daten)
- Karten (Produkt/Anzahl oder vergleichbare Daten)
- Einlagen (Produktart, Guthaben, Verzinsung, Laufzeit oder vergleichbare Daten)
- Kredite (Produktart, Salden, Verzinsung, Laufzeit oder vergleichbare Daten)
- Depotwerte (Kurswert oder vergleichbare Daten)

Die folgende Einwilligung ist **freiwillig** und kann jederzeit – ohne Einfluss auf das Vertragsverhältnis – für die Zukunft widerrufen werden.

In diesem Rahmen entbinde ich/entbinden wir die PSD Bank zugleich vom Bankgeheimnis.

 Ich bin/ Wir sind einverstanden. Ich bin/ Wir sind nicht einverstanden.

Der Verwendung der Daten für Werbezwecke kann jederzeit widersprochen werden.

### Datenübermittlung an die SCHUFA und Befreiung vom Bankgeheimnis

Die Bank übermittelt im Rahmen dieses Vertragsverhältnisses erhobene personenbezogene Daten über die Beantragung, die Durchführung und Beendigung dieser Geschäftsbeziehung sowie Daten über nicht vertragsgemäßes Verhalten oder betrügerisches Verhalten an die SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden. Rechtsgrundlagen dieser Übermittlungen sind Artikel 6 Absatz 1 Buchstabe b und Artikel 6 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung (DSGVO).

Übermittlungen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO dürfen nur erfolgen, soweit dies zur Wahrung berechtigter Interessen der Bank oder Dritter erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Der Datenaustausch mit der SCHUFA dient auch der Erfüllung gesetzlicher Pflichten zur Durchführung von Kreditwürdigkeitsprüfungen von Kunden (§ 505a des Bürgerlichen Gesetzbuches, § 18a des Kreditwesengesetzes).

Der Kunde befreit die Bank insoweit auch vom Bankgeheimnis.

Die SCHUFA verarbeitet die erhaltenen Daten und verwendet sie auch zum Zwecke der Profilbildung (Scoring), um ihren Vertragspartnern im Europäischen Wirtschaftsraum und in der Schweiz sowie ggf. weiteren Drittländern (sofern zu diesen ein Angemessenheitsbeschluss der Europäischen Kommission besteht) Informationen unter anderem zur Beurteilung der Kreditwürdigkeit von natürlichen Personen zu geben. Nähere Informationen zur Tätigkeit der SCHUFA können dem SCHUFA-Informationsblatt entnommen oder online unter [www.schufa.de/datenschutz](http://www.schufa.de/datenschutz) eingesehen werden.

## Information zur außergerichtlichen Streitschlichtung

Die Bank nimmt am Streitbelegungsverfahren der deutschen genossenschaftlichen Bankengruppe teil. Für die Beilegung von Streitigkeiten mit der Bank besteht daher für Privatkunden, Firmenkunden sowie bei Ablehnung eines Antrags auf Abschluss eines Basiskontovertrags für Nichtkunden die Möglichkeit, den Ombudsmann für die genossenschaftliche Bankengruppe anzurufen (<http://www.bvr.de/Service/Kundenbeschwerdestelle>). Näheres regelt die "Verfahrensordnung für die außergerichtliche Schlichtung von Kundenbeschwerden im Bereich der deutschen genossenschaftlichen Bankengruppe", die auf Wunsch zur Verfügung gestellt wird. Die Beschwerde ist in Textform (z. B. mittels Brief, Telefax oder E-Mail) an die Kundenbeschwerdestelle beim Bundesverband der Deutschen Volksbanken und Raiffeisenbanken – BVR, Schellingstraße 4, 10785 Berlin, Fax: 030 2021-1908, E-Mail: [kundenbeschwerdestelle@bvr.de](mailto:kundenbeschwerdestelle@bvr.de) zu richten.

Betrifft der Beschwerdegegenstand eine Streitigkeit aus dem Anwendungsbereich des Zahlungsdiensterechts (§§ 675c bis 676c des Bürgerlichen Gesetzbuchs, Art. 248 des Einführungsgesetzes zum Bürgerlichen Gesetzbuch, § 48 des Zahlungskontengesetzes und Vorschriften des Zahlungsdiensterechtsaufsichtsgesetzes), besteht zudem die Möglichkeit, eine Beschwerde bei der Bundesanstalt für Finanzdienstleistungsaufsicht einzulegen. Die Verfahrensordnung ist bei der Bundesanstalt für Finanzdienstleistungsaufsicht erhältlich. Die Adresse lautet: Bundesanstalt für Finanzdienstleistungsaufsicht, Graurheindorfer Straße 108, 53117 Bonn. Zudem besteht in diesen Fällen auch die Möglichkeit, eine Beschwerde unmittelbar bei der Bank einzulegen. Die Bank wird Beschwerden in Textform (z. B. mittels Brief, Telefax oder E-Mail) beantworten.

Die Europäische Kommission stellt unter <https://ec.europa.eu/consumers/odr/> eine Plattform zur außergerichtlichen Online-Streitbeilegung (sogenannte OS-Plattform) bereit.

Zudem besteht die Möglichkeit, eine zivilrechtliche Klage einzureichen.

## Richtigkeit der Angaben

Mir/uns ist bekannt, dass die Angaben in diesem Antrag Grundlagen für eine Darlehensgewährung sind. **Ich bestätige/Wir bestätigen die Richtigkeit und Vollständigkeit der gemachten Angaben.**

Ferner versichere ich/versichern wir, dass zum jetzigen Zeitpunkt und in den letzten zehn Jahren keine **Mahnverfahren, Zahlungsklagen, Zwangsvollstreckungen, Verfahren zur Abgabe der eidesstattlichen Versicherung, Wechsel – oder Scheckproteste und Insolvenzverfahren** bestehen bzw. bestanden haben.

Ich versichere/ Wir versichern, dass die **bestehenden Kredite ungekündigt sind und keine Rückstände bestehen.**

Die Bank ist berechtigt, die Angaben zu überprüfen und entsprechende Nachweise anzufordern. Unrichtige und unvollständige Angaben können insbesondere zum Rücktritt vom Darlehensvertrag oder zur Kündigung des Darlehens seitens der Bank führen.

<input type="text"/>	<input type="text"/>	<input type="text"/>
Ort, Datum	Unterschrift 1. Kreditnehmer	Unterschrift 2. Kreditnehmer

## Legitimationsprüfung für den 1. Kontoinhaber

Die Unterschrift(en) unter diesen Vertrag  wurde(n) vor mir von dem/den Unterzeichner(n) geleistet.  wurde(n) von mir geprüft.  PostIdent  
Er/Sie hat/haben sich ausgewiesen durch  Personalausweis  Reisepass  Geburtsurkunde (genügt bei Minderjährigen)  Sofort-Legitimation

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Nr.	ausstellende Behörde	Ausstellungsdatum	gültig bis
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Staatsangehörigkeit	Geburtsdatum	Geburtsort	
<input type="text"/>	<input type="text"/>		
Ort, Datum	Mitarbeiter der PSD Bank/Stempel und Unterschrift der bescheinigenden Stelle		

## Legitimationsprüfung für den 2. Kontoinhaber

Die Unterschrift(en) unter diesen Vertrag  wurde(n) vor mir von dem/den Unterzeichner(n) geleistet.  wurde(n) von mir geprüft.  PostIdent  
Er/Sie hat/haben sich ausgewiesen durch  Personalausweis  Reisepass  Geburtsurkunde (genügt bei Minderjährigen)  Sofort-Legitimation

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Nr.	ausstellende Behörde	Ausstellungsdatum	gültig bis
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Staatsangehörigkeit	Geburtsdatum	Geburtsort	
<input type="text"/>	<input type="text"/>		
Ort, Datum	Mitarbeiter der PSD Bank/Stempel und Unterschrift der bescheinigenden Stelle		

## Einzelverfügungsrecht der Kontoinhaber (Oder-Konto)

### 1 Jeder Kontoinhaber ist allein berechtigt:

- über das jeweilige Guthaben sowie über etwa den Kontoinhabern gemeinsam eingeräumte Kredite zu verfügen und darüber hinaus vorübergehende geduldete Überziehungen im banküblichen Rahmen herbeizuführen;
- weitere Gemeinschaftskonten und Gemeinschaftsdepots mit Einzelverfügungsberechtigung für die Kontoinhaber zu den getroffenen Vereinbarungen zu eröffnen; die Bank wird die anderen Kontoinhaber hierüber unterrichten;
- Konto-/Depotauszüge, Rechnungsabschlüsse sowie Wertpapieraufstellungen, sonstige Abrechnungen und Anzeigen für die Kontoinhaber entgegenzunehmen, zu prüfen und anzuerkennen sowie den gesamten das Gemeinschaftskonto betreffenden Schriftwechsel für die Kontoinhaber verbindlich zu unterzeichnen;
- im Fall des Ablebens eines der Kontoinhaber über das jeweilige Guthaben auch ohne Mitwirkung der Erben zu verfügen; eine Auflösung oder Umschreibung wird die Bank nur zulassen, wenn alle überlebenden ursprünglichen Kontoinhaber dies verlangen (vgl. Nummer 5).

### 1.1 Kreditverträge und Kontoüberziehungen

Für den Abschluss und die Änderung von Kreditverträgen und eingeräumten Kontoüberziehungen zulasten der Konten ist die Mitwirkung aller Kontoinhaber erforderlich.

### 1.2 Termingeschäfte

Zum Abschluss und zur Durchführung von Termingeschäften zulasten der Gemeinschaftskonten bedarf es einer Vereinbarung mit allen Kontoinhabern.

### 1.3 Erteilung und Widerruf von Vollmachten

Eine Kontovollmacht kann nur von allen Kontoinhabern gemeinschaftlich erteilt werden. Der Widerruf durch einen der Kontoinhaber führt zum Erlöschen der Vollmacht. Über den Widerruf ist die Bank unverzüglich und aus Beweisgründen möglichst in Textform zu unterrichten. Vollmachten, die ein Kontoinhaber vor der Eröffnung des Gemeinschaftskontos erteilt hat, gelten nur dann, wenn der andere Kontoinhaber dem zustimmt.

### 1.4 Kontoauflösung

Eine Auflösung von Gemeinschaftskonten kann nur durch alle Kontoinhaber gemeinschaftlich erfolgen. Eine Ausnahme hiervon besteht im Todesfall eines Kontoinhabers (vgl. Nummer 5).

## 2 Gesamtschuldnerische Haftung

Für die Verbindlichkeiten aus Gemeinschaftskonten haften die Kontoinhaber als Gesamtschuldner. Die Bank kann von daher von jedem einzelnen Kontoinhaber die Erfüllung sämtlicher Ansprüche fordern.

## 3 Widerruf der Einzelverfügungsberechtigung

Jeder Kontoinhaber kann die Einzelverfügungsberechtigung eines anderen Kontoinhabers mit Wirkung für die Zukunft der Bank gegenüber – aus Beweisgründen möglichst in Textform – widerrufen. In diesem Fall können alle Kontoinhaber nur noch gemeinschaftlich über Gemeinschaftskonten verfügen. Die Bank wird die anderen Kontoinhaber hierüber unterrichten.

## 4 Kontomitteilungen

Kontomitteilungen werden in der vereinbarten Form übermittelt. Wenn eine unmittelbare Benachrichtigung geboten ist (z.B. bei Nichtausführung von Zahlungsverkehrsaufträgen), wird die Bank die Mitteilung an die im Vertrag angegebene Postanschrift versenden. Konto- und Kreditkündigungen sowie die Ankündigung solcher Maßnahmen werden jedem Kontoinhaber zugeschickt. Jeder Kontoinhaber kann verlangen, dass auch ihm künftig alle Kontomitteilungen zusätzlich übermittelt werden.

## 5 Tod eines Kontoinhabers

Nach dem Tod eines Kontoinhabers bleiben die Befugnisse der anderen Kontoinhaber unverändert bestehen. Jedoch können die überlebenden Kontoinhaber ohne Mitwirkung der Erben Gemeinschaftskonten auflösen oder auf ihren Namen umschreiben lassen. Die Rechte des Verstorbenen werden durch dessen Erben gemeinschaftlich wahrgenommen. Das Recht zum Widerruf der Einzelverfügungsberechtigung steht jedoch jedem einzelnen Miterben zu. Widerruft ein Miterbe, bedarf jede Verfügung über Gemeinschaftskonten seiner Mitwirkung. Widerrufen mehrere Miterben die Einzelverfügungsberechtigung eines Kontoinhabers, so können sämtliche Kontoinhaber nur noch gemeinschaftlich mit den widerrufenden Miterben über die Gemeinschaftskonten verfügen.





# Informationsbogen für den Einleger



PSD Personennummer

Kundenname:

Sehr geehrte Kundin,  
sehr geehrter Kunde,

gemäß § 23a Abs. 1 Satz 3 KWG sind wir verpflichtet, Sie mit Hilfe dieses Informationsbogens über die gesetzliche Einlagensicherung zu informieren. Zusätzlich sind Ihre Einlagen wie bisher durch die freiwillige Sicherungseinrichtung des BVR geschützt.

Gesetzliches Einlagensicherungssystem der PSD Banken	BVR Institutssicherung GmbH <sup>1</sup>
Sicherungsobergrenze	100 000 EUR pro Einleger pro Kreditinstitut <sup>2</sup>
Mehrere Einlagen bei demselben Kreditinstitut	Alle Ihre Einlagen bei demselben Kreditinstitut werden „aufaddiert“; die Gesamtsumme unterliegt der Obergrenze von 100 000 EUR <sup>2</sup>
Gemeinschaftskonto mit einer anderen Person oder mehreren anderen Personen	Die Obergrenze von 100 000 EUR gilt für jeden einzelnen Einleger <sup>3</sup>
Erstattungsfrist bei Ausfall eines Kreditinstituts	7 Arbeitstage <sup>4</sup>
Währung der Erstattung	EUR
Kontaktdaten	BVR Institutssicherung GmbH Schellingstraße 4 10785 Berlin Tel.: 030 2021 – 0 E-Mail: info@bvr-institutssicherung.de
Weitere Informationen	<a href="https://www.bvr-institutssicherung.de">https://www.bvr-institutssicherung.de</a> <sup>5</sup>

## Erläuterungen

<sup>1</sup> Ihre Einlage wird von einem gesetzlichen Einlagensicherungssystem gedeckt. Außerdem ist Ihr Kreditinstitut Teil eines institutsbezogenen Sicherungssystems, in dem sich alle Mitglieder gegenseitig unterstützen, um eine Insolvenz zu vermeiden. Im Fall einer Insolvenz werden alle Einlagen bis zu 100 000 EUR vom Einlagensicherungssystem erstattet.

<sup>2</sup> Sollte eine Einlage nicht verfügbar sein, weil ein Kreditinstitut seinen finanziellen Verpflichtungen nicht nachkommen kann, so werden die Einleger von dem Einlagensicherungssystem entschädigt. Die betreffende Deckungssumme beträgt maximal 100 000 EUR pro Kreditinstitut. Das heißt, dass bei der Ermittlung dieser Summe alle bei demselben Kreditinstitut gehaltenen Einlagen addiert werden. Hält ein Einleger beispielsweise 90 000 EUR auf einem Sparkonto und 20 000 EUR auf einem Girokonto, so werden ihm lediglich 100 000 EUR erstattet.

<sup>3</sup> Bei Gemeinschaftskonten gilt die Obergrenze von 100 000 EUR für jeden Einleger. Einlagen auf einem Konto, über das zwei oder mehrere Personen als Mitglieder einer Personengesellschaft oder Sozietät, einer Vereinigung oder eines ähnlichen Zusammenschlusses ohne Rechtspersönlichkeit verfügen können, werden bei der Berechnung der Obergrenze von 100 000 EUR allerdings zusammengefasst und als Einlage eines einzigen Einlegers behandelt. In den Fällen des § 8 Abs 2 bis 4 EinSiG sind Einlagen über 100 000 EUR hinaus gesichert. Weitere Informationen sind erhältlich über <https://www.bvr-institutssicherung.de>.

<sup>4</sup> Haben Sie die Erstattung innerhalb der genannten Frist nicht erhalten, sollten Sie mit dem Einlagensicherungssystem Kontakt aufnehmen, da der Gültigkeitszeitraum für Erstattungsforderungen nach einer bestimmten Frist abgelaufen sein kann. Weitere Informationen sind erhältlich über <https://www.bvr-institutssicherung.de>.

<sup>5</sup> Einlagen von Privatkunden und Unternehmen sind im Allgemeinen durch Einlagensicherungssysteme gedeckt. Für bestimmte Einlagen geltende Ausnahmen werden auf der Website des zuständigen Einlagensicherungssystems mitgeteilt. Ihr Kreditinstitut wird Sie auf Anfrage auch darüber informieren, ob bestimmte Produkte gedeckt sind oder nicht. Wenn Einlagen entschädigungsfähig sind, wird das Kreditinstitut dies auch auf dem Kontoauszug bestätigen.

Ort, Datum

Unterschrift(en) Kontoinhaber/gesetzl. Vertreter



# SCHUFA-Information

## 1. Name und Kontaktdaten der verantwortlichen Stelle sowie des betrieblichen Datenschutzbeauftragten

SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden, Tel.: +49 (0) 6 11-92 78 0

Der betriebliche Datenschutzbeauftragte der SCHUFA ist unter der o.g. Anschrift, zu Hd. Abteilung Datenschutz oder per E-Mail unter [datenschutz@schufa.de](mailto:datenschutz@schufa.de) erreichbar.

## 2. Datenverarbeitung durch die SCHUFA

### 2.1 Zwecke der Datenverarbeitung und berechtigte Interessen, die von der SCHUFA oder einem Dritten verfolgt werden

Die SCHUFA verarbeitet personenbezogene Daten, um berechtigten Empfängern Informationen zur Beurteilung der Kreditwürdigkeit von natürlichen und juristischen Personen zu geben. Hierzu werden auch Scorewerte errechnet und übermittelt. Sie stellt die Informationen nur dann zur Verfügung, wenn ein berechtigtes Interesse hieran im Einzelfall glaubhaft dargelegt wurde und eine Verarbeitung nach Abwägung aller Interessen zulässig ist. Das berechtigte Interesse ist insbesondere vor Eingehung von Geschäften mit finanziellem Ausfallrisiko gegeben. Die Kreditwürdigkeitsprüfung dient der Bewahrung der Empfänger vor Verlusten im Kreditgeschäft und eröffnet gleichzeitig die Möglichkeit, Kreditnehmer durch Beratung vor einer übermäßigen Verschuldung zu bewahren. Die Verarbeitung der Daten erfolgt darüber hinaus zur Betrugsprävention, Seriositätsprüfung, Geldwäscheprävention, Identitäts- und Altersprüfung, Ansnrften-ermittlung, Kundenbetreuung oder Risikosteuerung sowie der Tarifierung oder Konditionierung. Neben den vorgenannten Zwecken verarbeitet die SCHUFA personenbezogene Daten auch zu internen Zwecken (z. B. Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten, allgemeine Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten, Gewährleistung der IT-Sicherheit und des IT-Betriebs). Das berechtigte Interesse hieran ergibt sich aus den jeweiligen Zwecken und ist im Übrigen wirtschaftlicher Natur (effiziente Aufgabenerfüllung, Vermeidung von Rechtsrisiken). Über etwaige Änderungen der Zwecke der Datenverarbeitung wird die SCHUFA gemäß Art. 14 Abs. 4 DS-GVO informieren.

### 2.2 Rechtsgrundlagen für die Datenverarbeitung

Die SCHUFA verarbeitet personenbezogene Daten auf Grundlage der Bestimmungen der Datenschutz-Grundverordnung. Die Verarbeitung erfolgt auf Basis von Einwilligungen sowie auf Grundlage des Art. 6 Abs. 1 Buchstabe f) DS-GVO, soweit die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Einwilligungen können jederzeit gegenüber dem betreffenden Vertragspartner widerrufen werden. Dies gilt auch für Einwilligungen, die bereits vor Inkrafttreten der DS-GVO erteilt wurden. Der Widerruf der Einwilligung berührt nicht die Rechtmäßigkeit der bis zum Widerruf verarbeiteten personenbezogenen Daten.

### 2.3 Herkunft der Daten

Die SCHUFA erhält ihre Daten von ihren Vertragspartnern. Dies sind im europäischen Wirtschaftsraum und in der Schweiz sowie ggf. weiteren Drittländern (sofern zu diesen ein entsprechender Angemessenheitsbeschluss der Europäischen Kommission existiert) ansässige Institute, Finanzunternehmen und Zahlungsdienstleister, die ein finanzielles Ausfallrisiko tragen (z. B. Banken, Sparkassen, Genossenschaftsbanken, Kreditkarten-, Factoring- und Leasingunternehmen) sowie weitere Vertragspartner, die zu den unter Ziffer 2.1 genannten Zwecken Produkte der SCHUFA nutzen, insbesondere aus dem (Versand-)Handels-, eCommerce-, Dienstleistungs-, Vermietungs-, Energieversorgungs-, Telekommunikations-, Versicherungs-, oder Inkassobereich. Darüber hinaus verarbeitet die SCHUFA Informationen aus allgemein zugänglichen Quellen wie öffentlichen Verzeichnissen und amtlichen Bekanntmachungen (Schuldnerverzeichnisse, Insolvenzbeschlüsse).

### 2.4 Kategorien personenbezogener Daten, die verarbeitet werden (Personendaten, Zahlungsverhalten und Vertragstreue)

- Personendaten, z. B. Name (ggf. auch vorherige Namen, die auf gesonderten Antrag beauskunftet werden), Vorname, Geburtsdatum, Geburtsort, Anschrift, frühere Anschriften
- Informationen über die Aufnahme und vertragsgemäße Durchführung eines Geschäftes (z. B. Girokonten, Ratenkredite, Kreditkarten, Pfändungsschutzkonten, Basiskonten)
- Informationen über unbestrittene, fällige und mehrfach angemahnte oder titulierte Forderungen sowie deren Erledigung
- Informationen zu missbräuchlichem oder sonstigem betrügerischem Verhalten wie Identitäts- oder Bonitätstäuschungen
- Informationen aus öffentlichen Verzeichnissen und amtlichen Bekanntmachungen
- Scorewerte

### 2.5 Kategorien von Empfängern der personenbezogenen Daten

Empfänger sind im europäischen Wirtschaftsraum, in der Schweiz sowie ggf. weiteren Drittländern (sofern zu diesen ein entsprechender Angemessenheitsbeschluss der Europäischen Kommission existiert) ansässige Vertragspartner gem. Ziffer 2.3. Weitere Empfänger können externe Auftragnehmer der SCHUFA nach Art. 28 DS-GVO sowie externe und interne SCHUFA-Stellen sein. Die SCHUFA unterliegt zudem den gesetzlichen Eingriffsbefugnissen staatlicher Stellen.

### 2.6 Dauer der Datenspeicherung

Die SCHUFA speichert Informationen über Personen nur für eine bestimmte Zeit. Maßgebliches Kriterium für die Festlegung dieser Zeit ist die Erforderlichkeit. Für eine Prüfung der Erforderlichkeit der weiteren Speicherung bzw. die Löschung personenbezogener Daten hat die SCHUFA Regelfristen festgelegt. Danach beträgt die grundsätzliche Speicherdauer von personenbezogenen Daten jeweils drei Jahre taggenau nach deren Erledigung. Davon abweichend werden z. B. gelöscht:

- Angaben über Anfragen nach zwölf Monaten taggenau
- Informationen über störungsfreie Vertragsdaten über Konten, die ohne die damit begründete Forderung dokumentiert werden (z. B. Girokonten, Kreditkarten, Telekommunikationskonten oder Energiekonten), Informationen über Verträge, bei denen die Evidenzprüfung gesetzlich vorgesehen ist (z. B. Pfändungsschutzkonten, Basiskonten) sowie Bürgschaften und Handelskonten, die kreditorisch geführt werden, unmittelbar nach Bekanntgabe der Beendigung.
- Daten aus den Schuldnerverzeichnissen der zentralen Vollstreckungsgerichte nach drei Jahren taggenau, jedoch vorzeitig, wenn der SCHUFA eine Löschung durch das zentrale Vollstreckungsgericht nachgewiesen wird

- Informationen über Verbraucher-/Insolvenzverfahren oder Restschuldbefreiungsverfahren taggenau drei Jahre nach Beendigung des Insolvenzverfahrens oder Erteilung der Restschuldbefreiung. In besonders gelagerten Einzelfällen kann auch abweichend eine frühere Löschung erfolgen.
- Informationen über die Abweisung eines Insolvenzantrages mangels Masse, die Aufhebung der Sicherungsmaßnahmen oder über die Versagung der Restschuldbefreiung taggenau nach drei Jahren
- Personenbezogene Voranschriften bleiben taggenau drei Jahre gespeichert; danach erfolgt die Prüfung der Erforderlichkeit der fortwährenden Speicherung für weitere drei Jahre. Danach werden sie taggenau gelöscht, sofern nicht zum Zwecke der Identifizierung eine länger währende Speicherung erforderlich ist.

### 3. Betroffenenrechte

Jede betroffene Person hat gegenüber der SCHUFA das Recht auf Auskunft nach Art. 15 DS-GVO, das Recht auf Berichtigung nach Art. 16 DS-GVO, das Recht auf Löschung nach Art. 17 DS-GVO und das Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO. Die SCHUFA hat für Anliegen von betroffenen Personen ein Privatkunden ServiceCenter eingerichtet, das schriftlich unter SCHUFA Holding AG, Privatkunden ServiceCenter, Postfach 10 34 41, 50474 Köln, telefonisch unter +49 (0) 6 11-92 78 0 und über ein Internet-Formular unter [www.schufa.de](http://www.schufa.de) erreichbar ist. Darüber hinaus besteht die Möglichkeit, sich an die für die SCHUFA zuständige Aufsichtsbehörde, den Hessischen Datenschutzbeauftragten, zu wenden. Einwilligungen können jederzeit gegenüber dem betreffenden Vertragspartner widerrufen werden.

**Wir sind verpflichtet Sie darauf hinzuweisen, dass Sie nach Art. 21 Abs. 1 DS-GVO der Datenverarbeitung aus Gründen, die sich aus Ihrer besonderen Situation ergeben (z. B. Zeugenschutz, Frauenhaus), widersprechen können.  
Der Widerspruch kann formfrei erfolgen und ist zu richten an  
SCHUFA Holding AG, Privatkunden ServiceCenter, Postfach 10 34 41, 50474 Köln.**

### 4. Profilbildung (Scoring)

Vor Geschäften mit einem finanziellen Ausfallrisiko möchten Geschäftspartner möglichst gut einschätzen können, ob den eingegangenen Zahlungsverpflichtungen nachgekommen werden kann. Durch die SCHUFA-Auskunft und die Profilbildung mittels sogenannter Scorewerte unterstützt die SCHUFA Kredit gebende Unternehmen bei der Entscheidungsfindung und hilft dabei, alltägliche Kreditgeschäfte rasch abwickeln zu können. Beim Scoring wird anhand von gesammelten Informationen und Erfahrungen aus der Vergangenheit eine Prognose über zukünftige Ereignisse erstellt. Die Berechnung aller Wahrscheinlichkeitswerte erfolgt bei der SCHUFA grundsätzlich auf Basis der zu einer betroffenen Person bei der SCHUFA gespeicherten Informationen, die auch in der Auskunft nach Art. 15 DS-GVO ausgewiesen werden. Darüber hinaus berücksichtigt die SCHUFA beim Scoring die Bestimmungen des § 31 BDSG. Anhand der zu einer Person gespeicherten Einträge erfolgt eine Zuordnung zu statistischen Personengruppen, die in der Vergangenheit ähnliche Einträge aufwiesen. Die Scoreberechnungen erfolgen auf mathematisch-statistisch anerkannten und bewährten Verfahren.

Folgende Datenarten werden bei der SCHUFA zur Scoreberechnung verwendet, wobei nicht jede Datenart auch in jede einzelne Scoreberechnung mit einfließt: Allgemeine Daten (z. B. Geburtsdatum, Geschlecht oder Anzahl im Geschäftsverkehr verwendeter Anschriften), bisherige Zahlungsverstörungen, Kreditaktivität letztes Jahr, Kreditnutzung, Länge Kredithistorie sowie Anschriftendaten (nur wenn wenige personenbezogene kreditrelevante Informationen vorliegen). Bestimmte Informationen werden weder gespeichert noch bei der Berechnung von Scorewerten berücksichtigt, z. B. Angaben zur Staatsangehörigkeit oder besonders sensible Daten nach Art. 9 DS-GVO (z. B. ethnische Herkunft oder Angaben zu politischen oder religiösen Einstellungen). Auch die Geltendmachung von Rechten nach der DS-GVO, also z. B. die Einsichtnahme in die bei der SCHUFA gespeicherten Informationen nach Art. 15 DS-GVO, hat keinen Einfluss auf die Scorewerte.

Mit welcher Wahrscheinlichkeit eine Person einen Baufinanzierungskredit zurückzahlen wird, muss nicht der Wahrscheinlichkeit entsprechen, mit der sie eine Rechnung beim Versandhandel termingerecht bezahlt. Aus diesem Grund bietet die SCHUFA ihren Vertragspartnern unterschiedliche branchenspezifische Scoremodelle an, die sogenannten SCHUFA-Branchenscores. Diese repräsentieren in der Regel die Wahrscheinlichkeit einer Zahlungsverstörung innerhalb von 15 Monaten. Bei einzelnen Branchen kann der Zeitraum abweichen, um besser auf Eigenheiten der branchenüblichen Geschäftsmodelle einzugehen (z. B. Telekommunikation, Baufinanzierung). Scores verändern sich stetig, da sich auch die Informationen, die bei der SCHUFA über eine Person gespeichert sind, verändern. So kommen neue Informationen hinzu, während andere aufgrund von Speicherfristen gelöscht werden. Außerdem ändern sich auch die Informationen selbst im Zeitverlauf (etwa die Dauer des Bestehens einer Geschäftsbeziehung), so dass auch ohne neue Informationen Veränderungen auftreten.

Wichtig zu wissen: Die SCHUFA selbst trifft keine Entscheidungen, sie unterstützt die ihr angeschlossenen Vertragspartner lediglich mit ihren Informationen bei der Entscheidungsfindung. Die Risikoeinschätzung und Beurteilung der Kreditwürdigkeit erfolgt allein durch den direkten Geschäftspartner, da nur dieser über zahlreiche zusätzliche Informationen – wie zum Beispiel die aus einem Kreditantrag – verfügt. Dies gilt selbst dann, wenn er sich einzig auf die von der SCHUFA gelieferten Informationen und Scorewerte verlässt.

Unabhängig vom Bonitätsscoring unterstützt die SCHUFA ihre Geschäftspartner mit dem FraudPreCheck (FPC) durch Profilbildungen bei der Erkennung auffälliger Sachverhalte (z. B. zum Zwecke der Betrugsprävention im Versandhandel). Hierzu erfolgt eine Analyse von Anfragen von Geschäftspartnern der SCHUFA, um diese auf potenzielle Auffälligkeiten hin zu prüfen. In diese Berechnung, die für den jeweiligen Geschäftspartner individuell erfolgt, können neben Anfragen der zurückliegenden 90 Tage, die aufgrund von Erkenntnissen der SCHUFA zu bekannten Manipulationsmustern von der angefragten betroffenen Person stammen, auch Anschriftendaten, Informationen ob und in welcher Funktion in allgemein zugänglichen Quellen ein Eintrag zu einer Person des öffentlichen Lebens mit übereinstimmenden Personendaten existiert, sowie aggregierte statistische Informationen aus dem SCHUFA-Datenbestand einfließen. Darüber hinaus können auch die jeweils aufgeführten Anfragezeiten bei der Ermittlung der Auffälligkeit berücksichtigt werden, wobei die SCHUFA davon ausgeht, dass innerhalb von drei Stunden vor dem aufgeführten Anfragezeitpunkt die Antragstellung durch die betroffene Person erfolgte.

Unter Einbeziehung dieser Informationen wird sodann ein zehnstelliger Auffälligkeitswert (FPC-Wert) zwischen 0 und 1 ermittelt und an den Geschäftspartner ausgegeben. Dabei gilt: je kleiner der ermittelte FPC-Wert, desto unauffälliger sind die Anfragedaten, je größer der Wert, desto größer die Auffälligkeit. Die Geschäftspartner der SCHUFA können den Wert zur weiteren risikovermindernden Steuerung ihrer Geschäftsprozesse einsetzen. Welche Bedeutung ein konkreter FPC-Wert für den jeweiligen Geschäftspartner hat, entscheidet dieser stets selbst anhand der jeweiligen Risikostruktur. Eine erhöhte Auffälligkeit kann z. B. dazu führen, dass der Geschäftspartner risikobehaftete Zahlungsarten wie den Rechnungskauf nicht anbietet, sie ist jedoch allein kein Grund, einen Antrag abzulehnen. Die Geschäftspartner setzen neben dem FPC-Wert auch eigene Verfahren zur Betrugsprävention ein, die häufig miteinander kombiniert werden.

Da sich ein Geschäftsvorgang im Distanzhandel bis beispielsweise zur Auslieferung der bestellten Ware über mehrere Schritte hinziehen kann, kann der Geschäftspartner bis zum Abschluss des Geschäftsvorgangs neu bekannt gewordene Informationen über Auffälligkeiten in Form aktualisierter FPC-Werte abrufen.

Die von den Geschäftspartnern zum Zwecke der Betrugsprävention übermittelten Anfragedaten werden bei der SCHUFA taggenau 12 Monate gespeichert und auf der Datenkopie (nach Art. 15 DS-GVO) ausgewiesen. Ferner werden die personenbezogenen Daten ausgewiesen, die zur Verarbeitung in diesem Verfahren aktuell bei der SCHUFA gespeichert sind. Auswirkungen auf die Bonitätsbeurteilung und das Bonitätsscoring durch die SCHUFA hat das FPC-Verfahren nicht.

Weitere Informationen zum Kreditwürdigkeitsscoring oder zur Erkennung auffälliger Sachverhalte sind unter <http://www.scoring-wissen.de> erhältlich.

# Sonderbedingungen für das PSD OnlineBanking



PSD Bank Nürnberg eG

Stand: September 2019, gültig ab 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 Zahlungsdienstenaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.

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

(3) Zur Nutzung des Online Banking gelten die mit der Bank gesondert vereinbarten Verfügungsmitel. Eine Änderung dieser Mitel kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

## 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 berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des Personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).

(3) Authentifizierungselemente sind

- Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer (PIN) oder der Nutzungscode für die elektronische Signatur) und
- 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), sowie
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

(4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements 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, Anmeldename) 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 (z. B. Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z. B. Eingabe einer TAN oder elektronische Signatur als Nachweis des Besitzelements) zu verwenden, sofern mit der Bank nichts anderes vereinbart wurde. 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 (z. B. Sonderbedingungen 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.

## 5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der 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 Arbeitslaufs. 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 darauffolgenden 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).
- 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 (vgl. Nummer 1 Absatz 3 dieser Bedingungen).
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Sonderbedingungen 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 (z. B. Sonderbedingungen für den Überweisungsverkehr, Sonderbedingungen für Wertpapiergeschäfte) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen und dem Teilnehmer eine Information 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 zur Verfügung stellen.

## 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 (vgl. Nummern 3 und 4 dieser Bedingungen).

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

- Wissenselemente, 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) weitergegeben 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 Fingerabdruck-sensor) 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) weitergegeben werden und
  - muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das Online Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen 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 (z. B. Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.

(4) Die für das mobileTAN-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 (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (z. B. 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. Bei Feststellung von Abweichungen ist die Transaktion abzubrechen.

## 8. Anzeigepflichten 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) 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 eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.

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

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

### 8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte 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 der Nutzungscode für die elektronische Signatur dreimal in Folge 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 den 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 (z. B. Sonderbedingungen für den Überweisungsverkehr, Sonderbedingungen für Wertpapiergeschäfte).

### **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-gekomenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

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

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

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine 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 den Absätzen 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 Absätzen 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Sorgfalts- und Anzeigepflichten 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**

Beruhen 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.

## **11. Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit**

Für die Beilegung von Streitigkeiten mit der Bank kann sich der Teilnehmer an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- oder Beschwerdestellen wenden.



# Sonderbedingungen für die Nutzung des elektronischen Postfachs



PSD Bank Nürnberg eG

Stand: Juli 2017

## 1. Das elektronische Postfach

Die Bank bietet dem Kunden die Möglichkeit eines Zugangs zu seinen bei der Bank geführten Konten und Depots über das Internet. Im Rahmen der Geschäftsbeziehung zwischen der Bank und dem Kunden, der für die Nutzung des elektronischen Postfachs freigeschaltet ist, gilt das elektronische Postfach als Kommunikationsweg. Der Kunde kann das elektronische Postfach im bereitgestellten Funktionsumfang nutzen. Wenn der Bevollmächtigte Zugang zum Online Banking hat, ist ihm die Nutzung des elektronischen Postfachs in gleicher Weise wie dem Kontoinhaber bzw. den Kontoinhabern gestattet.

## 2. Übermittlung von Konto- und Kundendokumenten

Bei Nutzung des elektronischen Postfachs werden dem Kunden sämtliche Konto- und Kundendokumente dort eingestellt. Dies umfasst beispielsweise Konto- und Depotauszüge, Rechnungsabschlüsse, Kreditkartenabrechnungen sowie Angebote zur Änderung der Allgemeinen Geschäftsbedingungen, Sonderbedingungen oder Entgelte.

## 3. Verzicht auf papierhafte Konto- und Kundendokumente

Die Bank kann ihre Informationsverpflichtungen aus der Geschäftsbeziehung dadurch erfüllen, dass sie Informationen elektronisch in den Posteingang übersendet. Die Übersendung der Mitteilung erfolgt insbesondere durch Einstellung von Dateien im PDF-Format in das elektronische Postfach. Die Bank wird die Informationen, die sie im Posteingang bereitstellt, grundsätzlich nicht zusätzlich papierhaft versenden. Der Kunde verzichtet ausdrücklich auf den postalischen Versand dieser Informationen, wenn die entsprechenden Konten auf das elektronische Postfach umgestellt sind. Die Bank bleibt dazu berechtigt, dem Kunden Dokumente per Post zuzusenden, wenn sie dies unter Berücksichtigung der Kundeninteressen für zweckmäßig hält oder es aus rechtlichen Gründen erforderlich ist.

## 4. Mitwirkungspflichten des Kunden

Der Kunde ist verpflichtet, regelmäßig und zeitnah die Informationen im Posteingang abzurufen und die Inhalte zu prüfen. Er hat der Bank eventuelle Unstimmigkeiten unverzüglich anzuzeigen.

## 5. Kündigung

Der Kunde kann die Nutzung des elektronischen Postfachs jederzeit in Textform ohne Einhaltung einer Frist kündigen. Die Bank kann die Nutzung des elektronischen Postfachs jederzeit mit einer Frist von 2 Monaten kündigen, es sei denn, es liegt ein wichtiger Grund vor, der sie zu einer außerordentlichen Kündigung berechtigen würde. Ein wichtiger Grund liegt insbesondere dann vor, wenn es der Bank auch unter angemessener Berücksichtigung der Belange des Kunden unzumutbar erscheint, den elektronischen Postfach-Dienst fortzusetzen.

Die Bank wird nach dem Wirksamwerden einer Kündigung alle Informationen im Rahmen der Geschäftsbeziehung per Post an die vom Kunden angegebene Anschrift versenden. Im Falle einer fristlosen Kündigung durch den Kunden kann dieses jedoch erst nach einer angemessenen Bearbeitungszeit erfolgen. Die Bank ist nicht verpflichtet, dem Kunden die im Zeitpunkt des Wirksamwerdens der Kündigung im Posteingang befindlichen Informationen nachträglich postalisch zuzusenden. Die Entgelte ergeben sich aus dem „Preis- und Leistungsverzeichnis“.

## 6. Anerkennung durch Finanzbehörden

Kunden, die handels- und steuerrechtlichen Aufbewahrungspflichten unterliegen, sollten sich bei einem Angehörigen der steuerberatenden Berufe informieren, was im Fall des Bezugs von elektronischen Dokumenten (z. B. Kontoauszügen) zur Erfüllung dieser Pflichten zu beachten ist.

Die Informationen können nach ihrer Übermittlung in den Posteingang nicht verändert werden. Die Bank garantiert die Unveränderbarkeit der in das elektronische Postfach bereit gestellten Daten. Diese Garantie gilt jedoch nicht, sofern die Daten außerhalb des elektronischen Postfachs gespeichert oder aufbewahrt werden. Dabei ist zu beachten, dass ein Ausdruck eines Dokuments aufgrund der individuellen Hard- oder Softwareeinstellung von der Darstellung am Bildschirm abweichen kann. Soweit die Dokumente verändert werden oder in veränderter Form in Umlauf gebracht werden, haftet die Bank hierfür nicht.