

Basiskonto



Nürnberg eG

DE 133546227

Steuernummer bzw. Umsatzsteuer-Identifikationsnummer

Umsatzsteuerbefreite Finanzdienstleistung, soweit sie nicht die Verwahrung und Verwaltung von Wertpapieren zum Gegenstand hat.

PSD Personennummer

Rechnungsnummer gemäß § 14 Abs. 4 Nr. 4 UStG

MH: | B: | I: | A: | IQ: | VK:

Vertriebsdokumentation (**wird von der Bank ausgefüllt**)

Antwort

PSD Bank Nürnberg eG
90328 Nürnberg

Kontoinhaber

Frau Herr

Vorname, Name

Straße, Hausnummer

PLZ, Ort

Geburtsdatum

Geburtsort

Geburtsname

Ich beantrage die Eröffnung eines Einzelkundenstammes zu den aktuell gültigen Bedingungen der PSD Bank.

Weitere Angaben zum Kontoinhaber

Steuer-Identifikationsnummer

- | | | |
|--|--|---|
| <input type="checkbox"/> Angestellte/r | <input type="checkbox"/> Schüler/in | <input type="checkbox"/> Hausfrau/Hausmann |
| <input type="checkbox"/> Beamter/Beamtin | <input type="checkbox"/> Student/in | <input type="checkbox"/> Selbstständige/r (Kontoführung nur für private Zwecke) |
| <input type="checkbox"/> Arbeiter/in | <input type="checkbox"/> Auszubildende/r | <input type="checkbox"/> Öffentlicher Dienst |
| <input type="checkbox"/> Rentner | <input type="checkbox"/> Pensionär | |

Familienstand

- ledig verheiratet verwitwet
 geschieden getrennt lebend eingetragene Lebenspartnerschaft

Güterstand

- Zugewinngemeinschaft (gesetzlich)
 Gütertrennung Gütergemeinschaft

Beruf

Name und Anschrift des Arbeitgebers

Staatsangehörigkeit

Telefon privat

Telefon geschäftlich

Mobil

E-Mail

Kundenzeitschrift „Geld & Gewinn“ per Mail (E-Mailadresse bitte angeben)

Eröffnung eines Basiskontos

Ich beantrage die Eröffnung eines Basiskontos mit vierteljährlichem Rechnungsabschluss und monatlichem Kontoauszug.

Karte

Ja, ich möchte eine girocard V PAY (Debitkarte) mit Geheimzahl¹

¹Auf dem Chip der girocard V PAY (Debitkarte) wird das Geburtsdatum verschlüsselt – also für Dritte nicht lesbar – hinterlegt. Dadurch ist es möglich, sich beispielsweise an Automaten, die eine Alterserkennung prüfen, zu legitimieren, um die angebotene Ware zu erwerben.

Selbstauskunft Auslandssteuer (nur wenn zutreffend, bitte ankreuzen)

Ich bin Staatsangehöriger der USA.

Ich bin in den USA steuerlich ansässig.¹

US-Steuer-Identifikationsnummer (TIN / SSN)

Ich bin steuerlich im Ausland ansässig¹ in

Land (außer Deutschland und USA)

Steuer-Identifikationsnummer aus diesem Land

Die Selbstauskunft ersetzt alle vorausgegangenen Selbstauskünfte des Kontoinhabers/Treuegebers.

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

¹Die 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.

Geldwäschegesetz

Angaben zum wirtschaftlich Berechtigten gemäß Geldwäschegesetz: Ich versichere/wir versichern, dass ich/wir für die gesamte Kundenverbindung unter der o. a. Kundennummer im eigenen wirtschaftlichen Interesse und nicht auf fremde Veranlassung (insbesondere nicht als Treuhänder) handle/handeln.

Informationen zum Kundenstammvertrag

Der Kundenstammvertrag ist ein Vorvertrag, der sich auf die Kontoführung aller gegenwärtigen und künftigen Konten und Depots des Kunden bei der Bank zu den im Kundenstammvertrag festgelegten Daten und getroffenen Vereinbarungen bezieht. Er dient dazu, das Verfahren zwischen der Bank und dem Kunden auch beim Vorhandensein mehrerer Konten und Anlageformen zu vereinfachen. Es gibt keinen Leistungsvorbehalt, es sei denn, dieser ist ausdrücklich vereinbart. Der Abschluss des Kundenstammvertrags begründet für den Kunden keine Zahlungsverpflichtung und für die Bank keine Leistungsverpflichtungen.

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.

Vereinbarung

Alle gegenwärtigen und künftigen Konten und Depots unter der vorstehend genannten Kundennummer wird die Bank zu den im Kundenstamm-Vertrag festgelegten Daten und getroffenen Vereinbarungen führen.

Zweck / Sicherheiten

Der/die Kontoinhaber dürfen die eingeräumte oder geduldete Kontoüberziehung nicht für einen gebäudewirtschaftlichen Zweck im Sinne von § 491 Abs. 3 BGB in Anspruch nehmen. Der PSD Bank als Sicherheit eingeräumte, bestehende oder zukünftige Grundpfandrechte sowie bestehende oder zukünftige Reallasten haften nicht für eingeräumte bzw. geduldete Kontoüberziehungen.

Vorvertragliche Information (inkl. Fernabsatz)

Die Vorvertragliche Information (inkl. Fernabsatz) zum PSD GiroVertrag habe/n ich/wir erhalten bzw. wurde/n mir/uns zugesandt.

Bedingungen

Für den gesamten Geschäftsverkehr gelten ergänzend die Allgemeinen Geschäftsbedingungen der Bank und deren Sonderbedingungen für den Überweisungsverkehr, 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 eingesehen werden; auf Verlangen werden diese Bedingungen auch ausgehändigt oder zugesandt.

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 und 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 eingesehen werden.

Kündigung eines Basiskontos durch die Bank

Die PSD Bank kann den Basiskontovertrag unter Einhaltung einer Kündigungsfrist von mindestens 2 Monaten kündigen, wenn

- über das Basiskonto in mehr als 24 aufeinanderfolgenden Monaten kein vom Kontoinhaber in Auftrag gegebener Zahlungsvorgang ausgeführt wurde,
- der Kontoinhaber die Voraussetzungen des § 31 Absatz 1 Satz 2 Zahlungskontengesetz nicht mehr erfüllt,
- der Kontoinhaber ein weiteres Zahlungskonto, das von ihm nach Maßgabe des § 35 Abs. 1 Satz 1 und 2 Zahlungskontengesetz genutzt werden kann, im Geltungsbereich des Zahlungskontengesetzes eröffnet hat oder
- der Kontoinhaber eine angekündigte Änderung des Basiskontovertrages nach § 675g des Bürgerlichen Gesetzbuchs abgelehnt hat, die die PSD Bank allen Inhabern von bei ihr geführten entsprechenden Basiskonten wirksam angeboten hat.

Darüber hinaus kann die PSD Bank den Basiskontovertrag unter den Voraussetzungen des § 42 Absatz 2 und 3 des Zahlungskontengesetzes unter Einhaltung einer Kündigungsfrist von mindestens zwei Monaten kündigen. Ohne Einhaltung einer Kündigungsfrist kann die PSD Bank den Basiskontovertrag unter den Voraussetzungen des § 42 Absätze 4 und 5 des Zahlungskontengesetzes kündigen.

Information zur außergerichtlichen Streitschlichtung

Die Bank nimmt am Streitbeilegungsverfahren 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 zu richten.

Betrifft der Beschwerdegegenstand eine Streitigkeit aus dem Anwendungsbereich des Zahlungsdiensterechts (§§ 675c bis 676c des Bürgerlichen Gesetzbuches, 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, E-Mail: schlichtungsstelle@bafin.de.

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

Ort, Datum


Unterschrift des Kontoinhabers/gesetzlichen Vertreters

Legitimationsprüfung

Die Unterschrift(en) unter diesen Vertrag
Er/Sie hat/haben sich ausgewiesen durch

- wurde(n) vor mir von dem/den Unterzeichner(n) geleistet. wurde(n) von mir geprüft. Postident
 Personalausweis Reisepass Geburtsurkunde Sofort-Legitimation

Nr. _____ ausstellende Behörde _____ Ausstellungsdatum _____ gültig bis _____
Staatsangehörigkeit _____ Geburtsdatum _____ Geburtsort _____

Ort, Datum

Mitarbeiter der PSD Bank/Stempel und Unterschrift der bescheinigenden Stelle

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

Erläuterungen

¹ 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.

² 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.

³ 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 <http://www.bvr-institutssicherung.de>.

⁴ 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 <http://www.bvr-institutssicherung.de>.

⁵ 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

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 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, Anschriftenermittlung, Kundenbetreuung oder Risikosteuerung sowie der Tarifierung oder Konditionierung. Über etwaige Änderungen der Zwecke der Datenverarbeitung wird die SCHUFA gemäß Artikel 14 Absatz 4 DSGVO 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 Artikel 6 Absatz 1 Buchstabe f DSGVO, 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 DSGVO 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, Insolvenzbekanntmachungen).

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 Artikel 28 DSGVO 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 wählende Speicherung erforderlich ist.

3. Betroffenenrechte

Jede betroffene Person hat gegenüber der SCHUFA das Recht auf Auskunft nach Artikel 15 DSGVO, das Recht auf Berichtigung nach Artikel 16 DSGVO, das Recht auf Löschung nach Artikel 17 DSGVO und das Recht auf Einschränkung der Verarbeitung nach Artikel 18 DSGVO. 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 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.

Nach Artikel 21 Absatz 1 DSGVO kann der Datenverarbeitung aus Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, widersprochen werden. Der Widerspruch kann formfrei erfolgen und ist zu richten an SCHUFA Holding AG, Privatkunden ServiceCenter, Postfach 10 34 41, 50474 Köln.

4. Profilbildung (Scoring)

Die SCHUFA-Auskunft kann um sogenannte Scorewerte ergänzt werden. Beim Scoring wird anhand von gesammelten Informationen und Erfahrungen aus der Vergangenheit eine Prognose über zukünftige Ereignisse erstellt. Die Berechnung aller Scorewerte erfolgt bei der SCHUFA grundsätzlich auf Basis der zu einer betroffenen Person bei der SCHUFA gespeicherten Informationen, die auch in der Auskunft nach Artikel 15 DSGVO ausgewiesen werden. Darüber hinaus berücksichtigt die SCHUFA beim Scoring die Bestimmungen § 31 BDSG. Anhand der zu einer Person gespeicherten Einträge erfolgt eine Zuordnung zu statistischen Personengruppen, die in der Vergangenheit ähnliche Einträge aufwiesen. Das verwendete Verfahren wird als „logistische Regression“ bezeichnet und ist eine fundierte, seit langem praxiserprobte, mathematisch-statistische Methode zur Prognose von Risikowahrscheinlichkeiten.

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 Zahlungsstörungen, 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 besondere Kategorien personenbezogener Daten wie ethnische Herkunft oder Angaben zu politischen oder religiösen Einstellungen nach Artikel 9 DSGVO. Auch die Geltendmachung von Rechten nach der DSGVO, also z.B. die Einsichtnahme in die bei der SCHUFA gespeicherten Informationen nach Artikel 15 DSGVO, hat keinen Einfluss auf die Scoreberechnung.

Die übermittelten Scorewerte unterstützen die Vertragspartner bei der Entscheidungsfindung und gehen dort in das Risikomanagement ein. Die Risikoeinschätzung und Beurteilung der Kreditwürdigkeit erfolgt allein durch den direkten Geschäftspartner, da nur dieser über zahlreiche zusätzliche Informationen – zum Beispiel aus einem Kreditantrag – verfügt. Dies gilt selbst dann, wenn er sich einzig auf die von der SCHUFA gelieferten Informationen und Scorewerte verlässt. Ein SCHUFA-Score alleine ist jedenfalls kein hinreichender Grund einen Vertragsabschluss abzulehnen.

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: April 2017, gültig bis 12.01.2018

1. Leistungsangebot

(1) Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.

(2) Der Teilnehmer kann Bankgeschäfte mittels OnlineBanking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels OnlineBanking abrufen.

(3) Zur Nutzung des OnlineBanking gelten die mit der Bank gesondert vereinbarten Verfügungsmitte. Eine Änderung dieser Limite kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

2. Voraussetzungen zur Nutzung des OnlineBanking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels OnlineBanking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (vgl. Nummer 3) und Aufträge zu autorisieren (vgl. Nummer 4).

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind:

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

2.2 Authentifizierungsinstrumente

Die TAN bzw. die elektronische Signatur können dem Teilnehmer auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:

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

Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

3. Zugang zum OnlineBanking

Der Teilnehmer erhält Zugang zum OnlineBanking, wenn

- der Teilnehmer die Kontonummer oder seine individuelle Kundenkennung (PSD-Key oder Alias) und seine PIN oder elektronische Signatur übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (vgl. Nummer 7.1 und 8) vorliegt.

Nach Gewährung des Zugangs zum OnlineBanking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

4. OnlineBanking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss OnlineBanking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (TAN oder elektronische Signatur) autorisieren und der Bank mittels OnlineBanking übermitteln. Die Bank bestätigt mittels OnlineBanking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

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

5. Bearbeitung von OnlineBanking-Aufträgen durch die Bank

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

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

- Der Teilnehmer hat sich mit dem Personalisierten Sicherheitsmerkmal autorisiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das OnlineBanking-Datenformat ist eingehalten.
- Das gesondert vereinbarte OnlineBanking-Verfügungsmitte ist nicht überschritten.
- Die Ausführungsvoraussetzungen 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 OnlineBanking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den OnlineBanking-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 OnlineBanking zur Verfügung stellen.

6. Sorgfaltspflichten des Teilnehmers

6.1 Technische Verbindung zum OnlineBanking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum OnlineBanking nur über die von der Bank gesondert mitgeteilten OnlineBanking-Zugangskanäle (z. B. Internetadresse) herzustellen.

6.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer hat

- seine Personalisierten Sicherheitsmerkmale (vgl. Nummer 2.1) geheim zu halten und nur im Rahmen einer Auftragserteilung über die von der Bank gesondert mitgeteilten OnlineBanking-Zugangskanäle an diese zu übermitteln sowie
 - sein Authentifizierungsinstrument (vgl. Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.
- Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen Personalisierten Sicherheitsmerkmal das OnlineBanking-Verfahren missbräuchlich nutzen.

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

- Die Personalisierten Sicherheitsmerkmale dürfen nicht elektronisch gespeichert werden (z. B. im Kundensystem).
- Bei Eingabe der Personalisierten Sicherheitsmerkmale ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- Die Personalisierten Sicherheitsmerkmale dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf Online-Händlerseiten).

- Die Personalisierten Sicherheitsmerkmale dürfen nicht außerhalb des OnlineBanking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die PIN und der Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung z. B. eines Auftrags, der Aufhebung einer Sperre nicht mehr als eine TAN verwenden.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht für das OnlineBanking genutzt werden.

6.3 Sicherheit des Kundensystems

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

6.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

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

7. Anzeige- und Unterrichtungspflichten

7.1 Sperranzeige

(1) Stellt der Teilnehmer den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seiner Persönlichen Sicherheitsmerkmale fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über eine gesondert mitgeteilte Telefonnummer aufgeben.

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

- Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt
 - den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seiner Personalisierten Sicherheitsmerkmale erlangt hat oder
 - das Authentifizierungsinstrument oder die Personalisierten Sicherheitsmerkmale verwendet,
 muss er ebenfalls eine Sperranzeige abgeben.

7.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

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

8. Nutzungssperre

8.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 7.1,

- den OnlineBanking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument.

8.2 Sperre auf Veranlassung der Bank

- (1) Die Bank darf den OnlineBanking-Zugang für einen Teilnehmer sperren, wenn
 - sie berechtigt ist, den OnlineBanking-Vertrag aus wichtigem Grund zu kündigen,
 - sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
 - der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.

(2) Die Bank wird den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

8.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal bzw. das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber.

8.4 Automatische Sperre eines chip-basierten Authentifizierungsinstruments

- (1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn der Nutzungscode für die elektronische Signatur dreimal in Folge falsch eingegeben wird.
- (2) Ein TAN-Generator, der die Eingabe eines eigenen Nutzungscode erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.
- (3) Die in den Absätzen 1 und 2 genannten Authentifizierungsinstrumente können dann nicht mehr für das OnlineBanking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des OnlineBanking wiederherzustellen.

9. Haftung

9.1 Haftung der Bank bei nicht autorisierten und nicht oder fehlerhaft ausgeführten OnlineBanking-Verfügungen

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

9.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

9.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

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

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

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

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 7.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

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

- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmale der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (vgl. Nummer 7.1 Absatz 1),
- die Personalisierten Sicherheitsmerkmale im Kundensystem gespeichert hat (vgl. Nummer 6.2 Absatz 2, 1. Spiegelstrich),
- die Personalisierten Sicherheitsmerkmale einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde (vgl. Nummer 6.2 Absatz 1, 2. Spiegelstrich),
- die Personalisierten Sicherheitsmerkmale erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (vgl. Nummer 6.2 Absatz 2, 3. Spiegelstrich),
- die Personalisierten Sicherheitsmerkmale außerhalb des OnlineBanking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (vgl. Nummer 6.2 Absatz 2, 4. Spiegelstrich),
- die Personalisierten Sicherheitsmerkmale auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (vgl. Nummer 6.2 Absatz 2, 5. Spiegelstrich),

- mehr als eine TAN zur Autorisierung eines Auftrags verwendet (vgl. Nummer 6.2 Absatz 2, 6. Spiegelstrich),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das OnlineBanking nutzt (vgl. Nummer 6.2 Absatz 2, 7. Spiegelstrich).

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

9.2.2 Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhend nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften der Kontoinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

9.2.3 Haftung der Bank ab der Sperranzeige

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

9.2.4 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.

10. 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.

11. Hinweis nach § 13 Abs. 1 TMG (Telemediengesetz)

Alle im Rahmen des OnlineBanking anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und gegebenenfalls dem von ihr beauftragten Rechenzentrum innerhalb Deutschlands bzw. der Europäischen Union verarbeitet.

Sonderbedingungen für das PSD OnlineBanking



PSD Bank Nürnberg eG

Stand: Januar 2018, gültig ab 13.01.2018

1. Leistungsangebot

(1) Der Konto-/Depotinhaber und dessen Bevollmächtigte können Bankgeschäfte mittels OnlineBanking in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels OnlineBanking abrufen. Der Inhaber eines Zahlungskontos und dessen Bevollmächtigte sind zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrages einen Zahlungsauslösedienst gemäß § 1 Absatz 33 Zahlungsdienststeuergesetz zu nutzen und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienst gemäß § 1 Absatz 34 Zahlungsdienststeuergesetz zu nutzen.

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

(3) Zur Nutzung des OnlineBanking 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 OnlineBanking

Der Teilnehmer benötigt für die Nutzung des OnlineBanking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Zahlungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4). Statt eines Personalisierten Sicherheitsmerkmals kann auch ein biometrisches Merkmal des Teilnehmers zum Zwecke der Authentifizierung bzw. Autorisierung vereinbart werden.

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die die Bank dem Teilnehmer zum Zwecke der Authentifizierung bzw. Autorisierung bereitstellt. Dies sind beispielsweise:

- die persönliche Identifikationsnummer (PIN) oder der Nutzungscode für die elektronische Signatur und
- einmal verwendbare Transaktionsnummern (TAN).

2.2 Zahlungsinstrumente

Zahlungsinstrumente sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurden und die vom Teilnehmer zur Erteilung eines OnlineBanking-Auftrags verwendet werden. Insbesondere mittels folgender Zahlungsinstrumente kann die TAN bzw. die elektronische Signatur dem Teilnehmer zur Verfügung gestellt werden:

- TAN-Generator, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist,
- OnlineBanking-App auf einem mobilen Endgerät (z. B. Mobiltelefon) zum Empfang oder zur Erzeugung von TAN,
- mobiles Endgerät (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
- Chipkarte mit Signaturfunktion oder
- sonstiges Zahlungsinstrument, auf dem sich Signaturschlüssel befinden.

3. Zugang zum OnlineBanking

Der Teilnehmer erhält Zugang zum OnlineBanking, wenn

- der Teilnehmer die Kontonummer oder seine individuelle Teilnehmererkennung (PSD-Key oder Alias) und seine PIN oder elektronische Signatur übermittelt oder sein biometrisches Merkmal eingesetzt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummer 9) vorliegt.

Nach Gewährung des Zugangs zum OnlineBanking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen. Die Sätze 1 und 2 gelten auch, wenn Zahlungsaufträge über einen Zahlungsauslösedienst ausgelöst und Zahlungskontoinformationen über einen Kontoinformationsdienst angefordert werden (siehe Nummer 1 Absatz 1 Satz 3).

4. OnlineBanking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss OnlineBanking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem von der Bank bereitgestellten Personalisierten Sicherheitsmerkmal (z. B. TAN oder elektronische Signatur) oder mit dem vereinbarten biometrischen Sicherheitsmerkmal autorisieren und der Bank mittels OnlineBanking übermitteln, sofern mit der Bank nichts anderes vereinbart wurde. Die Bank bestätigt mittels OnlineBanking den Eingang des Auftrags. Die Sätze 1 und 2 gelten auch, wenn der Inhaber eines Zahlungskontos und dessen Bevollmächtigte Zahlungsaufträge über einen Zahlungsauslösedienst (siehe Nummer 1 Absatz 1 Satz 3) auslösen und übermitteln.

4.2 Widerruf von Aufträgen

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

5. Bearbeitung von OnlineBanking-Aufträgen durch die Bank

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

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

- Der Teilnehmer hat den Auftrag autorisiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das OnlineBanking-Datenformat ist eingehalten.
- Das gesondert vereinbarte OnlineBanking-Verfügungslimit ist nicht überschritten.
- Die weiteren Ausführungsvoraussetzungen 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 OnlineBanking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den OnlineBanking-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 OnlineBanking zur Verfügung stellen.

6. Information des Kontoinhabers über OnlineBanking-Verfügungen

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

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum OnlineBanking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum OnlineBanking über die von der Bank gesondert mitgeteilten OnlineBanking-Zugangskanäle (z. B. Internetadresse) herzustellen. Der Inhaber eines Zahlungskontos und dessen Bevollmächtigte können zur Auslösung von Zahlungsaufträgen und zur Anforderung von Zahlungskontoinformationen auch über einen von ihnen ausgewählten Zahlungsauslösedienst oder Kontoinformationsdienst (siehe Nummer 1 Absatz 1 Satz 3) die technische Verbindung zum OnlineBanking herstellen.

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Zahlungsinstrumente

(1) Der Teilnehmer hat

- seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten sowie
- sein Zahlungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Zahlungsinstruments ist, kann in Verbindung mit der Kenntnis des dazugehörigen Personalisierten Sicherheitsmerkmals das OnlineBanking-Verfahren missbräuchlich nutzen.

Die Geheimhaltungspflicht bezüglich des Personalisierten Sicherheitsmerkmals nach Satz 1 gilt nicht für den Inhaber eines Zahlungskontos und dessen Bevollmächtigte gegenüber Zahlungsauslösediensten und Kontoinformationsdiensten (siehe Nummer 1 Absatz 1 Satz 3), wenn diese Zahlungsaufträge über einen Zahlungsauslösedienst auslösen oder Zahlungskontoinformationen über einen Kontoinformationsdienst anfordern.

(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Zahlungsinstruments zu beachten:

- Die Personalisierten Sicherheitsmerkmale dürfen nicht ungesichert elektronisch gespeichert werden.
- Bei Eingabe der Personalisierten Sicherheitsmerkmale ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- Die Personalisierten Sicherheitsmerkmale dürfen nicht per E-Mail oder anderen Telekommunikationsmitteln weitergegeben werden.
- Das Personalisierte Sicherheitsmerkmal (z. B. PIN) darf nicht zusammen mit dem Zahlungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung z. B. eines Auftrags oder der Aufhebung einer Sperre nicht mehr als eine TAN verwenden.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht für das OnlineBanking genutzt werden.

7.3 Sicherheitshinweise der Bank

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

7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

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

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer den Verlust oder den Diebstahl des Zahlungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Zahlungsinstruments oder eines seiner Personalisierten Sicherheitsmerkmale fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

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

(3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt

- den Besitz an seinem Zahlungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder
 - das Zahlungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet,
- muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

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

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

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

- den OnlineBanking-Zugang für ihn oder alle Teilnehmer oder
- sein Zahlungsinstrument.

9.2 Sperre auf Veranlassung der Bank

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

- sie berechtigt ist, den OnlineBanking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Zahlungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Zahlungsinstruments besteht.

(2) Die Bank wird den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal bzw. das Zahlungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber unverzüglich.

9.4 Automatische Sperre eines Chip-basierten Zahlungsinstruments

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

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

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

10. Haftung

10.1 Haftung der Bank bei einer nicht autorisierten OnlineBanking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten OnlineBanking-Verfügung

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

10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung eines Personalisierten Sicherheitsmerkmals oder eines Zahlungsinstruments

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen oder sonst abhanden gekommenen Zahlungsinstruments oder auf der sonstigen missbräuchlichen Verwendung eines Zahlungsinstruments, haftet der Kontoinhaber 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 Kontoinhaber 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 Zahlungsinstruments vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Zahlungsinstruments 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 Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er

- den Verlust oder Diebstahl des Zahlungsinstruments oder die missbräuchliche Nutzung des Zahlungsinstruments oder des Personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1 Absatz 1),
- das Personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe Nummer 7.2 Absatz 2, 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1),
- das Personalisierte Sicherheitsmerkmal per E-Mail oder anderen Telekommunikationsmitteln weitergegeben hat (siehe Nummer 7.2 Absatz 2, 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Zahlungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2, 4. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet (siehe Nummer 7.2 Absatz 2, 5. Spiegelstrich),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das OnlineBanking nutzt (siehe Nummer 7.2 Absatz 2, 6. Spiegelstrich).

(4) Abweichend von den Absätzen 1 und 3 ist der Kontoinhaber nicht zum Schadenersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdienstenaufsichtsgesetz nicht verlangt hat, obwohl die Bank zur starken Kundenauthentifizierung nach § 68 Absatz 4 Zahlungsdienstenaufsichtsgesetz verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, das der Teilnehmer weiß, z. B. PIN), Besitz (etwas, das der Teilnehmer besitzt, z. B. TAN-Generator) oder Inhärenz (etwas, das der Teilnehmer ist, z. B. Fingerabdruck).

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

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

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

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

- Der Kontoinhaber 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 Depotinhabers bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhend nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Zahlungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Zahlungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften der Depotinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige des Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte OnlineBanking-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.

Vorvertragliche Information (inkl. Fernabsatz) zum PSD GiroVertrag



Sehr geehrte Kundin, sehr geehrter Kunde,

bevor Sie im Fernabsatz (per Internet, Telefon, E-Mail, Telefax, oder Briefverkehr) oder außerhalb von Geschäftsräumen mit uns Verträge schließen, möchten wir Ihnen gemäß den gesetzlichen Bestimmungen einige allgemeine Informationen zur Bank, zur angebotenen Dienstleistung und zum Vertragsschluss geben:

Übersicht

- I. Allgemeine Informationen
- II. Informationen zu den einzelnen Produkten
 - a) PSD Girokonten/Basiskonto
 - b) girocard (Debitkarte)
 - c) Überziehungsmöglichkeit
 - d) PSD OnlineBanking und PSD ServiceDirekt
- III. Informationen über die Besonderheiten des Fernabsatzvertrages
- IV. Hinweis zur Verarbeitung personenbezogener Daten gemäß EU-Geldtransferverordnung

I. Allgemeine Informationen

Name und Anschrift der Bank

Name der Bank:

PSD Bank Nürnberg eG
Willy-Brandt-Platz 8
90402 Nürnberg
Telefon 0911 / 2385-0
Telefax 0911 / 2385-198
E-Mail: info@psd-nuernberg.de

Zuständige Hauptstelle:

PSD Bank Nürnberg eG
Willy-Brandt-Platz 8
90402 Nürnberg
Telefon 0911 / 2385-0
Telefax 0911 / 2385-198
E-Mail: info@psd-nuernberg.de

Gesetzlich Vertretungsberechtigte der Bank:

Vorstand:
Johann Büchler
Helmut Hollweck

Service Nummern der Bank:

Geldanlage / PrivatKredit	0800 2 385 555	Service Nummer der DTAG für den Anrufer kostenlos
Wertpapier	0800 2 385 585	Service Nummer der DTAG für den Anrufer kostenlos
Baufinanzierung	0800 2 385 544	Service Nummer der DTAG für den Anrufer kostenlos
ServiceDirekt	0800 5 888 977	Service Nummer der DTAG für den Anrufer kostenlos
Beschwerdehotline	0800 2 385 600	Service Nummer der DTAG für den Anrufer kostenlos
Kartensperre	116 116	(kostenfrei)

Name und Anschrift des für die Bank handelnden Vermittlers / Dienstleisters:

Dienstleister:
Bausparkasse Schwäbisch Hall
Crailsheimer Str. 52
74523 Schwäbisch Hall
Telefon: 0791 / 46 44-44
Telefax: 0791 / 46 44-46
E-Mail: service@schwaebisch-hall.de

R+V Allgemeine Versicherung AG
Taanusstraße 1
65193 Wiesbaden
Telefon: 0611 / 533-0
Telefax: 0611 / 533-770
E-Mail: info@ruv.de

Hauptgeschäftstätigkeit der Bank:

Gegenstand des Unternehmens ist der Betrieb von Bankgeschäften aller Art und von damit zusammenhängenden Geschäften.

Zuständige Aufsichtsbehörde:

Die für die Zulassung von Kreditinstituten zuständige Aufsichtsbehörde ist die Europäische Zentralbank, Sonnemannstraße 20, 60314 Frankfurt a. M. (Postanschrift: Europäische Zentralbank, 60640 Frankfurt a.M., Deutschland); die für den Schutz der kollektiven Verbraucherinteressen zuständige Aufsichtsbehörde ist die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Graurheindorfer Str. 108, 53117 Bonn bzw. Marie-Curie-Str. 24-28, 60439 Frankfurt a.M. (Internet: www.bafin.de)

Eintragung (der Hauptniederlassung) im Genossenschaftsregister:

Amtsgericht Nürnberg, GnR Nr. 281

Umsatzsteueridentifikationsnummer:

DE 133 546 227

Vertragsprache:

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

Rechtsordnung/Gerichtsstand:

Gemäß Nr. 6 Abs. 1 der „Allgemeinen Geschäftsbedingungen (AGB-Banken) der Bank“ gilt für den Vertragsschluss und die gesamte Geschäftsverbindung zwischen dem Kunden und der Bank deutsches Recht. Es gibt keine vertragliche Gerichtsstandsklausel.

Außergerichtliche Streitschlichtung:

Beschwerden sind an die PSD Bank Nürnberg eG, Willy-Brandt-Platz 8, 90402 Nürnberg zu richten. Darüber hinaus besteht für die Beilegung von Streitigkeiten mit der Bank die Möglichkeit, den Ombudsmann der genossenschaftlichen 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 Ihnen auf Wunsch zur Verfügung gestellt wird. Die Beschwerde ist schriftlich an die Kundenbeschwerdestelle beim Bundesverband der Deutschen Volksbanken und Raiffeisenbanken – BVR, Schellingstraße 4, 10785 Berlin, E-Mail: kundenbeschwerdestelle@bvr.de, zu richten. Schlichtungsstelle bei Streitigkeiten aus der Anwendung der Vorschriften des Bürgerlichen Gesetzbuches betreffend Fernabsatzverträge über Finanzdienstleistungen ist die Deutsche Bundesbank, Schlichtungsstelle, Postfach 11 12 32, 60047 Frankfurt a. Main, E-Mail: schlichtung@bundesbank.de. Schlichtungsstelle bei Streitigkeiten aus der Anwendung sonstiger Vorschriften im Zusammenhang mit dem Vertrag, der ein Bankgeschäft nach § 1 Abs. 1 S. 2 des Kreditwesengesetzes oder eine Finanzdienstleistung nach § 1 Abs. 1a S. 2 des Kreditwesengesetzes betrifft, ist die Bundesanstalt für Finanzdienstleistungsaufsicht, Graurheindorfer Straße 108, 53117 Bonn, E-Mail: schlichtungsstelle@bafin.de. Die Europäische Kommission stellt unter <http://ec.europa.eu/consumers/odr/> eine Plattform zur außergerichtlichen Online-Streitbeilegung (sogenannte OS-Plattform) bereit.

Hinweis zum Sicherungssystem

Die Bank ist der BVR Institutssicherung GmbH und der Sicherungseinrichtung des Bundesverbandes der Deutschen Volksbanken und Raiffeisenbanken e.V. angeschlossen (Näheres vgl. Nr. 20 der „Allgemeinen Geschäftsbedingungen“ der Bank). Diese institutsbezogenen Sicherungssysteme haben die Aufgabe, drohende oder bestehende wirtschaftliche Schwierigkeiten bei ihnen angeschlossenen Instituten abzuwenden oder zu beheben. Alle Institute, die diesen Sicherungssystemen angeschlossen sind, unterstützen sich gegenseitig, um eine Insolvenz zu vermeiden.

Gebundener Versicherungsvertreter nach §34d Abs. 7 der Gewerbeordnung

Vermittlerregisternummer: D-R3Y6-01UR4-51

Die Eintragung im Vermittlerregister kann wie folgt überprüft werden:

Deutscher Industrie- und Handelskammertag (DIHK) e.V.
Breite Straße 29, 10178 Berlin, Telefon: 0180 / 6005850 (Festnetzpreis 0,20 Euro / Anruf; Mobilfunkpreise maximal 0,60 Euro/ Anruf).
www.vermittlerregister.info

Berufsrechtliche Regelungen

- §34d Gewerbeordnung
- §§59 – 68 VVG
- Verordnung über die Versicherungsvermittlung und -beratung (VersVermV)

Die berufsrechtlichen Regelungen können über die vom Bundesministerium der Justiz und von der juris GmbH betriebenen Homepage www.gesetzte-im-internet.de eingesehen und abgerufen werden.

Außergerichtliche Schlichtungsstelle für Versicherungen:

Versicherungsombudsmann e.V., Postfach 08 06 32, 10006 Berlin
www.versicherungsombudsmann.de

Ombudsmann Private Kranken- und Pflegeversicherung

Postfach 06 02 22, 10052 Berlin
www.pkv-ombudsmann.de

II. Informationen zu den einzelnen Produkten und Dienstleistungen

a) PSD Girokonten/Basiskonto

Wesentliche Leistungsmerkmale:

Die Bank richtet für den Kunden ein Konto in laufender Rechnung (Girokonto) ein, schreibt eingehende Zahlungen auf dem Konto gut und wickelt von ihm veranlasste Zahlungsvorgänge (z.B. Überweisungen) zulasten dieses Kontos ab, soweit das Konto ausreichend Guthaben oder Kredit aufweist.

Im Einzelnen sind insbesondere folgende Dienstleistungen vom Girovertrag erfasst:

- Kontoführung,
- Bargeldein- und Bargeldauszahlungen,
- Überweisungen (vgl. hierzu im Einzelnen die ‚Sonderbedingungen für den Überweisungsverkehr‘,
- Daueraufträge,
- Lastschriftbelastungen (vgl. hierzu im Einzelnen die ‚Sonderbedingungen für den Lastschriftverkehr‘),
- Scheckinkasso,
- Eingeräumte Kontoüberziehung; ausgenommen Basiskonto,
- Geduldete Kontoüberziehung
- Scheckeinlösungen (vgl. hierzu im Einzelnen die ‚Sonderbedingungen für den Scheckverkehr‘),
- girocard (Debitkarte) zur Abhebung an in- und ausländischen Geldautomaten, zur bargeldlosen Zahlung an automatisierten Kassen im Rahmen des electronic cash-, Maestro- und V PAY-Systems und zur Nutzung der GeldKarte-Funktion (vgl. hierzu im Einzelnen die ‚Sonderbedingungen für die girocard (Debitkarte)‘).

Leistungsmerkmale für alle Girokontenmodelle:

- Kostenlos 2 girocards (Debitkarten)
- Kostenfreies PSD OnlineBanking und PSD ServiceDirekt
- 13 mal im Quartal kostenlos Bargeld an Automaten im BankCard ServiceNetz

Leistungsmerkmale und Vorbehalt je Kontomodell:

PSD GiroDirekt (mit Gehaltseingang):

- Kostenlose Kontoführung
- Zinslose Überziehungsmöglichkeit bis 500,00 Euro
- Überziehungsmöglichkeit bei Gehaltseingang
- Kostenlose MasterCard Classic (Kreditkarte)

PSD GiroSt@r:

- Kostenlose Kontoführung
- Zinsspecial
- Überziehungsmöglichkeit bei Gehaltseingang
- Nach Vollendung des 27. Lebensjahres erfolgt eine automatische Umwandlung in ein PSD GiroDirekt mit Gehaltseingang oder ein gebührenpflichtiges PSD Girokonto ohne Gehaltseingang

PSD GiroDepot

- Kostenlose Kontoführung als Abrechnungskonto bei Depot im Haus
- Bei Auflösung vom Depot wird das Abrechnungskonto aufgelöst oder ggf. in ein anderes Girokontomodell umgewandelt

PSD Girokonto/Basiskonto:

- Monatliche Grundgebühr gem. Preis- und Leistungsverzeichnis

Leistungsvorbehalt:

Hinsichtlich einzelner im Zusammenhang mit dem Konto stehender Dienstleistungen (z.B. Gutschrift bei Scheckeinlösung) gelten die Vorbehalte, wie sie mit dem Kunden über die hierfür maßgeblichen Geschäftsbedingungen und Sonderbedingungen vereinbart wurden (z.B. Vorbehalt der Einlösung und des Eingangs des Gegenwertes) oder entsprechend dem jeweiligen Kontomodell.

Zahlung und Erfüllung des Vertrages:

- Zahlung der Entgelte und eventuell anfallender Zinsen durch den Kunden
- Monatliches Kontoführungsentgelt sowie Zinsen zum Quartalsende, Dienstleistungen im Zusammenhang mit der girocard (Debitkarte), sowie weitere Entgelte entsprechend vom Kundenauftrag gemäß dem ‚Preis- und Leistungsverzeichnis‘. Die Änderung von Zinsen und Entgelten während der Laufzeit des Girovertrages erfolgt nach Maßgabe von Nr. 12 der ‚Allgemeinen Geschäftsbedingungen (AGB)‘. Eigene Kosten (z.B. für Ferngespräche, Porti) hat der Kunde selbst zu tragen.
- Kontoführung
- Die vollumfängliche Nutzung der Leistungen ist in der Regel nur bei einem PSD Gehaltsgirokonto möglich. Die Bank erfüllt ihre Verpflichtungen aus dem Girovertrag durch Verbuchung der Gutschriften und Belastungen auf Basis der zugrunde liegenden Aufträge und Weisungen (z.B. aus Überweisungen, Lastschriften, Bargeldein- und Bargeldauszahlungen, Bankentgelte) auf dem in laufender Rechnung geführten Konto. Dabei werden die jeweiligen Buchungspositionen zum Ende der vereinbarten Rechnungsperiode – in der Regel zum Ende des Kalenderquartals – miteinander verrechnet und das Ergebnis (Saldo) dem Kunden als Rechnungsabschluss mitgeteilt. Alle von der Bank vorgenommenen Buchungen werden auf dem Kontoauszug mit Angabe des Buchungsdatums, des Betrags, einer kurzen Erläuterung über die Art des Geschäftes sowie der Valuta (Wertstellung) aufgelistet. Kontoauszüge werden in der jeweils vereinbarten Form (z. B. Postversand, Kontoauszugsdrucker, elektronisches Postfach) übermittelt.
- Bargeldeinzahlungen und Zahlungseingänge
- Eingezahlte Geldbeträge und Zahlungseingänge schreibt die Bank dem Konto gut.
- Bargeldauszahlung
- Die Bank erfüllt eine Auszahlungsverpflichtung durch Bargeldauszahlung an Schalter oder an Geldautomaten.
- Überweisung
- Bei einer institutsinternen Überweisung ist diese mit Gutschrift auf dem Konto des Zahlungsempfängers und Übermittlung der Angaben zur Person des Zahlers und des angegebenen Verwendungszwecks erfüllt. Bei einer institutsübergreifenden Überweisung ist diese mit Gutschrift auf dem Konto des Kreditinstituts des Zahlungsempfängers und Übermittlung der Angaben zur Person des Zahlers und des angegebenen Verwendungszwecks erfüllt. Die weiteren Einzelheiten ergeben sich aus den ‚Sonderbedingungen für den Überweisungsverkehr‘.
- Lastschriftbelastung
- Lastschriften sind eingelöst, wenn die Belastungsbuchung nicht spätestens am zweiten Bankarbeitstag (alle Werktagen außer Sonnabende, 24. und 31. Dezember) nach ihrer Vornahme rückgängig gemacht wird (vgl. Nr. 9 Abs. 2 der ‚Allgemeinen Geschäftsbedingungen‘). Für Lastschriften aus anderen Verfahren gelten die Einlösungsregeln in den hierfür vereinbarten ‚Sonderbedingungen für den Lastschriftverkehr‘.
- Scheckinkasso
- Ist der Scheck auf ein Kreditinstitut im Inland gezogen, erfüllt die Bank ihre Verpflichtung aus dem Scheckinkasso mit Vorlage des Schecks oder dessen Daten beim bezogenen Kreditinstitut. Bei einem auf ein Kreditinstitut im Ausland gezogenen Scheck ist die Verpflichtung der Bank aus dem Scheckinkasso durch auftragsgemäße Weiterleitung des Schecks (oder der Scheckdaten) erfüllt. Vor Eingang des Scheckgegenwertes bei der Bank erfolgt die Gutschrift in der Regel nur unter dem Vorbehalt des Eingangs (vgl. Nr. 9 Abs. 1 der ‚Allgemeinen Geschäftsbedingungen‘).
- Scheckeinlösung
- Auf die Bank gezogene Schecks sind eingelöst, wenn die Belastungsbuchung nicht spätestens am zweiten Bankarbeitstag nach ihrer Vornahme rückgängig gemacht wird. Barschecks sind bereits mit Zahlung an den Scheckvorleger eingelöst. Schecks sind auch schon dann eingelöst, wenn die Bank im Einzelfall eine Bezahlungsmeldung absendet. Schecks, die über eine Abrechnungsstelle der Bundesbank vorgelegt werden, sind eingelöst, wenn sie nicht bis zu dem von der Bundesbank festgesetzten Zeitpunkt zurückgegeben werden (vgl. Nr. 9 Abs. 2 der ‚Allgemeinen Geschäftsbedingungen‘). Im Übrigen gelten die ‚Sonderbedingungen für den Scheckverkehr‘.
- Kartenzahlung mit girocard (Debitkarte)
- Vom Kunden veranlasste Kartenzahlungen erfüllt die Bank durch Zahlung an den Händler als Akzeptanten der Kartenzahlung. Die Nutzung von Zahlungskarten ist in den ‚Sonderbedingungen für die girocard (Debitkarte)‘ geregelt.

Der Girovertrag kann vom Kunden jederzeit gekündigt werden. Im Übrigen gelten die in Nr. 18 und 19 der AGB für den Kunden und die Bank festgelegten Kündigungsregeln. Es besteht keine Mindestlaufzeit.

b) Informationen zur girocard (Debitkarte)

Wesentliche Leistungsmerkmale:

Der Karteninhaber kann die girocard (Debitkarte), soweit diese entsprechend ausgestattet ist, in Verbindung mit der persönlichen Geheimzahl (PIN) u.a. zur Bargeldauszahlung mit der der Debitkarte am Geldautomaten und zum Bezahlen bei Handels- und Dienstleistungsunternehmen an automatisierten Kassen nutzen. Zu den Leistungsbedingungen im Einzelnen vergleiche die ‚Sonderbedingungen für die girocard (Debitkarte)‘.

Zahlung und Erfüllung des Vertrages:

Der Vertrag über die girocard (Debitkarte) wird seitens der Bank durch Zurverfügungstellung der Karte zu den vereinbarten Konditionen erfüllt. Die girocard (Debitkarte) kann vom Kunden jederzeit gekündigt werden. Es besteht keine Mindestlaufzeit.

c) Überziehungsmöglichkeit

Wesentliche Leistungsmerkmale:

Die Bank stellt Ihnen eine Überziehungsmöglichkeit auf Ihrem Girokonto zur Verfügung. Über die eingeräumte Kontoüberziehung können Sie frei verfügen. Die Rückführung erfolgt mittels der auf Ihrem Girokonto eingehenden Zahlungen. Die Zinsabrechnung erfolgt immer vierteljährlich im Rahmen der Kostenabrechnung für Ihr Girokonto.

Preise:

Die eingeräumte Kontoüberziehung, den hierfür geltenden Sollzinssatz und den Sollzinssatz für darüber hinausgehende geduldete Kontoüberziehungen teilt Ihnen die Bank auf dem Kontoauszug mit. Zusätzliche Preise für die Inanspruchnahme der Überziehungsmöglichkeit entstehen nicht.

Leistungsvorbehalt:

Die Überziehungsmöglichkeit kann auf Ihrem Girokonto bereitgestellt werden, wenn

- Ihre über ein Fernkommunikationsmittel gemachten Angaben mit den ggf. einzureichenden Unterlagen übereinstimmen,
- Sie eine regelmäßige Zahlung in Form von Gehalt, Rente, Pension, etc. erhalten,
- Ihre Bonität und die SCHUFA-Auskunft bzw. Auskünfte anderer Art eine Bereitstellung zulassen und
- die übrigen ggf. in einem Kreditvertrag vereinbarten Bereitstellungsvoraussetzungen vorliegen.

d) PSD OnlineBanking und PSD ServiceDirekt

Allgemeines zu PSD OnlineBanking und PSD ServiceDirekt (Telefonbanking)

Preise:

Die Teilnahme am PSD OnlineBanking bzw. PSD ServiceDirekt (Telefonbanking) ist kostenfrei. Die Kosten, die dem Kunden seitens des Internetproviders in Rechnung gestellt werden, sind vom Kunden selbst zu tragen. Für das Sm@rt-TAN-plus-Verfahren ist die Anschaffung eines kostenpflichtigen sogenannten TAN-Generators notwendig

PSD OnlineBanking

Wesentliche Leistungsmerkmale:

Auf der Grundlage einer Vereinbarung mit der Bank über die Nutzung des PSD OnlineBanking kann der Kunde Konto- und Depotabfragen tätigen bzw. Bankgeschäfte über das Internet in dem von der Bank angebotenen Umfang abwickeln. Für Depotabfragen bzw. An- und Verkäufe von Wertpapieren ist die Zusatzvereinbarung PSD Brokerage erforderlich. Voraussetzung für die Nutzung für Bank- und Depotgeschäfte ist, dass der Kunde bei der Bank ein Konto bzw. Depot unterhält. Der Nutzungsumfang des PSD OnlineBankings kann dabei auf bestimmte Geschäftsvorfälle und auf Höchstbeträge begrenzt werden. Zur Abwicklung von Bankgeschäften über PSD OnlineBanking mittels Sm@rt-TAN-Plus oder mobileTAN-Verfahren benötigen der Kontoinhaber und etwaige Bevollmächtigte jeweils eine eigene Zugangskennung (PSD Key) und eine eigene Identifikationsnummer (Online-PIN). Zur Erstellung und zum Anzeigen der individuellen, einmaligen TAN mittels Sm@rt-TAN-Plus benötigt der Kunde einen TAN-Generator und eine girocard (Debitkarte). Die Zuordnung kann durch den Kunden über die TAN-Verwaltung im Onlinebanking erfolgen. Beim mobileTAN-Verfahren (m-TAN-Verfahren) benötigt der Kunde ein Mobiltelefon eines deutschen Providers. Die Freischaltung seiner Konten muss der Kunde selbst veranlassen und seine Handynummer hinterlegen. Es kann nur eine Handynummer hinterlegt werden. Nach Eingabe seiner Transaktionsdaten erhält der Kunde eine mobile TAN mittels SMS für ausschließlich Transaktion.

Daneben gelten die ‚Sonderbedingungen für das PSD OnlineBanking‘, die ‚Sonderbedingungen für das PSD Brokerage‘ und die ‚Sonderbedingungen für die Nutzung des elektronischen Postfachs‘.

Zahlung und Erfüllung des Vertrages:

Die Bank erfüllt ihre Verpflichtungen aus der Vereinbarung über die Nutzung des PSD OnlineBanking, indem sie dem Kunden die erforderlichen Sicherungsmedien zur Verfügung stellt und den Kunden für die Nutzung des PSD OnlineBanking freischaltet. Sie wird des Weiteren die vom Kunden freigegebenen, mittels PSD OnlineBanking übermittelten Aufträge im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeiten. Ein Anspruch des Kunden darauf, dass die Bank jederzeit online erreichbar ist, besteht nicht. Die Vereinbarung über die Nutzung des PSD OnlineBanking mit dem jeweiligen Sicherungsmedium kann vom Kunden jederzeit gekündigt werden. Im Übrigen gelten die in Nr. 18 und 19 der ‚Allgemeinen Geschäftsbedingungen (AGB)‘ der Bank für die Kunden und die Bank festgelegten Kündigungsregeln. Es besteht keine Mindestlaufzeit.

Sonstige Rechte und Pflichten von Bank und Kunde:

Die Bank erwirbt als Sicherheit für ihre Forderungen ein Pfandrecht an den Wertpapieren und Sachen, an denen eine inländische Geschäftsstelle Besitz erlangt oder noch erlangen wird. Die Bank erwirbt ein Pfandrecht auch an den Ansprüchen, die dem Kunden gegen die Bank aus der bankmäßigen Geschäftsverbindung zustehen oder künftig zustehen werden. Das Pfandrecht dient der Sicherung aller bestehenden, künftigen und bedingten Ansprüche, die der Bank gegen den Kunden zustehen.

Für den gesamten Geschäftsverkehr gelten die ‚Allgemeinen Geschäftsbedingungen (AGB)‘ der Bank. Daneben gelten die Sonderbedingungen, die Abweichungen oder Ergänzungen zu diesen ‚Allgemeinen Geschäftsbedingungen (AGB)‘ enthalten:

‚Sonderbedingungen für den Überweisungsverkehr‘
‚Sonderbedingungen für den Lastschriftverkehr‘
‚Sonderbedingungen für den Scheckverkehr‘
‚Sonderbedingungen für die girocard (Debitkarte)‘
‚Sonderbedingungen für PSD OnlineBanking‘
‚Sonderbedingungen für PSD ServiceDirekt (Telefonbanking)‘
‚Sonderbedingungen für PSD Brokerage‘
‚Sonderbedingungen für das elektronische Postfach‘
‚Sonderbedingungen für den Kontoauszugsdrucker‘

Zahlung und Erfüllung des Vertrages:

Die Bank stellt Ihnen den Kreditbetrag nach Erfüllung der unter „Leistungsvorbehalt“ genannten Voraussetzungen auf Ihrem Girokonto zur Verfügung.

Vertragliche Kündigungsregeln:

Beendigung des Kreditverhältnisses durch den Kreditnehmer:

Sie können das Kreditverhältnis jederzeit beenden, indem Sie den Sollsaldo auf Ihrem Girokonto ausgleichen.

Beendigung des Kreditverhältnisses durch die Bank:

Kredite und Kreditzusagen, für die weder eine Laufzeit noch eine abweichende Kündigungsregelung vereinbart ist, kann die Bank jederzeit ohne Einhaltung einer Kündigungsfrist kündigen. Die Bank wird bei der Ausübung dieses Kündigungsrechtes auf die berechtigten Belange des Kreditnehmers Rücksicht nehmen.

Mindestlaufzeit des Vertrages:

Eine Mindestlaufzeit des Vertrages besteht nicht.

PSD ServiceDirekt (TelefonBanking)

Wesentliche Leistungsmerkmale:

Auf der Grundlage einer Vereinbarung mit der Bank über die Nutzung des PSD ServiceDirekt kann der Kunde Konto- und Depotabfragen tätigen bzw. Bankgeschäfte mit der PIN über das Telefon in dem von der Bank angebotenen Umfang abwickeln. Für An- und Verkäufe von Wertpapieren ist ein Rahmenvertrag PSD Brokerage erforderlich. Voraussetzung für die Nutzung für Bank- und Depotgeschäfte ist, dass der Kunde bei der Bank ein Konto bzw. Depot unterhält. Der Nutzungsumfang des PSD ServiceDirekt (TelefonBanking) kann dabei auf bestimmte Geschäftsvorfälle und auf Höchstbeträge begrenzt werden. Als Sicherungsmedien erhält der Kunde für die Übermittlung von Erklärungen oder Aufträgen eine persönliche Identifikationsnummer (Telefon-PIN). Daneben gelten die ‚Sonderbedingungen für das TelefonBanking (PSD ServiceDirekt)‘ und die ‚Sonderbedingungen für das PSD Brokerage‘.

Zahlung und Erfüllung des Vertrages:

Die Bank erfüllt ihre Verpflichtungen aus der Vereinbarung über die Nutzung des PSD ServiceDirekt, indem sie dem Kunden die erforderlichen Sicherungsmedien (Telefon-PIN) zur Verfügung stellt und den Kunden für die Nutzung des PSD ServiceDirekt (TelefonBanking) freischaltet. Sie wird des Weiteren die vom Kunden freigegebenen, mittels PSD ServiceDirekt übermittelten Aufträge im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeiten. Die Bank erfüllt ihre Verpflichtung zur Erreichbarkeit dadurch, dass sie zu den für das jeweilige Angebot dem Kunden mitgeteilten Zeiten grundsätzlich erreichbar ist. Ein Anspruch darauf, jederzeit telefonisch erreichbar zu sein, besteht hingegen nicht. Die Vereinbarung über die Nutzung des PSD ServiceDirekt (TelefonBanking) mit dem jeweiligen Sicherungsmedium kann vom Kunden jederzeit gekündigt werden. Im Übrigen gelten die in Nr. 18 und 19 der ‚Allgemeinen Geschäftsbedingungen (AGB-Banken)‘ der Bank für die Kunden und die Bank festgelegten Kündigungsregeln. Es besteht keine Mindestlaufzeit.

Hinweis auf vom Kunden zu zahlende Steuern und Kosten:

Soweit im Rahmen der Kontoführung Guthabenzinsen anfallen, sind diese Einkünfte steuerpflichtig. Bei Fragen sollte sich der Kunde an die für ihn zuständige Steuerbehörde oder seinen steuerlichen Berater wenden. Dies gilt insbesondere, wenn er im Ausland steuerpflichtig ist. Eigene Kosten (z. B. für Ferngespräche, Porti) hat der Kunde selbst zu tragen.

Die genannten Bedingungen stehen nur in deutscher Sprache zur Verfügung. Bei Änderungsvereinbarungen ergeben sich weiterführende Informationen auch aus der ursprünglichen Vertragsurkunde.

Allgemeine Preis und Entgelte:

Eine Übersicht der aktuellen Zinssätze der Bank und das jeweils gültige ‚Preis- und Leistungsverzeichnis‘ können in den Geschäftsräumen der Bank oder auf der Internetseite psd-nuernberg.de eingesehen werden; auf Verlangen werden sie ausgehändigt bzw. zugesandt.

Leistungsvorbehalt:

Grundsätzlich besteht kein Leistungsvorbehalt, es sei denn, dieser ist ausdrücklich vereinbart.

III. Informationen über die Besonderheiten des Fernabsatzvertrages

Information zum Zustandekommen des Vertrages:

Der Kunde gibt gegenüber der Bank ein ihm bindendes Angebot über einen von der Bank angebotenen Kommunikationsweg (z. B. über Telefon, Internet) ab, das die Bank annimmt. Ist für den Vertragsschluss die Schriftform vorgesehen, gibt der Kunde ein ihm bindendes Angebot ab, indem ein von ihm unterzeichnetes Exemplar der Bank zugeht und diese das Angebot annimmt. Durch die im Nachgang vorgenommene Übersendung der Vertragsunterlagen wird der abgeschlossene Vertrag lediglich bestätigt.

Widerrufsbelehrung bei außerhalb von Geschäftsräumen geschlossenen Verträgen und bei Fernabsatzverträgen über Finanzdienstleistungen

Widerrufsrecht:

Sie können Ihre Vertragserklärung innerhalb von 14 Tagen ohne Angabe von Gründen mittels einer eindeutigen Erklärung widerrufen. Die Frist beginnt nach Erhalt dieser Belehrung auf einem dauerhaften Datenträger, jedoch nicht vor Vertragsschluss und auch nicht vor Erfüllung unserer Informationspflichten gemäß Artikel 246b § 2 Absatz 1 in Verbindung mit § 1 Absatz 1 Nummer 7 bis 12, 15 und 19 sowie Artikel 248 § 4 Absatz 1 EGBGB.
Zur Wahrung der Widerrufsfrist genügt die rechtzeitige Absendung des Widerrufs, wenn die Erklärung auf einem dauerhaften Datenträger (z. B. Brief, Telefax, E-Mail) erfolgt. Der Widerruf ist zu richten an:

PSD Bank Nürnberg eG
Willy-Brandt-Platz 8
90402 Nürnberg
Telefax: 0911/2385-199
E-Mail: info@psd-nuernberg.de
Internet: www.psd-nuernberg.de

Widerrufsfolgen:

Im Falle eines wirksamen Widerrufs sind die beiderseits empfangenen Leistungen zurückzugewähren. Überziehen Sie Ihr Konto ohne eingeräumte Kontoüberziehung oder überschreiten Sie die Ihnen eingeräumte Kontoüberziehung, können wir von Ihnen über die Rückzahlung des Betrags der Überziehung oder Überschreitung hinaus weder Kosten noch Zinsen verlangen, wenn wir Sie nicht ordnungsgemäß über die Bedingungen und Folgen der Überziehung oder Überschreitung (z. B. anwendbarer Sollzinssatz, Kosten) informiert haben.

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

Besondere Hinweise:

Keine

Ende der Widerrufsbelehrung

IV. Hinweis zur Verarbeitung personenbezogener Daten gemäß EU-Geldtransferverordnung

Hinweis zur Verarbeitung personenbezogener Daten gemäß EU-Geldtransferverordnung

Die „VERORDNUNG (EU) 2015/847 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers“ (EU-Geldtransferverordnung) dient dem Zweck der Verhinderung, Aufdeckung und Ermittlung von Geldwäsche und Terrorismusfinanzierung bei Geldtransfers. Sie verpflichtet uns als Bank bei der Ausführung von Geldtransfers Angaben zum Auftraggeber (Zahler) und Begünstigten (Zahlungsempfänger) zu prüfen und zu übermitteln. Diese Angaben bestehen aus Name und Kundenkennung von Zahler und Zahlungsempfänger und der Adresse des Zahlers. Bei Geldtransfers innerhalb des Europäischen Wirtschaftsraums kann auf die Weiterleitung der Adresse des Zahlers zunächst verzichtet werden, jedoch kann diese Angabe vom Zahlungsdienstleister des Zahlungsempfängers gegebenenfalls angefordert werden. Bei der Angabe von Name und gegebenenfalls Adresse nutzen wir die in unseren Systemen hinterlegten Daten, um der gesetzlichen Vorgabe zu entsprechen.

Mit der Verordnung wird erreicht, dass aus den Zahlungsverkehrsdatensätzen selber immer eindeutig bestimmbar ist, wer Zahler und Zahlungsempfänger ist. Das heißt auch, dass die Bank Zahlungsdaten prüfen, Nachfragen anderer Zahlungsdienstleister zur Identität des Zahlers bzw. Zahlungsempfängers beantworten und auf Anfrage diese Daten den zuständigen Behörden zur Verfügung stellen muss.

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 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, Anschriftenermittlung, Kundenbetreuung oder Risikosteuerung sowie der Tarifierung oder Konditionierung. Über etwaige Änderungen der Zwecke der Datenverarbeitung wird die SCHUFA gemäß Artikel 14 Absatz 4 DSGVO 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 Artikel 6 Absatz 1 Buchstabe f DSGVO, 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 DSGVO 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, Insolvenzbekanntmachungen).

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 Artikel 28 DSGVO 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 wählende Speicherung erforderlich ist.

3. Betroffenenrechte

Jede betroffene Person hat gegenüber der SCHUFA das Recht auf Auskunft nach Artikel 15 DSGVO, das Recht auf Berichtigung nach Artikel 16 DSGVO, das Recht auf Löschung nach Artikel 17 DSGVO und das Recht auf Einschränkung der Verarbeitung nach Artikel 18 DSGVO. 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 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.

Nach Artikel 21 Absatz 1 DSGVO kann der Datenverarbeitung aus Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, widersprochen werden. Der Widerspruch kann formfrei erfolgen und ist zu richten an SCHUFA Holding AG, Privatkunden ServiceCenter, Postfach 10 34 41, 50474 Köln.

4. Profilbildung (Scoring)

Die SCHUFA-Auskunft kann um sogenannte Scorewerte ergänzt werden. Beim Scoring wird anhand von gesammelten Informationen und Erfahrungen aus der Vergangenheit eine Prognose über zukünftige Ereignisse erstellt. Die Berechnung aller Scorewerte erfolgt bei der SCHUFA grundsätzlich auf Basis der zu einer betroffenen Person bei der SCHUFA gespeicherten Informationen, die auch in der Auskunft nach Artikel 15 DSGVO ausgewiesen werden. Darüber hinaus berücksichtigt die SCHUFA beim Scoring die Bestimmungen § 31 BDSG. Anhand der zu einer Person gespeicherten Einträge erfolgt eine Zuordnung zu statistischen Personengruppen, die in der Vergangenheit ähnliche Einträge aufwiesen. Das verwendete Verfahren wird als „logistische Regression“ bezeichnet und ist eine fundierte, seit langem praxiserprobte, mathematisch-statistische Methode zur Prognose von Risikowahrscheinlichkeiten.

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 Zahlungsstörungen, 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 besondere Kategorien personenbezogener Daten wie ethnische Herkunft oder Angaben zu politischen oder religiösen Einstellungen nach Artikel 9 DSGVO. Auch die Geltendmachung von Rechten nach der DSGVO, also z.B. die Einsichtnahme in die bei der SCHUFA gespeicherten Informationen nach Artikel 15 DSGVO, hat keinen Einfluss auf die Scoreberechnung.

Die übermittelten Scorewerte unterstützen die Vertragspartner bei der Entscheidungsfindung und gehen dort in das Risikomanagement ein. Die Risikoeinschätzung und Beurteilung der Kreditwürdigkeit erfolgt allein durch den direkten Geschäftspartner, da nur dieser über zahlreiche zusätzliche Informationen – zum Beispiel aus einem Kreditantrag – verfügt. Dies gilt selbst dann, wenn er sich einzig auf die von der SCHUFA gelieferten Informationen und Scorewerte verlässt. Ein SCHUFA-Score alleine ist jedenfalls kein hinreichender Grund einen Vertragsabschluss abzulehnen.

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