

### Einwilligungen zur GenialCard (nachfolgend „Karte“ genannt)

Im Rahmen des Antrags willigt der Kunde in die Übermittlung oder das Einholen von Daten entsprechend den nachfolgenden Ziffern ein. Die Einwilligungen sind freiwillig und können jederzeit gegenüber der Hanseatic Bank GmbH & Co KG, Bramfelder Chaussee 101, 22177 Hamburg, einzeln widerrufen werden. Wird eine Einwilligung widerrufen, erklärt der Kunde damit zugleich die Kündigung seines Vertrags.

#### 1. Schufa-Hinweis

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

Der Kunde befreit die Hanseatic Bank insoweit auch vom Bankgeheimnis.

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

#### 2. Bankauskunft

Ich willige ein, dass die Bank erforderliche bankübliche Auskünfte bei der Bank einholt, bei der ich mein Girokonto (Referenzkonto) führe (z. B. bei einem Auftrag zur Erhöhung des Verfügungsrahmens). Diese wird zur Erteilung von Auskünften ermächtigt.

### Erläuterungen zur GenialCard (nachfolgend „Karte“ genannt)

Die Karte ist ein Zahlungsinstrument, das mit einem revolvingenden bonitätsabhängigen Kreditrahmen (nachfolgend „Verfügungsrahmen“ genannt) unterlegt ist, aber mit monatlichem Zahlungsziel auch zinsfrei nutzbar ist. Grundlage ist ein Rahmenkreditvertrag mit einem variablen Sollzinssatz zwischen Ihnen und der Hanseatic Bank. Mit der Karte können Sie bei Vertragsunternehmen des Visa-Verbundes (Akzeptanzstellen) Waren und Dienstleistungen im Handel oder im Internet bargeldlos bezahlen und an zugelassenen Geldautomaten sowie an Kassen von Kreditinstituten Bargeld beziehen. Bitte beachten Sie, dass Betreiber von Geldautomaten oder Bankfilialen eigene Gebühren erheben können. Für die Verbuchung von Kartenverfügungen sowie ggf. anfallender Entgelte und Zinsen wird ein Kartenkonto eingerichtet.

Die Rechnungsstellung erfolgt im Rahmen eines monatlichen Kontoauszuges, sofern Sie Kartenverfügungen getätigt haben oder ein Entgelt bzw. Zinsen auf dem Kartenkonto verbucht wurden. In dem Kontoauszug teilen wir Ihnen mit, wie hoch der Saldo Ihres Kartenkontos ist. Für den Ausgleich eines negativen Kartenkontosaldos können Sie die Teilzahlung nutzen, d. h., Sie zahlen monatlich einen Teilbetrag des negativen Saldos zurück, der in der Regel per Lastschrift von Ihrem Girokonto eingezogen wird. Die Höhe des gewünschten Teilbetrags ist mit der Bank zu vereinbaren und muss monatlich mindestens 3 % des negativen Kartenkontosaldos, jedoch nicht weniger als 20 €, betragen. Für jeden Tag, den Sie die Teilzahlung nutzen, fallen Zinsen an, die am Ende des Kalendermonats dem Kartenkonto belastet werden. Sie haben jederzeit das Recht zur kostenfreien vollständigen oder teilweisen Rückzahlung eines negativen Saldos auf Ihrem Kartenkonto.

Sofern Sie die Teilzahlung nicht nutzen möchten, können Sie die Vollzahlung als Rückzahlungsvariante wählen. Dann wird Ihnen monatlich der gesamte negative Kartenkontosaldo in Rechnung gestellt und in der Regel per Lastschrift von Ihrem Girokonto eingezogen. Zinsen auf den negativen Kartenkontosaldo fallen insoweit nicht an.

Sie können den Kartenvertrag innerhalb einer Frist von 14 Tagen widerrufen; Einzelheiten zu Ihrem Widerrufsrecht finden Sie im Kartenantrag und in den Europäischen Standardinformationen für Verbraucherkreidite.

Mit der Karte haben Sie flexible Möglichkeiten zur Zahlung und Finanzierung von Waren und Dienstleistungen. Bitte bedenken Sie, dass Sie mit der Nutzung der Teilzahlung monatliche Zahlungsverpflichtungen eingehen, und nehmen Sie die Teilzahlung nur insoweit in Anspruch, wie es Ihnen Ihre persönliche Einkommens- und Vermögenssituation erlaubt. Sofern Sie mit den monatlichen Zahlungsverpflichtungen in Rückstand geraten, kann dies weitere Kosten verursachen, zur Kündigung des Kartenvertrags führen und Ihre persönliche Bonität erheblich beeinträchtigen.

Ihre Hanseatic Bank

### 1. Konditionen

Jahresgebühr	
Hauptkarte	0 €
Kontoauszug und Rechnungsabschluss	
Kreditkartenabrechnung	
Standard: online in die Postbox des Online Bankings	0 €
Als Zusatzleistung nach gesonderter Vereinbarung: per Post	1,90 € pro Versand
Überweisung aus dem Verfügungsrahmen	
Standard: online durch das Online Banking	0 €
Nach gesonderter Vereinbarung: textlich oder telefonisch	3,95 €
Bargeldauszahlungen am Geldautomaten bzw. in Bankfilialen <sup>1</sup>	0 €
Entgelt für den Auslandseinsatz innerhalb des Europäischen Wirtschaftsraumes (Nicht-Euro-Umsätze) <sup>2</sup>	0 €
Entgelt für den Auslandseinsatz außerhalb des Europäischen Wirtschaftsraumes (Nicht-Euro-Umsätze) <sup>2</sup>	0 €
<sup>1</sup> Bitte beachten Sie, dass Betreiber von Geldautomaten oder Bankfilialen eigene Gebühren erheben können. <sup>2</sup> Fremdwährungen werden zu den ermittelten Wechselkursen von Visa umgerechnet. Der Abrechnungstag kann von dem Tag, an dem die Kartenverfügung getätigt wurde, abweichen, je nachdem, wann die Kartenverfügung bei der Bank eingereicht wird. Den Kurs erfahren Sie unter <a href="https://www.visa.co.uk/support/consumer/travel-support/exchange-rate-calculator.html">https://www.visa.co.uk/support/consumer/travel-support/exchange-rate-calculator.html</a>	
Finanzielle Nutzungsgrenzen (sofern Verfügungsrahmen ausreichend)	
Interneteinkäufe	3.000 € pro Tag
Sonstige Einkäufe	10.000 € pro Tag
Bargeldauszahlungen am Geldautomaten bzw. in Bankfilialen <sup>3</sup>	500 € pro Tag
<sup>3</sup> Bitte beachten Sie, dass z. B. Betreiber von Geldautomaten die Anzahl und den Betrag von Abhebungen begrenzen können.	

### 2. Zinsen

Zins bei Nutzung der Teilzahlung (veränderlich)	p.a.
Sollzinssatz	12,82 %
Effektiver Jahreszins	13,60 %

### 3. Versicherungen

Versicherung „SicherKreditkarte“	0,89 % des mtl. negativen Kartenkontosaldos
Versicherung „SicherPortemonnaie“	30 € pro Jahr

### 4. Annahme-/Ausführungsfrist

Annahmefristen	
Überweisungen vom Kartenkonto auf das Referenzkonto zur taggleichen Bearbeitung	
Per Telefon	bis 17 Uhr an Geschäftstagen
Textlich	bis 16 Uhr an Geschäftstagen
Per Online-Auftrag	bis 16 Uhr an Geschäftstagen
Ausführungsfristen	
Der Zahlungsbetrag wird beim Zahlungsdienstleister des Zahlungsempfängers spätestens wie folgt eingehen:	
Zahlungsauftrag im EWR in €	max. 1 Geschäftstag
Zahlungsauftrag im EWR in einer anderen EWR-Währung als €	max. 4 Geschäftstage
Zahlungsauftrag außerhalb des EWR unabhängig von der Währung	Zahlungsauftrag wird baldmöglichst bewirkt
Die Geschäftstage der Bank ergeben sich aus Ziffer IV. c der AGB.	

Die Bank kann für Leistungen, die nicht Gegenstand einer Vereinbarung oder im Konditionsverzeichnis aufgeführt sind und die im Auftrag des Kunden oder in dessen mutmaßlichem Interesse erbracht werden und die, nach den Umständen zu urteilen, nur gegen eine Vergütung zu erwarten sind, ein nach Maßgabe der gesetzlichen Bestimmungen angemessenes Entgelt verlangen.

Allgemeine Geschäfts- und Nutzungsbedingungen für die GenialCard (nachfolgend „Karte“ genannt) der Hanseatic Bank GmbH & Co KG (nachfolgend „Bank“ genannt)

### I. Vertragspartner

Hanseatic Bank GmbH & Co KG, Bramfelder Chaussee 101, 22177 Hamburg, info@hanseaticbank.de, Handelsregister Hamburg: HRA 68192

Zuständige Aufsichtsbehörde: Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Graurheindorfer Straße 108, 53117 Bonn, und Marie-Curie-Straße 24–28, 60439 Frankfurt am Main, www.bafin.de, sowie Europäische Zentralbank, Sonnemannstraße 20, 60314 Frankfurt am Main, www.ecb.europa.eu

### II. Allgemeines

Die Karte ist ein Zahlungsinstrument, das mit einem revolvingenden bonitätsabhängigen Kreditrahmen (nachfolgend „Verfügungsrahmen“ genannt) unterlegt, aber mit monatlichem Zahlungsziel auch zinsfrei nutzbar ist. Dem Karteninhaber wird nach Annahme des Antrags ein in laufender Rechnung geführtes Kreditkonto (nachfolgend „Kartenkonto“ genannt) eingerichtet; Einzelheiten nachstehend. Der Vertrag wird zwischen der Bank und dem Karteninhaber nach Annahme des Antrags durch die Bank geschlossen. Der verfügbare Betrag des Kartenkontos errechnet sich aus dem von der Bank mitgeteilten Verfügungsrahmen abzüglich, soweit noch nicht ausgeglichen, der vom Karteninhaber getätigten und autorisierten Kartenvorgängen sowie weiterer sonstiger Belastungen und abzüglich auf den Verfügungsrahmen anzurechnender Ratenkredite. Das Konditionsverzeichnis ist Bestandteil dieser Bedingungen. Der Vertrag berechtigt den Karteninhaber zur Nutzung seiner Karte im Rahmen dieser Bedingungen. Die Karte steht und verbleibt im Eigentum der Bank und ist nicht übertragbar. Die Abtretung der Ansprüche des Karteninhabers aus dem Vertrag, insbesondere der Ansprüche auf Auszahlung, ist ohne die schriftliche Zustimmung der Bank ausgeschlossen. Der Karteninhaber kann die Rückzahlung des offenen Saldos auch durch Inanspruchnahme des vereinbarten Verfügungsrahmens in monatlichen Teilzahlungen erbringen, Einzelheiten hierzu unter dem Abschnitt Krediträumung.

### III. Nutzung und Verwendung der Karte/Kartenkonto mit Verfügungsrahmen

#### a) Verwendungsmöglichkeiten

Die Karte ist eine von der Bank herausgegebene Kreditkarte mit verbundenem Verfügungsrahmen, mit der der Karteninhaber bei Vertragsunternehmen des Visa-Verbundes Waren und Dienstleistungen bargeldlos bezahlen und an zugelassenen Geldautomaten sowie an Kassen von Kreditinstituten Bargeld beziehen kann. Für die Nutzung an Geldautomaten und an Zahlungsterminals wird zusätzlich zur Kreditkarte eine persönliche Geheimzahl (PIN) als personalisiertes Sicherheitsmerkmal zur Verfügung gestellt. Beim Karteneinsatz an automatisierten Kassen kann zur kontaktlosen Bezahlung von Kleinbeträgen von der Anforderung eines vereinbarten Authentifizierungselements (z. B. PIN oder Unterschrift) abgesehen werden. Hierbei ist die Kreditkarte mit Kontaktfunktion an ein Kartenlesegerät zu halten. Die Karte kann auch als virtuelle Kreditkarte zum mobilen Bezahlen (z. B. mit einem Smartphone) eingesetzt werden. Die Kreditkarte wird für den privaten Gebrauch einer natürlichen Person ausgestellt und darf nicht zu gewerblichen Zwecken verwendet werden.

#### b) Kartenkonto / Abrechnung

Die Kartenvorgänge werden dem Kartenkonto belastet. Eine Übersicht über die Buchungen auf dem Kartenkonto erhält der Karteninhaber einmal monatlich mit einem Kontoauszug mit Rechnungsabschluss.

#### c) Verfügungsrahmen

Die Nutzung der Karte ist lediglich im Rahmen der Einkommens- und Vermögensverhältnisse des Karteninhabers sowie innerhalb des Verfügungsrahmens gestattet. Grundsätzlich kann die Bank jederzeit in angemessenem Rahmen die Offenlegung der wirtschaftlichen Verhältnisse des Karteninhabers anhand von Selbstauskünften und aktuellen Vermögensnachweisen verlangen. Die Bank ist bei Nichteinhaltung des Verfügungsrahmens berechtigt, den sofortigen Ausgleich der Forderungen zu verlangen. Eine eventuelle Genehmigung einzelner Kartenvorgänge führt nicht zu einer Erhöhung des eingeräumten Verfügungsrahmens. Der Karteninhaber hat Überschreitungen des Verfügungsrahmens unverzüglich auszugleichen. Die Bank ist berechtigt, bei Vorliegen eines wichtigen Grundes, den Verfügungsrahmen einseitig zu reduzieren und weitere Kartenvorgänge abzulehnen. Der Verfügungsrahmen kann schrittweise, maximal bis zu einer Höhe von 10.000 €, erhöht werden. Die Erhöhung oder Reduzierung des Verfügungsrahmens wird die Bank dem Karteninhaber mindestens in Textform mitteilen.

#### d) Ablehnung von Zahlungsaufträgen durch die Bank

Die Bank ist berechtigt, eine Kartenvorgang abzulehnen, wenn der mitgeteilte Verfügungsrahmen überschritten wird, die Nutzungsgrenzen der Karte (z. B. Bargeldverfügungsgrenzen) nicht eingehalten werden, die Karte gesperrt ist, bei Einsatz der Karte der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der Karte besteht, der Karteninhaber sich nicht mit den angeforderten und für die Transaktion erforderlichen Authentifizierungselementen legitimiert hat, oder der Karteninhaber die Verfügung nicht entsprechend dieser Bedingungen autorisiert hat. Hierüber wird der Karteninhaber während des Bezahlvorgangs bzw. über das Terminal, an dem die Kreditkarte eingesetzt wird, soweit möglich unter Angabe der Gründe und der Möglichkeiten, den Fehler zu vermeiden, unterrichtet.

#### e) Reservierung eines verfügbaren Geldbetrages

Die Bank ist berechtigt, auf dem Konto des Karteninhabers einen im Rahmen der finanziellen Nutzungsgrenzen verfügbaren Geldbetrag zu reservieren, wenn

- der Zahlungsvorgang vom Zahlungsempfänger ausgelöst worden ist und
- der Karteninhaber auch der genauen Höhe des zu reservierenden Geldbetrags zugestimmt hat.

Den reservierten Geldbetrag gibt die Bank unbeschadet sonstiger gesetzlicher oder vertraglicher Rechte unverzüglich frei, nachdem ihr der genaue Zahlungsbetrag mitgeteilt worden oder der Zahlungsauftrag zugegangen ist.

#### f) Nutzungsgrenzen

Die Verwendungsmöglichkeiten mit der Karte unterliegen aus Sicherheitsgründen täglichen Nutzungsgrenzen. Diese sind im Konditionsverzeichnis aufgeführt.

### IV. Autorisierung von Zahlungsaufträgen, Reklamationen und Beanstandungen, Ausführungsfrist

#### a) Autorisierung von Zahlungsaufträgen

Bei der Nutzung der Karte bei Vertragsunternehmen des Visa-Verbundes ist zusätzlich zur Vorlage der Karte gegebenenfalls entweder einen Beleg zu unterzeichnen, auf den das Vertragsunternehmen die Kartendaten übertragen hat, die PIN einzugeben oder eine sonstige Authentifizierung (Identitätsprüfung) durch ein Authentifizierungselement erforderlich.

Ein Authentifizierungselement ist:

- ein Element aus der Kategorie Wissen, welches nur dem Karteninhaber bekannt ist (z. B. PIN oder Passwort),
- ein Element aus der Kategorie Besitz als ein Gegenstand, den nur der Karteninhaber besitzt (z. B. ein mobiles Endgerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern TAN) oder
- ein Element aus der Kategorie Inhärenz als ein nur dem Karteninhaber innewohnendes persönliches Merkmal (z. B. Fingerabdruck).

Im Falle der kontaktlosen Nutzung an automatisierten Kassen ist die Karte zur Autorisierung der Zahlung an ein geeignetes Lesegerät zu halten. Der kontaktlose Einsatz kann im Rahmen der festgelegten Betrags- und Nutzungsgrenzen ohne Einsatz der PIN oder eines sonstigen Authentifizierungselements erfolgen, soweit dies an den Terminals für den jeweiligen kontaktlosen Einsatz nicht verlangt wird. Bei Einsatz der Karte im Internet zur Autorisierung von Online-Bezahlvorgängen erfolgt die Authentifizierung des Karteninhabers, indem er auf Aufforderung die gesondert vereinbarten und der Bank aufgrund der Geschäftsbeziehung bekannten Authentifizierungselemente einsetzt. Mit dem Einsatz der Karte erteilt der Karteninhaber die Zustimmung (Autorisierung) zur Ausführung der Kartenvorgänge. Soweit dafür zusätzlich eine PIN, die Unterschrift oder ein sonstiges Authentifizierungselement erforderlich ist, wird die Zustimmung erst mit deren Einsatz erteilt. Nach der Erteilung der Zustimmung kann der Karteninhaber die Kartenvorgänge nicht mehr widerrufen. Die Ausführung des Zahlungsauftrags durch die Bank erfolgt auf der Grundlage der durch die Kartennutzung elektronisch übermittelten Informationen. In dieser Autorisierung ist zugleich die ausdrückliche Zustimmung enthalten, dass die Bank die für die Ausführung der Kartenzahlung notwendigen personenbezogenen Daten des Karteninhabers verarbeitet, übermittelt und speichert.

#### b) Reklamationen / Beanstandungen

Reklamationen oder Beanstandungen aus dem Vertragsverhältnis zwischen dem Karteninhaber und dem Vertragsunternehmen des Visa-Verbundes sind unmittelbar zwischen diesen zu klären; sie berühren nicht die Zahlungsverpflichtung des Karteninhabers gegenüber der Bank.

#### c) Ausführungsfrist

Der Zahlungsauftrag des Karteninhabers wird wirksam, wenn er der Bank zugeht. Sofern der Zeitpunkt des Zugangs nicht auf einen Geschäftstag der Bank fällt, gilt der Zahlungsauftrag als am nächsten Tag zugegangen. Ein Zahlungsauftrag, der nach 16 Uhr bei der Bank eingeht, gilt als am darauffolgenden Geschäftstag zugegangen. Die Bank stellt sicher, dass nach Zugang des Zahlungsauftrags der Zahlungsbetrag innerhalb eines Geschäftstages beim Zahlungsempfänger eingeht, sofern der Zahlungsauftrag in Euro zu erfüllen ist und die Bank des Zahlungsempfängers ihren Sitz innerhalb des Europäischen Wirtschaftsraums hat. Bei Zahlungsvorgängen innerhalb des Europäischen Wirtschaftsraums, die nicht in Euro erfolgen, gilt eine Frist von vier Geschäftstagen. Die genannten Fristen gelten nicht für die Erbringung von Zahlungen in der Währung eines Staates außerhalb des Europäischen Wirtschaftsraums oder sofern die Bank des Zahlungsempfängers ihren Sitz außerhalb des Europäischen Wirtschaftsraums hat. Geschäftstag ist jeder Tag, an dem die Ausführung eines Zahlungsvorgangs beteiligten Zahlungsdienstleister den für die Ausführung von Zahlungsvorgängen erforderlichen Geschäftsbetrieb unterhalten. Die Bank unterhält den für die Ausführung von Zahlungsvorgängen erforderlichen Geschäftsbetrieb an allen Werktagen eines Kalenderjahres bis auf samstags und den 24. Dezember sowie den 31. Dezember.

#### d) Das Kartenkonto ist kein Zahlungsverkehrskonto.

### V. Entgelte, Zinsen und Wechselkurse

#### a) Entgelte und Zinsen

Die vom Karteninhaber geschuldeten Entgelte für die im Zusammenhang mit dem Vertrag von der Bank erbrachten Leistungen ergeben sich aus dem zum Zeitpunkt der Inanspruchnahme gültigen Konditionsverzeichnis. Für die Inanspruchnahme der Teilzahlung fallen die vereinbarten Zinsen an. Die Zinsen werden taggenau errechnet und monatlich dem Kartenkonto belastet sowie im Kontoauszug ausgewiesen.

#### b) Wechselkurse

Kartenvorgänge, die nicht in Euro erfolgen, werden zu den von Visa täglich festgesetzten Wechselkursen umgerechnet. Die Bank wird den Fremdwährungsumsatz, den Euro-Betrag und den sich daraus ergebenden Kurs auf dem Kontoauszug mitteilen. Die Umrechnung in Euro erfolgt an dem Tag, an dem die Belastung der Kartenvorgänge bei Visa eingereicht wurde. Dieser Tag kann gegebenenfalls von dem Tag abweichen, an dem die Kartenvorgänge durch den Karteninhaber getätigt wurde. Der im Kontoauszug mitgeteilte Kurs stellt den Referenzwechsellkurs dar. Änderungen dieses von Visa festgesetzten Wechselkurses werden unmittelbar und ohne vorherige Benachrichtigung wirksam.

### VI. Sicherheit der Karte / Sorgfaltspflichten, Abhilfemaßnahmen, Haftung, Berichtigungs- und Erstattungsansprüche

#### a) Sorgfaltspflichten

i) Der Karteninhaber hat mit der ihm zur Verfügung gestellten Karte sorgfältig umzugehen. Er hat die Karte unverzüglich nach Erhalt zu unterzeichnen. Zusätzlich ist er verpflichtet, alle zumutbaren Vorkehrungen zu treffen, um die Karte oder die PIN vor unbefugtem Zugriff zu schützen. Der Karteninhaber muss die PIN jedem Dritten gegenüber geheim halten. Die PIN darf nicht zusammen mit der Karte aufbewahrt oder darauf

notiert und auch nicht in sonstiger Weise gespeichert werden, auch nicht in verschlüsselter Form. Die Karte darf insbesondere nicht unbeaufsichtigt im Kraftfahrzeug aufbewahrt werden.

Jede Person, die im Besitz der Karte und / oder der PIN ist, hat die Möglichkeit, missbräuchliche Verfügungen (z. B. Geld an Automaten abzuheben) zu tätigen.

ii) Der Karteninhaber hat alle zumutbaren Vorkehrungen zu treffen, um seine mit der Bank vereinbarten Authentifizierungselemente für Online-Bezahlvorgänge vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass die Authentifizierungselemente für Online-Bezahlvorgänge missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt werden. Zum Schutz der einzelnen Authentifizierungselemente für Online-Bezahlvorgänge hat der Karteninhaber vor allem Folgendes zu beachten:

- Authentifizierungselemente aus dem Bereich Wissen (z. B. Online-Banking-Passwort) sind geheim zu halten und dürfen nicht mündlich, in Textform (z. B. E-Mail) oder auf sonstige Weise weitergegeben oder ungesichert elektronisch gespeichert (zum Beispiel Speicherung des Online-Passworts im Klartext im mobilen Endgerät) werden sowie nicht auf dem Gerät notiert oder als Abschrift zusammen mit dem Gerät, welches zum Nachweis des Authentifizierungselementes aus dem Bereich Besitz (zum Beispiel mobiles Endgerät) oder zur Prüfung des Elements aus dem Bereich Inhärenz (z.B. mobiles Endgerät mit Anwendung für Kreditkartenzahlung und Fingerabdrucksensor) dient, aufbewahrt werden.
- Authentifizierungselemente aus dem Bereich Besitz (z. B. mobiles Endgerät) sind vor dem unbefugten Zugriff Dritter sicher zu verwahren. Insbesondere ist sicherzustellen, dass unberechtigte Personen nicht auf das mobile Endgerät (z. B. Mobiltelefon) zugreifen können sowie dass mit dem mobilen Endgerät empfangene Benachrichtigungen nicht mündlich oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden dürfen.

Weiterhin

- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindlichen Anwendungen für Kreditkartenzahlungen (z. B. Karten-App, Authentifizierungs-App) nicht nutzen können
- ist die Anwendung für Online-Bezahlvorgänge (z.B. Karten-App, Authentifizierungs-App) auf dem mobilen Endgerät des Karteninhabers zu deaktivieren, bevor der Karteninhaber den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons) und
- dürfen die Nachweise des Besitzelements (z. B. TAN, Code) nicht außerhalb der Online-Bezahlvorgänge mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden
- Authentifizierungselemente aus dem Bereich Inhärenz (z. B. der Fingerabdruck des Karteninhabers) dürfen auf einem mobilen Endgerät des Karteninhabers für Online-Bezahlvorgänge nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Authentifizierungselemente aus dem Bereich Inhärenz anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für Online-Bezahlvorgänge genutzt wird, Authentifizierungselemente aus dem Bereich Inhärenz anderer Personen gespeichert, ist für Online-Bezahlvorgänge das von der Bank ausgegebene Wissensselement (z.B. Online-Passwort) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Authentifizierungselement aus dem Bereich Inhärenz.

Der Karteninhaber muss die im Verkehr erforderliche Sorgfalt bei Online-Bezahlvorgängen beachten und insbesondere angemessene Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem) treffen. Soweit dem Karteninhaber Daten aus seinem Online-Bezahlvorgang (z. B. Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät (z. B. Mobiltelefon oder App) zur Bestätigung angezeigt werden, ist der Karteninhaber verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen. Bei Abweichungen hat der Karteninhaber die Transaktion abzubrechen. Für den Fall, dass die Bank ein gesichertes Authentifizierungsverfahren (z. B. Visa Secure) anbietet und dieses von dem Vertragsunternehmen des Visa-Verbundes unterstützt wird, ist es vom Karteninhaber zu nutzen.

iii) Der Karteninhaber hat der Bank den Verlust, den Diebstahl, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung der Karte, der PIN oder eines sonstigen Authentifizierungselementes oder über einen entsprechenden Verdacht unverzüglich zu unterrichten, nachdem er davon Kenntnis erlangt hat. Die aktuelle Rufnummer der Bank ist auf der Rückseite der Karte vermerkt und im Internet unter [www.hanseaticbank.de](http://www.hanseaticbank.de) einsehbar.

b) Sperre der Karte durch die Bank

Die Bank kann die Karte sperren und die Einziehung der Karte (z. B. an Geldautomaten) veranlassen, wenn sie berechtigt ist, den Vertrag aus wichtigem Grund zu kündigen, wenn sachliche Gründe im Zusammenhang mit der Sicherheit der Karte dies rechtfertigen, der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der Karte besteht oder sich der Bank ein wesentlich erhöhtes Risiko darstellt, dass der Karteninhaber seiner Zahlungspflicht nicht nachkommen kann. Die Bank behält sich eine vorläufige Sperre bei Zahlungsverzug des Karteninhabers vor. Die Bank wird den Karteninhaber über die Sperrung oder Einziehung der Karte unter Angabe der hierfür maßgeblichen Gründe (soweit gesetzlich zulässig) möglichst vor, spätestens jedoch unverzüglich nach der Sperrung oder Einziehung mindestens in Textform unterrichten. Die Bank wird die Karte entsperren oder durch eine neue Karte ersetzen, wenn die Gründe für die Sperre nicht mehr gegeben sind und hierüber den Karteninhaber unverzüglich unterrichten.

c) Haftung für nicht autorisierte Kartenverfügungen

Beruhet ein nicht autorisierter Zahlungsvorgang darauf, dass die Kreditkarte oder die PIN oder sonstige für Online-Bezahlvorgänge vereinbarte Authentifizierungselemente verloren gegangen oder abhandengekommen sind, gestohlen oder in sonstiger Weise missbräuchlich genutzt wurden, haftet der Karteninhaber grundsätzlich nicht für Schäden, die bis zum Zeitpunkt der Sperranzeige verursacht werden. Der Karteninhaber haftet in vollem Umfang, wenn er in betrügerischer Absicht gehandelt hat oder den Schaden durch vorsätzliche oder grob fahrlässige Verletzung seiner ihm nach diesen Bedingungen obliegenden Sorgfaltspflichten herbeigeführt hat. Grobe Fahrlässigkeit kann insbesondere vorliegen, wenn der Karteninhaber

- die PIN oder das vereinbarte Authentifizierungselement aus dem Bereich Wissen (z. B. Online-Banking-Passwort) auf der Kreditkarte vermerkt oder zusammen mit der Kreditkarte aufbewahrt hat (z. B. im Brief, in welchem sie dem Karteninhaber mitgeteilt wurde).
- den Verlust oder den Diebstahl der Kreditkarte oder die missbräuchliche Verwendung der Bank schuldhaft nicht unverzüglich mitgeteilt hat, nachdem er hiervon Kenntnis erlangt hat.
- die PIN oder das vereinbarte Authentifizierungselement aus dem Bereich Wissen Dritten mitgeteilt hat und der Missbrauch darauf basiert.

Sofern die Bank bei Online Bezahlvorgängen eine starke Kundenauthentifizierung nicht verlangt oder der Zahlungsempfänger oder sein Zahlungsdienstleister eine starke Kundenauthentifizierung nicht akzeptiert, haftet der Karteninhaber nicht. Der Karteninhaber haftet jedoch in vollem Umfang, wenn er in betrügerischer Absicht gehandelt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, das der Karteninhaber weiß, z. B. PIN), Besitz (etwas, das der Karteninhaber besitzt, z. B. Kreditkarte) oder Inhärenz (etwas, das der

Karteninhaber ist, z. B. Fingerabdruck). Sobald der Verlust oder Diebstahl, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von Karte und/oder PIN oder eines sonstigen Authentifizierungselementes der Bank gegenüber angezeigt wurde (Sperranzeige), haftet der Karteninhaber für alle danach durch Zahlungsvorgänge entstehende Schäden nicht, es sei denn, er handelt in betrügerischer Absicht. Der Karteninhaber haftet nicht für Schäden, wenn der Karteninhaber die Sperranzeige nicht gegenüber der Bank abgeben konnte, weil die Bank die Möglichkeit die Sperranzeige vorzunehmen nicht durch geeignete Mittel sichergestellt hat. Dies gilt nicht, wenn der Karteninhaber in betrügerischer Absicht gehandelt hat.

d) Erstattung bei nicht autorisierter Kartenverfügung

Für den Fall eines nicht autorisierten Zahlungsvorgangs hat die Bank keinen Anspruch auf Erstattung ihrer Aufwendungen. Die Bank ist verpflichtet, dem Karteninhaber den Zahlungsbetrag unverzüglich zu erstatten und, sofern der Betrag dem Kartenkonto belastet worden ist, dieses Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung durch den nicht autorisierten Zahlungsvorgang befunden hätte. Diese Verpflichtung ist unverzüglich, spätestens jedoch bis zum Ende des Geschäftstags zu erfüllen, der auf den Tag folgt, an welchem der Bank angezeigt wurde, dass der Zahlungsvorgang nicht autorisiert ist, oder die Bank auf andere Weise davon Kenntnis erhalten hat. Hat die Bank einer zuständigen Behörde berechnete Gründe für den Verdacht, dass ein betrügerisches Verhalten des Zahlers vorliegt, schriftlich mitgeteilt, hat die Bank die Verpflichtung zur Erstattung unverzüglich zu prüfen und zu erfüllen, wenn sich der Betrugsverdacht nicht bestätigt.

e) Ansprüche bei nicht erfolgter, fehlerhafter oder verspäteter Ausführung einer autorisierten Kartenverfügung

Im Falle einer nicht erfolgten oder fehlerhaften Ausführung einer autorisierten Kartenverfügung kann der Karteninhaber von der Bank die unverzügliche und ungekürzte Erstattung des Verfügungsbetrags insoweit verlangen, als die Kartenverfügung nicht erfolgte oder fehlerhaft war. Wurde der Betrag einem Konto belastet, bringt die Bank dieses wieder auf den Stand, auf dem es sich ohne die nicht erfolgte oder fehlerhafte Kartenverfügung befunden hätte. Der Karteninhaber kann darüber hinaus die Erstattung der Entgelte und Zinsen insoweit verlangen, als ihm diese im Zusammenhang mit der nicht erfolgten oder fehlerhaften Ausführung der autorisierten Kartenverfügung in Rechnung gestellt oder seinem Konto belastet wurde. Geht der Zahlungsvorgang, den der Karteninhaber ausgelöst hat, beim Zahlungsdienstleister des Zahlungsempfängers erst nach Ablauf der Ausführungsfrist ein (Verspätung), kann der Karteninhaber von der Bank verlangen, dass diese den Zahlungsdienstleister des Empfängers darauf in Anspruch nimmt, dass dieser die Gutschrift auf dem Zahlungskonto des Empfängers so vornimmt, als sei der Zahlungsvorgang ordnungsgemäß ausgeführt worden. Der Karteninhaber kann im Falle eines nicht oder fehlerhaft ausgeführten autorisierten Zahlungsvorgangs verlangen, dass die Bank den Zahlungsvorgang nachvollzieht und den Karteninhaber über das Ergebnis unterrichtet. Die Haftung der Bank ist ausgeschlossen, wenn im Falle einer nicht erfolgten oder fehlerhaften Ausführung des Zahlungsvorgangs durch die Bank nachgewiesen wird, dass der Betrag ungekürzt eingegangen ist oder, im Falle einer Verspätung durch die Bank, nachgewiesen wird, dass der Betrag rechtzeitig eingegangen ist. Für den Fall, dass ein Zahlungsvorgang mit einer vom Karteninhaber angegebenen fehlerhaften Kundenkennung ausgeführt wurde, ist die Haftung der Bank ebenfalls ausgeschlossen. Der Karteninhaber kann in diesem Fall jedoch verlangen, dass sich die Bank im Rahmen der eigenen Möglichkeiten darum bemüht, den Zahlungsbetrag wieder zu erlangen. Ist dies nicht möglich, teilt die Bank auf Antrag des Karteninhabers alle verfügbaren Informationen mit, damit der Karteninhaber einen Anspruch auf Erstattung geltend machen kann. Im Falle einer nicht erfolgten oder fehlerhaften oder verspäteten Ausführung eines autorisierten Zahlungsvorgangs ist die Haftung der Bank – unabhängig von dem möglicherweise bestehenden gesetzlichen Erstattungsanspruch – für den über den Erstattungsanspruch hinausgehenden Schaden auf 12.500 € begrenzt, sofern die Bank überhaupt ein Verschulden trifft. Diese Haftungsbegrenzung gilt nicht bei Vorsatz und grober Fahrlässigkeit, für den Zinsschaden und für Gefahren, die die Bank besonders übernommen hat.

f) Frist für die Geltendmachung von Ansprüchen

Der Karteninhaber hat die Bank unverzüglich zu unterrichten, falls er feststellt, dass eine Kartenverfügung nicht autorisiert war oder fehlerhaft ausgeführt worden ist. Ein Erstattungsanspruch ist ausgeschlossen, wenn er nicht innerhalb von 13 Monaten ab dem Tag der Belastung des betreffenden Zahlungsvorgangs auf dem Kartenkonto gegenüber der Bank angezeigt wird. Für andere Ansprüche als die aus §§ 675u und 675y BGB wegen eines nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorgangs kann der Karteninhaber den Anspruch auch nach Ablauf der Frist geltend machen, wenn er ohne Verschulden an der Einhaltung der Frist verhindert war. Der Lauf der Frist beginnt nur, wenn die Bank den Karteninhaber entsprechend den vereinbarten Bedingungen über die aus der Kartenverfügung resultierende Belastungsbuchung mit dem monatlichen Abschluss (Kontoauszug) auf dem vereinbarten Weg unterrichtet hat, anderenfalls ist für den Fristbeginn der Tag der Unterrichtung maßgeblich.

g) Erstattungsanspruch bei einem vom oder über den Zahlungsempfänger ausgelösten autorisierten Zahlungsvorgang

Der Karteninhaber hat gegenüber der Bank einen Anspruch auf Erstattung einer Belastung des Kartenkontos, die auf einem autorisierten, vom oder über den Zahlungsempfänger ausgelösten Zahlungsvorgang beruht, wenn bei der Autorisierung der genaue Betrag nicht angegeben wurde und der Zahlungsbetrag den Betrag übersteigt, den der Karteninhaber entsprechend seinem bisherigen Ausgabeverhalten, den Bedingungen des Vertrags und den jeweiligen Umständen des Einzelfalls hätte erwarten können. Mit einem etwaigen Währungsumtausch zusammenhängende Gründe bleiben außer Betracht, wenn der zwischen den Parteien vereinbarte Referenzwechsellkurs zugrunde gelegt wurde. Der Karteninhaber ist verpflichtet, der Bank die Sachumstände darzulegen, aus denen er seinen Erstattungsanspruch herleitet. Der Anspruch auf Erstattung ist ausgeschlossen, wenn der Karteninhaber ihn nicht innerhalb von acht Wochen ab dem Tag der Belastung auf dem Kartenkonto gegenüber der Bank geltend macht.

## VII. Krediteinräumung für den Karteninhaber

a) Rückzahlungsmodalitäten – Teilzahlung/Vollzahlung

Der Karteninhaber kann gegenüber der Bank im Antrag oder später (fern-)mündlich oder mindestens in Textform bestimmen, dass er seine Zahlungsverpflichtungen aus dem Vertrag gegenüber der Bank durch Inanspruchnahme eines zinspflichtigen Kredits erfüllt und diesen in monatlichen Raten zurückzahlt (Teilzahlung). Die Bank gewährt dem Karteninhaber hierfür einen Kredit bis zur Höhe des mitgeteilten Verfügungsrahmens auf unbestimmte Zeit zu den im Antrag genannten und ggf. in der Folgezeit angepassten Konditionen, insbesondere Sollzinssätzen. Der Karteninhaber ist als Kreditnehmer verpflichtet, den gewährten Kredit monatlich mindestens in Höhe von 3 % des negativen Kartenkontosaldo, jedoch nicht weniger als 20 € (Mindestbetrag) zurückzuzahlen. Das Recht zur jederzeitigen kostenfreien vollständigen oder teilweisen Rückzahlung des Kredits bleibt davon unberührt. Alternativ kann der Karteninhaber auch bestimmen, dass er seinen Zahlungsverpflichtungen gegenüber der Bank einmal im Monat durch Zahlung des gesamten negativen Kartenkontosaldo nachkommt (Vollzahlung). Die Verpflichtung zur Teil- oder Vollzahlung entsteht, wenn zum Ende einer monatlichen Abrechnungsperiode ein negativer Saldo auf dem Kartenkonto entsteht, den die Bank dem Karteninhaber per Kontoauszug mitteilt.

**b) Rückzahlungsmodalitäten – Zinsberechnung**

Den Wechsel von der Vollzahlung zur Teilzahlung oder umgekehrt kann der Karteninhaber der Bank (fern-) mündlich oder mindestens in Textform mitteilen. Die Bank behält sich in Zweifelsfällen vor, einen entsprechenden Auftrag durch Nachfrage beim Karteninhaber auf Echtheit und inhaltliche Klarheit zu überprüfen. Weiterhin behält die Bank sich vor, einen Wechselauftrag aus organisatorischen Gründen erst binnen weniger Arbeitstage nach Eingang umzusetzen. Das Datum der Umsetzung teilt die Bank dem Karteninhaber per Kontoauszug mit. Ab Datum der Umsetzung des Wechsels gilt Folgendes: Beim Wechsel von Vollzahlung auf Teilzahlung wird ein am Tag der Umsetzung aufgelaufener negativer Kartenskontoausgang zu den Konditionen des Verfügungsrahmens verzinst. Beim Wechsel von Teilzahlung auf Vollzahlung wird ein bis dahin bestehender negativer Kartenskontoausgang bis zum Tag der Umsetzung verzinst. Die Verzinsung endet am Tag der Umsetzung, wobei die bis dahin etwa aufgelaufenen Kreditzinsen den Saldo entsprechend erhöhen und mit der nächsten Zahlungsfälligkeit zu begleichen sind. Die Zinsen werden ab dem Tag der ersten Inanspruchnahme des Kredits auf den jeweiligen negativen Kartenskontoausgang berechnet, jedoch erst ab dem Tag, an dem der Karteninhaber mit der Bank die Teilzahlung vereinbart hat. Die Berechnung der Zinsen endet mit dem Tag, an dem der negative Kartenskontoausgang vollständig ausgeglichen wurde oder der Karteninhaber mit der Bank die Vollzahlung vereinbart hat.

**c) Zahlungswege und Zahlungstermin – SEPA-Lastschriftverfahren**

Die Bank wird, sofern der Karteninhaber sein Kreditinstitut angewiesen hat, die fälligen Zahlungen im SEPA-Lastschriftverfahren zulasten des Referenzkontos von der Hanseatic Bank GmbH & Co KG einziehen zu lassen, von diesem Recht Gebrauch machen, solange der Einzug der fälligen Zahlungen ungestört verläuft und das Mandat nicht widerrufen wird. Die Frist für Vorankündigungen von Lastschriftverfahren beträgt mindestens einen Tag vor Einzug vom Referenzkonto. Die Vorankündigung ergeht regelmäßig durch die Kontoauszüge. Die Vorankündigung für den vertragsmäßigen Ratenanzug – falls vereinbart – ergibt sich aus den im Kreditantrag genannten Konditionen, insbesondere zur Ratenhöhe und zu den Fälligkeiten. Innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, kann der Karteninhaber die Erstattung des belasteten Betrages verlangen. Die Bank ist zum Einzug aber nicht verpflichtet, wenn dieser wenigstens einmal aus Gründen gescheitert ist, die nicht von der Bank, sondern vom Karteninhaber zu vertreten sind. Wenn die Bank auf den Einzug der fälligen Zahlungen aus diesen Gründen verzichtet, wird sie es dem Karteninhaber unverzüglich, mindestens in Textform, mitteilen. Die fälligen Zahlungen bleiben geschuldet. Nimmt der Karteninhaber nicht am Lastschriftverfahren teil, sind die fälligen Zahlungen spätestens bis zum 10. des dem Abrechnungsmonat folgenden Monats per Überweisung auf das Kartenkonto auszugleichen. Scheckzahlungen oder Rückzahlungen in bar sind nicht möglich.

**d) Zinsanpassung**

Der Zinssatz für die Inanspruchnahme des Kredits ist variabel. Die Zinsberechnung erfolgt nach der Formel 13,70 % pro Jahr plus aktueller Basiszinssatz (§ 247 BGB). Der Basiszinssatz kann sich gemäß den gesetzlichen Vorgaben jeweils zum 01.01. und zum 01.07. eines jeden Kalenderjahres ändern. Sollte eine Veränderung des Basiszinssatzes veröffentlicht werden, wird die Hanseatic Bank den Vertragszinssatz zum Ende der nächsten Abrechnungsperiode in dem auf die Veränderung folgenden Kalendermonat anpassen. Somit werden die Änderungen in den Monaten Februar bzw. August wirksam. Vor Änderung des Zinssatzes wird die Hanseatic Bank den Kreditnehmer darüber informieren. Der angepasste Zinssatz wird zum Zeitpunkt des Wirksamwerdens gültiger Bestandteil dieser Vereinbarung.

**e) Vereinbarung eines befristeten Darlehens (Ratenkredit)**

Neben dem oben beschriebenen Verfügungsrahmen kann die Bank dem Karteninhaber auch ein befristetes Darlehen mit fester Laufzeit, Ratenhöhe und besonderen Konditionen (fester Zinssatz) anbieten.

Dies setzt eine gesonderte Vereinbarung voraus. Im Falle der Gewährung reduziert die gewährte Darlehenssumme den verfügbaren Betrag entsprechend, während Rückzahlungen den verfügbaren Betrag entsprechend freigeben.

**VIII. Kreditsicherheit, Lohn- und Gehaltsabtretung**

Der Karteninhaber tritt der Bank den pfändbaren Teil seiner gegenwärtigen und zukünftigen Ansprüche auf Arbeitsentgelt jeder Art einschließlich Betriebsrenten, Ruhegeld, Provisionsforderungen, Tantiemen, Gewinnbeteiligungen, Erfindungsvergütungen, Abfindungen, Pensionen sowie auf laufende Geldleistungen gem. § 53 Absatz 2, Absatz 3, § 54 Absatz 2, Absatz 4 und Absatz 5 SGB I, nämlich Zahlungen von Arbeitslosengeld, Insolvenzgeld, Übergangsgeld, Rentenabfindung, Kurzarbeiter- und Schichtwettergeld, Leistungen der Kranken-, Unfall- und Rentenversicherung (auch Erwerbsunfähigkeits-, Witwen- und Waisenrente) einschließlich eventueller Abfindungen und Beitragsrückerstattungen gegen seinen jeweiligen Arbeitgeber, Leistungsträger oder Dritte zur Sicherung des aufgrund des Vertrags eingeräumten Verfügungsrahmens ab. Die Bank nimmt diese Abtretung an. Die Abtretung ist begrenzt auf den Verfügungsrahmen zuzüglich eines Pauschalbetrages von 20 % auf den Verfügungsrahmen für eventuelle Ansprüche wegen Zahlungsverzugs bzw. zusätzlich anfallender Kosten, insbesondere notwendiger Kosten der Rechtsverfolgung. Zur Berechnung des pfändbaren Teils der Gesamteinkünfte werden die abgetretenen Einkünfte des Karteninhabers entsprechend § 850e Nr. 2, 2a ZPO zusammengerechnet. Der nach den so festgestellten Gesamteinkünften unpfändbare Betrag ist in erster Linie dem Arbeitseinkommen zu entnehmen, welches die wesentliche Grundlage der Lebenshaltung des Darlehensnehmers bildet. Kommt der Karteninhaber mit der Zahlung in Verzug, ist die Bank berechtigt, die Abtretung gegenüber den Drittschuldnern offenzulegen und von der Abtretung Gebrauch zu machen, sofern sie dies gegenüber dem Karteninhaber mit einer Frist von einem Monat androht hat und der Karteninhaber nach Ablauf der Frist noch mit einem Betrag in Höhe von mindestens zwei monatlichen Teilbeträgen in Verzug ist. Die Ansprüche aus der Abtretung gehen mit vollständiger Tilgung der gesicherten Forderung auf den Karteninhaber zurück. Die Bank ist auf Verlangen des Karteninhabers zu einer Teilfreigabe der Abtretung durch entsprechende Herabsetzung des o. a. Höchstbetrages verpflichtet, falls der Nominalwert aller Sicherheiten den jeweiligen Restsaldo zuzüglich eines Sicherheitszuschlages von 20 % (Deckungsgrenze) nicht nur vorübergehend übersteigt.

**IX. Änderungen der Allgemeinen Geschäftsbedingungen**

Die Zustimmung zu den von der Bank beabsichtigten Änderungen dieser Bedingungen gilt als erteilt, wenn der Bank die Ablehnung der geplanten Änderung nicht vor dem Zeitpunkt des Wirksamwerdens der Änderungen angezeigt wird. Eine beabsichtigte Änderung wird frühestens zwei Monate nach Mitteilung der Änderungsabsicht wirksam. Die Bank wird auf diese Folge bei Bekanntgabe der Änderungen hinweisen.

**X. Kommunikation**

Bei diesem Produkt handelt es sich um ein Internet-Produkt. Die Bank erbringt Mitteilungen an den Karteninhaber durch Einstellen in die Postbox oder kann je nach Ermessen Mitteilungen per Post (textlich) oder über das Internet per E-Mail (in Textform) erbringen. Die Mitteilungen erfolgen in deutscher Sprache. Es besteht während der Vertragslaufzeit jederzeit das Recht, die Übermittlung der Vertragsbedingungen anzufordern.

**XI. Kontokorrentabrede und Rechnungsabschluss**

Einwendungen wegen Unrichtigkeit oder Unvollständigkeit eines Kontoauszugs hat der Karteninhaber spätestens vor Ablauf von sechs Wochen nach dessen Zugang zu erheben. Macht er Einwendungen textlich gel-

tend, genügt die Absendung innerhalb der Sechswochenfrist. Das Unterlassen rechtzeitiger Einwendungen gilt als Genehmigung. Auf diese Folge weist die Bank im Kontoauszug besonders hin. Auch nach Abschluss der Einwendungsfrist kann der Karteninhaber eine Berichtigung des Kontoauszugs verlangen. Dazu muss er aber beweisen, dass sein Kartenkonto zu Unrecht belastet oder ihm zu Unrecht eine Gutschrift nicht erteilt wurde.

**XII. Mitteilungspflichten, Auskünfte**

a) Der Karteninhaber hat der Bank Änderungen des Namens, der Anschrift inkl. der Kontaktdaten (z. B. Telefonnummer, E-Mail-Adresse), der persönlichen Verhältnisse (z. B. Heirat, Einkommen), des Beschäftigungsverhältnisses (z. B. Arbeitgeberwechsel, Kündigung) und bei Nutzung des Lastschriftverfahrens der Referenzkontoverbindung (z. B. Wechsel der Hausbank) umgehend textlich mitzuteilen. Unterbleibt die Mitteilung, hat er die daraus entstehenden Kosten zu tragen (z. B. Kosten für die Anfrage bei der Meldebehörde).

b) Die Bank steht dem Karteninhaber für Anfragen, Auskünfte, Aufträge (z. B. Änderung der Rückzahlungsmodalitäten, Sperren der Karte o. Ä.) auch telefonisch zur Verfügung. Die Bank behält sich das Recht vor, im Einzelfall weitere Auskünfte oder sonstige Belege zu verlangen. Die zwischen dem Karteninhaber und der Bank oder den von ihr hierfür Beauftragten geführten Telefonate können zum Zweck des Nachweises und zum Schutz des Karteninhabers aufgenommen und gespeichert werden.

**XIII. Anwendbares Recht**

Für die vertraglichen Beziehungen mit der Bank gilt deutsches Recht. Es gilt der gesetzliche Gerichtsstand.

# Datenschutzhinweise

## der Hanseatic Bank

DS/VS.07.2021

Mit diesen Informationen geben wir Ihnen einen Überblick über die Verarbeitung Ihrer personenbezogenen Daten durch die **Hanseatic Bank GmbH & Co KG** (im Weiteren **Hanseatic Bank**) und informieren Sie über Ihre Rechte als betroffene Person aus dem Datenschutzrecht. Welche Daten wir im Einzelnen verarbeiten und in welcher Weise diese genutzt werden, richtet sich maßgeblich nach den jeweils beantragten bzw. vereinbarten Dienstleistungen. Hierzu finden Sie im Rahmen dieses Datenschutzhinweises weitere Hinweise unter der jeweiligen Kategorie des Vertrages. Bitte geben Sie die Informationen auch den aktuell und künftig vertretungsberechtigten Personen und wirtschaftlichen Berechtigten sowie etwaigen Mitverpflichteten eines Kredites weiter. Dazu zählen z. B. Begünstigte im Todesfall, Prokuristen oder Bürgen.

### 1. Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?

#### Verantwortliche Stelle

Hanseatic Bank GmbH & Co KG  
Bramfelder Chaussee 101  
22177 Hamburg  
Telefon: 040 646 03-0  
Telefax: 040 646 03-297  
E-Mail: [info@hanseaticbank.de](mailto:info@hanseaticbank.de)

#### Datenschutzbeauftragter

Hanseatic Bank GmbH & Co KG  
Die Datenschutzbeauftragte  
Bramfelder Chaussee 101  
22177 Hamburg  
Telefon: 040 646 03-0  
Telefax: 040 646 03-297  
E-Mail: [datenschutz@hanseaticbank.de](mailto:datenschutz@hanseaticbank.de)

### 2. Welche Quellen nutzen wir?

Wir verarbeiten personenbezogene Daten, die wir im Rahmen unserer Geschäftsbeziehung von unseren Kunden erhalten. Zudem verarbeiten wir – soweit für die Erbringung unserer Dienstleistung erforderlich – personenbezogene Daten, die wir aus öffentlich zugänglichen Quellen (z. B. Schuldnerverzeichnisse, Grundbücher, Handels- und Vereinsregister, Presse, Internet) zulässigerweise gewinnen oder die uns von anderen Unternehmen (z. B. Kreditvermittler) oder von sonstigen Dritten (z. B. einer Kreditauskunftei) berechtigt übermittelt werden.

Auch im Rahmen eines persönlichen Kontaktes mit der Hanseatic Bank (z. B. anlässlich einer Messe / Veranstaltung / eines Seminars / sonstigen Termins / Telefonats oder per E-Mail / Brief / Fax) mitgeteilte personenbezogene Daten werden verarbeitet. Sofern es keinen persönlichen Kontakt gab, haben wir personenbezogene Daten über Dritte (z. B. Vermittler, Netzwerkpartner) erhalten oder aus öffentlich zugänglichen Quellen entnommen.

Die vorstehenden Ausführungen gelten auch für personenbezogene Daten von Ihnen in Ihrer Funktion als Vertreter / Bevollmächtigter einer juristischen Person.

### 3. Welche Daten nutzen wir?

a) Relevante personenbezogene Daten im Rahmen einer Kontakthanbahnung können sein:

- **Persönliche Daten**, z. B. vollständiger Name, Adresse, Kontaktdaten (z. B. E-Mail-Adresse und Telefon), Firma / Branche, Position im Unternehmen.

b) Relevante personenbezogene Daten im Rahmen einer Geschäftsanbahnung, im Zuge einer Bevollmächtigung (Kontovollmacht, Zugang zum Online-Banking) oder als Mitverpflichteter eines Kredites (z. B. Bürge) können sein:

- **Persönliche Daten**, z. B. vollständiger Name, Adresse, Kontaktdaten (z. B. E-Mail-Adresse und Telefon), Firma/Branche, Position im Unternehmen, Geburtsdatum und -ort, Staatsangehörigkeit, bei Nicht-EU-Staatsangehörigen Aufenthalts-/Arbeitslaubnis, Familienstand und Geschäftsfähigkeit, Beruf, Berufsgruppenschlüssel (z. B. unselbständig / selbständig), Wohnstatus (Miete / Eigentum), Steuer-ID, FATCA-Status, Scoring- / Ratingdaten.
  - **Legitimationsdaten**, z. B. Ausweis- / Reisepassdaten und Authentifikationsdaten (z. B. Unterschriftprobe).
  - **Bonitätsdaten / Daten über Ihre finanzielle Situation**, z. B. Angaben und Nachweise zu Vermögen und Verbindlichkeiten, Angaben zum Einkommen, Gehaltsabrechnungen, Einnahmen- / Überschussrechnungen und Bilanzen, Steuerunterlagen, Zahlungsverhalten, Immobilienwert oder Wert sonstiger Gegenstände, übernommene Bürgschaften, Kreditgeschichte, Einträge bei Auskunfteien, Mietkosten bzw. Rate Baufinanzierung, Anzahl unterhaltsberechtigter Kinder, Arbeitgeber, Art und Dauer Beschäftigungsverhältnis, Art und Dauer der Selbständigkeit, Verwendungszweck (bei Darlehen), Güterstand, Eigen- und Fremdsicherheiten: Objektunterlagen, Dokumentationsdaten (z. B. Beratungsprotokolle), Lebens- und Rentenversicherungen, Erwerbs- / Berufsunfähigkeits- und Pflegeversicherung.
  - **Werbe- und Vertriebsdaten**, z. B. Daten über Ihre Nutzung von durch die Hanseatic Bank angebotenen Telemedien (z. B. Aufruf der Webseiten der Hanseatic Bank, Apps) sowie andere mit den genannten Kategorien vergleichbare Daten.  
Die Hanseatic Bank nutzt insoweit insbesondere Cookies, Re-Targeting-Technologie (zur Wiedererkennung) und Webanalysedienste. Weitere Informationen zu diesen Diensten finden Sie in der Datenschutzerklärung der Hanseatic Bank unter [www.hanseaticbank.de/services/datenschutz](http://www.hanseaticbank.de/services/datenschutz).
- c) Relevante personenbezogene Daten im Rahmen einer Geschäftsbeziehung und der Nutzung von Produkten / Dienstleistungen, aus den im Folgenden aufgelisteten Produktkategorien, können sein:
- **Spar- und Einlagengeschäft**: Daten aus der Erfüllung unserer vertraglichen Verpflichtungen (z. B. Umsätze), steuerliche Informationen (z. B. Angaben zur Kirchensteuerpflicht), Angaben zu etwaigen Drittbegünstigten, Dokumentationsdaten (z. B. Beratungsprotokolle).
  - **Kreditkarten- und Co-Branding-Kreditkartengeschäft** (z. B. GenialCard, GoldCard, Deutschland-Kreditkarte Classic, Deutschland-Kreditkarte Gold): z. B. Kreditkartennummer, Kundennummer, Kreditkartenart, Mitgliedsnummer, Kreditkartenstatus, Mobilnummer, Bonuspunkte, Gesamtbetrag des mit der Kreditkarte getätigten Umsatzes, Stornierungen / Rückbuchungen, Datum und Ort der Benutzung der Karte, Ausgabedatum und Vertragsende.

- **Finanzierungen**: z. B. Dokumentationsdaten (z. B. Beratungsprotokolle), Darlehenshöhe, Darlehensraten, Fälligkeiten, Angaben / Nachweise zum Verwendungszweck, Eigen- und Fremdsicherheiten.
- **Online Banking**, z. B. Auftragsdaten (z. B. Zahlungsauftrag, Umsatzen im Zahlungsverkehr, Empfänger, IBAN, Verwendungszweck).
- **Digitale Services**: Hinsichtlich der beim Einsatz von digitalen Serviceprodukten verarbeiteten Daten wird verwiesen auf weiterführende Informationen zum Datenschutz im Zusammenhang mit dem jeweiligen digitalen Service.

Darüber hinaus können während der Geschäftsanbahnung und -beziehung, insbesondere durch persönliche, schriftliche oder telefonische Kontakte, durch Sie oder von der Hanseatic Bank initiiert, weitere personenbezogene Daten, z. B. Informationen über Kontaktkanal, Datum der Kontaktaufnahme, Anlass und Ergebnis des Kontakts, (elektronische) Kopien des Schriftverkehrs sowie Informationen über die Einbindung in Direktmarketingmaßnahmen verarbeitet werden.

### 4. Wofür verarbeiten wir Ihre Daten (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage?

Wir verarbeiten die oben genannten personenbezogenen Daten im Einklang mit den Bestimmungen der EU-Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG).

#### 4.1 Zur Erfüllung vertraglicher Pflichten (Artikel 6 Abs. 1 b DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt zur Erbringung und Vermittlung von Bankgeschäften, Finanzdienstleistungen sowie Versicherungs- und Immobiliengeschäften, insbesondere zur Durchführung vorvertraglicher Maßnahmen und der Erfüllung von Verträgen mit Ihnen und der Ausführung Ihrer Aufträge sowie aller mit dem Betrieb und der Verwaltung eines Kredit- und Finanzdienstleistungsinstituts erforderlichen Tätigkeiten.

Die Zwecke der Datenverarbeitung richten sich in erster Linie nach dem konkreten Produkt oder Service (z. B. Abwicklung Zahlungsverkehr, Kreditkartengeschäft, Einlagengeschäft, Vermittlung, Prüfungsvorgänge im Kredit- / Darlehensgeschäft) und können bei der Hanseatic Bank unter anderem die

- Abwicklung von Versicherungsfällen durch Versicherungen, die zur Kreditkarte gehören,
- Durchführung des Darlehensschutzes (Restschuldversicherung),
- Bargeldeinzahlungen und -auszahlungen,
- Anzeige des Finanzstatus des Kunden bei Fremdbankinstituten (Multibanking),
- Beratung, Bedarfsanalysen

sowie die Durchführung von weiteren Transaktionen, die Ihre Geschäftsbeziehung betreffen, umfassen.

Die weiteren Einzelheiten zum Zweck der Datenverarbeitung können Sie den jeweiligen Vertragsunterlagen und Geschäftsbedingungen entnehmen.

#### 4.2 Im Rahmen der Interessenabwägung (Artikel 6 Abs. 1 f DSGVO)

Soweit erforderlich, verarbeiten wir Ihre Daten über die eigentliche Erfüllung des Vertrages hinaus zur Wahrung berechtigter Interessen von uns oder Dritten. Beispiele:

- Kontakt- und Geschäftsanbahnung,
- Konsultation von und Datenaustausch mit Auskunfteien (z. B. SCHUFA, Creditreform) zur Ermittlung von Bonitäts- bzw. Ausfallrisiken,
- Datenaustausch mit Vermittlern über das Zustandekommen von Verträgen oder ggf. noch fehlende Unterlagen sowie zu Abrechnungszwecken,
- Prüfung und Optimierung von Verfahren zur Bedarfsanalyse inklusive Kundensegmentierung und Berechnung von Abschlusswahrscheinlichkeiten,
- Direktwerbung oder Markt- und Meinungsforschung, soweit zulässig und soweit Sie der Nutzung Ihrer Daten diesbezüglich nicht widersprochen haben,
- Visa Account Updater (im Folgenden „Aktualisierungsservice“):  
Der Aktualisierungsservice übermittelt im Rahmen eines automatisierten Datenaustausches aktualisierte Kreditkartendaten von Kunden an Visa.  
Dies beinhaltet die Kreditkartennummer und/oder die Änderung des Ablaufdatums und Benachrichtigungen über geschlossene und neue Konten.  
Visa übermittelt die Informationen in elektronischer Form an teilnehmende Akzeptanzstellen um diesen die Aktualisierung der Kreditkartendaten zu ermöglichen, bspw. um Zahlungen für wiederkehrende Dienstleistungen und mit mobilen Zahlungslösungen oder zuvor genehmigte Zahlungen (bspw. für Onlinedienste oder Abonnements) auch nach einer Aktualisierung der Kreditkartendaten automatisch sicherzustellen.  
Sollten Sie dies nicht wünschen, können Sie der Verarbeitung Ihrer Daten für diesen Service gem. Artikel 21 Datenschutz-Grundverordnung widersprechen, wodurch Ihre Teilnahme am Aktualisierungsservice nicht mehr möglich ist und automatisch endet.  
Der Widerspruch gilt für die entsprechende Karte.
- Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten,
- Gewährleistung der IT-Sicherheit und des IT-Betriebs der Hanseatic Bank,
- Verhinderung und Aufklärung von Straftaten,
- Videoüberwachungen zur Sammlung von Beweismitteln bei Straftaten oder zum Nachweis von Verfügungen und Einzahlungen (z. B. an Geldautomaten), zum Schutz von Kunden und Mitarbeitern sowie zur Wahrnehmung des Hausrechts,
- Maßnahmen zur Gebäude- und Anlagensicherheit (z. B. Zutrittskontrollen),
- Maßnahmen zur Sicherstellung des Hausrechts,
- Maßnahmen zur Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten,
- Maßnahmen zur Risikosteuerung sowie
- Maßnahmen zur Refinanzierung von Darlehen

#### 4.3 Aufgrund Ihrer Einwilligung (Art. 6 Abs. 1 a DSGVO)

Soweit Sie uns eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke (z. B. Weitergabe von Daten an Kooperationspartner im Co-Branding-Kreditkartengeschäft, Auswertung von Zahlungsverkehrsdaten für Marketingzwecke oder Informationen über neue Services) erteilt haben, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis Ihrer Einwilligung gegeben. **Eine erteilte Einwilligung ist freiwillig und kann jederzeit widerrufen werden.** Dies gilt auch für den Widerruf von Einwilligungserklärungen, die – wie beispielsweise die SCHUFA-Klausel – vor der Geltung der DSGVO, also vor dem 25. Mai 2018, der Hanseatic Bank gegenüber erteilt worden sind.

Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon also nicht betroffen.

#### 4.4 Aufgrund gesetzlicher Vorgaben (Art. 6 Abs. 1 Buchst. c DSGVO) oder im öffentlichen Interesse (Art. 6 Abs. 1 Buchst. e DSGVO)

Zudem unterliegt die Hanseatic Bank diversen rechtlichen Verpflichtungen, das heißt gesetzlichen Anforderungen (z. B. Kreditwesengesetz, Geldwäschegesetz, Wertpapierhandelsgesetz, Steuergesetze) sowie bankenaufsichtsrechtlichen Vorgaben (z. B. der Europäischen Zentralbank, der Europäischen Bankenaufsicht, der Deutschen Bundesbank und der Bundesanstalt für Finanzdienstleistungsaufsicht). Zu den Zwecken der Verarbeitung gehören unter anderem die Kreditwürdigkeitsprüfung, die Identitäts- und Altersprüfung, Betrugs- und Geldwäscheprevention, die Erfüllung steuerrechtlicher Kontroll- und Meldepflichten, Maßnahmen zur Gebäude- und Anlagensicherheit (z. B. Zutrittskontrollen) sowie die Bewertung und Steuerung von Risiken. Aufgrund der hohen Komplexität und Masse an individuellen Anforderungen im Rahmen der bankaufsichtsrechtlichen Vorgaben wenden Sie sich für weitere Informationen bitte mit einer Anfrage für die von Ihnen benötigten Informationen an unseren Datenschutzbeauftragten.

#### 5. Wer bekommt Ihre Daten?

Innerhalb der Hanseatic Bank erhalten diejenigen Stellen Zugriff auf Ihre Daten, die diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten brauchen. Auch von uns eingesetzte Dienstleister und Erfüllungsgehilfen können zu diesen Zwecken Daten erhalten, wenn diese das Bankgeheimnis und unsere schriftlichen datenschutzrechtlichen Weisungen wahren. Dies sind im wesentlichen Unternehmen aus den im Folgenden aufgeführten Kategorien.

Im Hinblick auf die Datenweitergabe an Empfänger außerhalb der Bank ist zunächst zu beachten, dass wir als Bank zur Verschwiegenheit über alle kundenbezogenen Tatsachen und Wertungen verpflichtet sind, von denen wir Kenntnis erlangen (Bankgeheimnis gemäß unserer Allgemeinen Geschäftsbedingungen). Informationen über Sie dürfen wir nur weitergeben, wenn gesetzliche Bestimmungen dies gebieten, Sie eingewilligt haben, wir zur Erteilung einer Bankauskunft befugt sind und/oder von uns beauftragte Auftragsverarbeiter gleichgerichtet die Einhaltung des Bankgeheimnisses sowie die Vorgaben der EU-Datenschutz-Grundverordnung /des Bundesdatenschutzgesetzes garantieren.

Unter diesen Voraussetzungen können Empfänger personenbezogener Daten z. B. sein:

- Öffentliche Stellen und Institutionen (z. B. Deutsche Bundesbank, Bundesanstalt für Finanzdienstleistungsaufsicht, Europäische Bankenaufsichtsbehörde, Europäische Zentralbank, Finanzbehörden) bei Vorliegen einer gesetzlichen oder behördlichen Verpflichtung.
- Andere Kredit- und Finanzdienstleistungsinstitute, vergleichbare Einrichtungen und Auftragsverarbeiter, an die wir zur Durchführung der Geschäftsbeziehung mit Ihnen personenbezogene Daten übermitteln. Im Einzelnen: Abwicklung von Bankauskünften, Unterstützung/Wartung von EDV-/IT-Anwendungen, Archivierung, Belegbearbeitung, CallCenter-Services, Compliance-Services, Controlling, Datenscreening für Anti-Geldwäsche-Zwecke, Datenvernichtung, Einkauf/Beschaffung, Flächenmanagement, Immobiliengutachten, Kreditabwicklungsservice, Sicherheitenverwaltung, Zahlkartenabwicklung (Kreditkarten), Kundenverwaltung, Lettershops, Marketing, Medientechnik, Meldewesen, Research, Risikocontrolling, Spesenabrechnung, Telefonie, Videolegitimation, Webseitenmanagement, Wertpapierdienstleistung, Wirtschaftsprüfungsdienstleistung.

Weitere Datenempfänger können diejenigen Stellen sein, für die Sie Ihre Einwilligung zur Datenübermittlung erteilt haben bzw. für die Sie uns vom Bankgeheimnis gemäß Vereinbarung oder Einwilligung befreit haben.

#### 6. Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?

Eine Übermittlung personenbezogener Daten in Drittländer (Staaten außerhalb des Europäischen Wirtschaftsraums (EWR)) erfolgt nur, soweit dem Drittland durch die EU-Kommission ein angemessenes Datenschutzniveau bestätigt worden ist oder andere angemessene Datenschutzgarantien (z. B. verbindliche unternehmensinterne Datenschutzvorschriften oder EU-Standarddatenschutzklauseln) vereinbart worden sind oder Sie der Hanseatic Bank Ihre Einwilligung erteilt haben.

Über Einzelheiten wird Sie die Hanseatic Bank, sofern gesetzlich vorgegeben, gesondert informieren.

#### 7. Wie lange werden Ihre Daten gespeichert?

Soweit erforderlich, verarbeitet und speichert die Hanseatic Bank Ihre personenbezogenen Daten für die Dauer der Geschäftsbeziehung, was beispielsweise auch die Anbahnung und die Abwicklung eines Vertrages umfasst. Dabei ist zu beachten, dass die Geschäftsbeziehung mit der Hanseatic Bank ein Dauerschuldverhältnis ist, welches auf Jahre angelegt ist. Für Organe juristischer Personen gilt, dass die Verarbeitung und Speicherung solange erfolgt, wie Sie für die jeweilige juristische Person der Hanseatic Bank gegenüber vertretungsberechtigt sind.

Darüber hinaus unterliegt die Hanseatic Bank verschiedenen Aufbewahrungs- und Dokumentationspflichten, die sich unter anderem aus dem Handelsgesetzbuch (HGB), der Abgabenordnung (AO), dem Kreditwesengesetz (KWG), dem Geldwäschegesetz (GwG) und dem Wertpapierhandelsgesetz (WpHG) ergeben. Die dort vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen zwei bis zehn Jahre.

Schließlich beurteilt sich die Speicherdauer auch nach den gesetzlichen Verjährungsfristen, die zum Beispiel nach den §§ 195 ff. des Bürgerlichen Gesetzbuches (BGB) in der Regel 3 Jahre, in gewissen Fällen aber auch bis zu 30 Jahre, betragen können.

#### 8. Welche Datenschutzrechte haben Sie?

Jede betroffene Person hat das Recht auf Auskunft nach Artikel 15 DSGVO, das Recht auf Berichtigung nach Artikel 16 DSGVO, das Recht auf Löschung nach Artikel 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Artikel 18 DSGVO, das Recht auf Widerspruch aus Artikel 21 DSGVO sowie das Recht auf Datenübertragbarkeit aus Artikel 20 DSGVO. Beim Auskunftsrecht und beim Lösungsrecht gelten die Ein-

schränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Artikel 77 DSGVO i. V. m. § 19 BDSG).

Eine erteilte Einwilligung in die Verarbeitung personenbezogener Daten können Sie jederzeit uns gegenüber widerrufen. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der EU-Datenschutz-Grundverordnung, also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

#### 9. Inwieweit gibt es eine automatisierte Entscheidungsfindung im Einzelfall?

Wir verwenden in Antragsstrecken oder im Internet-Banking für ausgewählte Produkte die technische Möglichkeit der automatisierten Entscheidung gem. Art. 22 DSGVO, z. B. Informationen von Auskunfteien bei der Bewilligung / Ablehnung von Darlehen und Kreditrahmen. In diesen ausgewählten Fällen wird die Hanseatic Bank Sie hierüber gesondert informieren, sofern dies gesetzlich vorgegeben ist. Sie können jederzeit eine Überprüfung der automatisierten Entscheidung fordern.

#### 10. Inwieweit werden Ihre Daten für die Profilbildung (Scoring) genutzt?

Wir verarbeiten teilweise Ihre Daten automatisiert mit dem Ziel, bestimmte persönliche Aspekte zu bewerten (Profiling). Die Hanseatic Bank setzt Profiling beispielsweise in folgenden Fällen ein:

- Aufgrund gesetzlicher und regulatorischer Vorgaben sind wir zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und vermögensgefährdenden Straftaten verpflichtet. Dabei werden auch Datenauswertungen (u. a. im Zahlungsverkehr) vorgenommen. Diese Maßnahmen dienen zugleich auch Ihrem Schutz.
- Um Sie zielgerichtet über Produkte informieren und beraten zu können, setzen wir Auswertungsinstrumente ein. Diese ermöglichen eine bedarfsgerechte Kommunikation und Werbung einschließlich Markt- und Meinungsforschung.
- Im Rahmen der Beurteilung Ihrer Kreditwürdigkeit nutzen wir das Scoring. Dabei wird die Wahrscheinlichkeit berechnet, mit der ein Kunde seinen Zahlungsverpflichtungen vertragsgemäß nachkommen wird. In die Berechnung können beispielsweise Einkommensverhältnisse, Ausgaben, bestehende Verbindlichkeiten, Beruf, Arbeitgeber, Beschäftigungsdauer, Erfahrungen aus der bisherigen Geschäftsbeziehung, vertragsgemäße Rückzahlung früherer Kredite sowie Informationen von Kreditauskunfteien einfließen. Das Scoring beruht auf einem mathematisch-statistisch anerkannten und bewährten Verfahren. Die errechneten Score-Werte unterstützen uns bei der Entscheidungsfindung im Rahmen von Produktabschlüssen und gehen in das laufende Risikomanagement mit ein.

#### Information über Ihr Widerspruchsrecht nach Artikel 21 EU-Datenschutz-Grundverordnung (DSGVO)

##### 1. Einzelfallbezogenes Widerspruchsrecht

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Abs. 1 e DSGVO (Datenverarbeitung im öffentlichen Interesse) und Artikel 6 Abs. 1 f DSGVO (Datenverarbeitung auf der Grundlage einer Interessenabwägung) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling im Sinne von Artikel 4 Abs. 4 DSGVO.

Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten in Zukunft nicht mehr verarbeiten, es sei denn, wir sind gesetzlich zu einer Aufbewahrung einzelner personenbezogener Daten verpflichtet oder können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

##### 2. Widerspruchsrecht gegen Verarbeitung von Daten zu Werbezwecken

In Einzelfällen verarbeiten wir Ihre personenbezogenen Daten, um Direktwerbung zu betreiben. Sie haben das Recht, jederzeit Widerspruch gegen die Verarbeitung Sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Widersprechen Sie der Verarbeitung für Zwecke der Direktwerbung, so werden wir Ihre personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten.

Der Widerspruch kann formfrei erfolgen und sollte möglichst per E-Mail gerichtet werden an: [info@hanseaticbank.de](mailto:info@hanseaticbank.de) oder an [datenschutz@hanseaticbank.de](mailto:datenschutz@hanseaticbank.de)

# SCHUFA-Information

## Information über Ihr Widerspruchsrecht nach Artikel 21 EU-Datenschutz-Grundverordnung (DSGVO)

SH V3, 10.2020

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

SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden, Tel.: 0611 9278-0

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

### 2. Datenverarbeitung durch die SCHUFA

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

Die SCHUFA verarbeitet personenbezogene Daten, um berechtigten Empfängern Informationen zur Beurteilung der Kreditwürdigkeit von natürlichen und juristischen Personen zu geben. Hierzu werden auch Scorewerte ermittelt 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, Geldwäscheprevention, Identitäts- und Altersprüfung, Anschriftenermittlung, Kundenbetreuung oder Risikosteuerung sowie der Tarifierung oder Konditionierung. Neben den vorgenannten Zwecken verarbeitet die SCHUFA personenbezogene Daten auch zu internen Zwecken (z. B. Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten, Weiterentwicklung von Dienstleistungen und Produkten, Forschung und Entwicklung insbesondere zur Durchführung interner Forschungsprojekte (z. B. SCHUFA-Kreditkompass) oder zur Teilnahme an nationalen und internationalen externen Forschungsprojekten im Bereich der genannten Verarbeitungszwecke sowie Gewährleistung der IT-Sicherheit und des IT-Betriebs). Das berechtigte Interesse hieran ergibt sich aus den jeweiligen Zwecken und ist im Übrigen wirtschaftlicher Natur (effiziente Aufgabenerfüllung, Vermeidung von Rechtsrisiken). Es können auch anonymisierte Daten verarbeitet werden. Über etwaige Änderungen der Zwecke der Datenverarbeitung wird die SCHUFA gemäß Art. 14 Abs. 4 DSGVO informieren.

#### 2.2 Rechtsgrundlagen für die Datenverarbeitung

Die SCHUFA verarbeitet personenbezogene Daten auf Grundlage der Bestimmungen der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes. Die Verarbeitung erfolgt auf Basis von Einwilligungen (Art. 6 Abs. 1 Buchstabe a DSGVO) sowie auf Grundlage des Art. 6 Abs. 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 einerseits 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 etwa öffentlichen Verzeichnissen und amtlichen Bekanntmachungen (z. B. Schuldnerverzeichnisse, Insolvenzbekanntmachungen) oder von Compliance-Listen (z. B. Listen über politisch exponierte Personen und Sanktionslisten) sowie von Datenlieferanten. Die SCHUFA speichert ggf. auch Eigenangaben der betroffenen Personen nach entsprechender Mitteilung und Prüfung.

#### 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 nicht erfüllte Zahlungsverpflichtungen wie z. B. unbestrittene, fällige und mehrfach angemahnte oder titulierte Forderungen sowie deren Erledigung | Informationen zu missbräuchlichem oder sonstigen betrügerischem Verhalten wie z. B. Identitäts- oder Bonitätstäuschungen | Informationen aus allgemein zugänglichen Quellen (z. B. Schuldnerverzeichnisse, Insolvenzbekanntmachungen) | Daten aus Compliance-Listen | Informationen ob und in welcher Funktion in allgemein zugänglichen Quellen ein Eintrag zu einer Person des öffentlichen Lebens mit übereinstimmenden Personendaten existiert | Anschriftendaten | 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 oder Standardvertragsklauseln vereinbart wurden, die unter [www.schufa.de](http://www.schufa.de) eingesehen werden können) ansässige Vertragspartner gem. Ziffer 2.3. Weitere Empfänger können externe Auftragnehmer der SCHUFA nach Art. 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 Dauer. Maßgebliches Kriterium für die Festlegung dieser Dauer ist die Erforderlichkeit der Verarbeitung zu den o. g. Zwecken. Im Einzelnen sind die Speicherfristen in einem Code of Conduct des Verbandes „Die Wirtschaftsauskunfteien e. V.“ festgelegt (einsehbar unter [www.schufa.de/loeschfristen](http://www.schufa.de/loeschfristen)). Angaben über Anfragen werden nach 12 Monaten taggenau gelöscht.

### 3. Betroffenenrechte

Jede betroffene Person hat gegenüber der SCHUFA das Recht auf Auskunft nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO, das Recht auf Löschung nach Art. 17 DSGVO und das Recht auf Einschränkung der Verarbeitung nach Art. 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 0611 9278-0 und über ein Rückfrageformular unter [www.schufa.de/rueckfrageformular](http://www.schufa.de/rueckfrageformular) erreichbar ist. Darüber hinaus besteht die Möglichkeit, sich an die für die SCHUFA zuständige Aufsichtsbehörde, den Hessischen Beauftragten für Datenschutz und Informationsfreiheit, zu wenden. Einwilligungen können jederzeit gegenüber dem betreffenden Vertragspartner widerrufen werden.

**Nach Art. 21 Abs. 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)

Neben der Erteilung von Auskünften über die zu einer Person gespeicherten Informationen unterstützt die SCHUFA ihre Vertragspartner bei deren Entscheidungsfindung durch Profilbildungen, insbesondere mittels sogenannter Scorewerte. Dies hilft z. B. dabei, alltägliche Kreditgeschäfte rasch abwickeln zu können.

Unter dem Oberbegriff der Profilbildung wird die Verarbeitung personenbezogener Daten unter Analyse bestimmter Aspekte zu einer Person verstanden. Besondere Bedeutung nimmt dabei das sogenannte Scoring im Rahmen der Bonitätsprüfung und Betrugsprävention ein. Scoring kann aber darüber hinaus der Erfüllung weiterer der in Ziffer 2.1 dieser SCHUFA-Information genannten Zwecke dienen. Beim Scoring wird anhand von gesammelten Informationen und Erfahrungen aus der Vergangenheit eine Prognose über zukünftige Ereignisse oder Verhaltensweisen erstellt. Anhand der zu einer Person bei der SCHUFA gespeicherten Informationen erfolgt eine Zuordnung zu statistischen Personengruppen, die in der Vergangenheit eine ähnliche Datenbasis aufwiesen.

Zusätzlich zu dem bereits seit vielen Jahren im Bereich des Bonitätsscorings etablierten Verfahren der Logistischen Regression, können bei der SCHUFA auch Scoringverfahren aus den Bereichen sogenannter Komplexer nicht linearer Verfahren oder Expertenbasierter Verfahren zum Einsatz kommen. Dabei ist es für die SCHUFA stets von besonderer Bedeutung, dass die eingesetzten Verfahren mathematisch-statistisch anerkannt und wissenschaftlich fundiert sind. Unabhängige externe Gutachter bestätigen uns die Wissenschaftlichkeit dieser Verfahren. Darüber hinaus werden die angewandten Verfahren der zuständigen Aufsichtsbehörde offengelegt. Für die SCHUFA ist es selbstverständlich, die Qualität und Aktualität der eingesetzten Verfahren regelmäßig zu prüfen und entsprechende Aktualisierungen vorzunehmen.

Die Ermittlung von Scorewerten zur Bonität erfolgt bei der SCHUFA auf Grundlage der zu einer Person bei der SCHUFA gespeicherten Daten, die auch in der Datenkopie nach Art. 15 DSGVO ausgewiesen werden. Anhand dieser bei der SCHUFA gespeicherten Informationen erfolgt dann eine Zuordnung zu statistischen Personengruppen, die in der Vergangenheit eine ähnliche Datenbasis aufwiesen. Für die Ermittlung von Scorewerten zur Bonität werden die gespeicherten Daten in sogenannte Datartern zusammengefasst, die unter [www.schufa.de/scoring-faq](http://www.schufa.de/scoring-faq) eingesehen werden können. Bei der Ermittlung von Scorewerten zu anderen Zwecken können auch weitere Daten(arten) einfließen. Angaben zur Staatsangehörigkeit oder besonders sensible Daten nach Art. 9 DSGVO (z. B. ethnische Herkunft oder Angaben zu politischen oder religiösen Einstellungen) werden bei der SCHUFA nicht gespeichert und stehen daher für die Profilbildung nicht zur Verfügung. Auch die Geltendmachung der Rechte der betroffenen Person nach der DSGVO, wie z. B. die Einsichtnahme in die zur eigenen Person bei der SCHUFA gespeicherten Daten nach Art. 15 DSGVO, hat keinen Einfluss auf die Profilbildung. Darüber hinaus berücksichtigt die SCHUFA beim Scoring die Bestimmungen des § 31 BDSG.

Mit welcher Wahrscheinlichkeit eine Person bspw. einen Baufinanzierungskredit zurückzahlen wird, muss nicht der Wahrscheinlichkeit entsprechen, mit der sie eine Rechnung beim Versandhandel termingerecht bezahlt. Aus diesem Grund bietet die SCHUFA ihren Vertragspartnern unterschiedliche branchen- oder sogar kundenspezifische Scoremodelle an. Scorewerte verändern sich stetig, da sich auch die Daten, die bei der SCHUFA gespeichert sind, kontinuierlich verändern. So kommen neue Daten hinzu, während andere aufgrund von Speicherfristen gelöscht werden. Außerdem ändern sich auch die Daten selbst im Zeitverlauf (z. B. die Dauer des Bestehens einer Geschäftsbeziehung), sodass auch ohne neue Daten Veränderungen auftreten können.

Wichtig zu wissen: Die SCHUFA selbst trifft keine Entscheidungen. Sie unterstützt die angeschlossenen Vertragspartner lediglich mit ihren Auskünften und Profilbildungen bei der Entscheidungsfindung. Die Entscheidung für oder gegen ein Geschäft trifft hingegen allein der direkte Geschäftspartner. Dies gilt selbst dann, wenn er sich einzig auf die von der SCHUFA gelieferten Informationen verlässt. Weitere Informationen zu Profilbildungen und Scoring bei der SCHUFA (z. B. über die derzeit im Einsatz befindlichen Verfahren) können unter [www.schufa.de/scoring-faq](http://www.schufa.de/scoring-faq) eingesehen werden.

# Online Banking

## Bedingungen für die Nutzung des Online Banking

BIB V7\_10.2020

### 1. Leistungsangebot

Der Kontoinhaber kann Bankgeschäfte mittels Online Banking in dem von der Hanseatic Bank (nachfolgend „Bank“) angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Online Banking abrufen. Im Rahmen des Online Banking ist der Kontoinhaber zusätzlich berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste zu nutzen. Darüber hinaus kann der Kontoinhaber von ihm ausgewählte Drittdienste nutzen.

### 2. Voraussetzungen zur Nutzung des Online Banking

(1) Nutzungsberechtigter des Online-Banking-Angebotes der Bank ist der Kontoinhaber. Die Stellvertretung durch andere Personen ist nicht gestattet, um Missbrauch auszuschließen.

(2) Der Kontoinhaber muss für die Abwicklung von Bankgeschäften mittels Online Banking durch die Bank authentifiziert werden. Mit der Authentifizierung überprüft die Bank die Identität des Kontoinhabers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments. Der Kontoinhaber weist sich mit den vereinbarten Authentifizierungselementen als berechtigter Teilnehmer aus und kann Informationen erhalten sowie Aufträge erteilen.

Ein Authentifizierungselement ist:

- ein Element aus der Kategorie Wissen, welches nur dem Kontoinhaber bekannt ist (z. B. Online-Banking-Passwort),
- ein Element aus der Kategorie Besitz als ein Gegenstand, den nur der Kontoinhaber besitzt (z. B. das Mobiltelefon) oder
- ein Element aus der Kategorie Inhärenz als ein nur dem Kontoinhaber innewohnendes persönliches Merkmal (z. B. Fingerabdruck).

(3) Die Authentifizierung des Kontoinhabers erfolgt, indem der Kontoinhaber gemäß der Anforderung der Bank das gesondert vereinbarte Element der Kategorie Wissen, den Nachweis des Elements aus der Kategorie Besitz und/oder den Nachweis des Elements aus der Kategorie Inhärenz an die Bank übermittelt.

### 3. Zugang zum Online Banking und Verfahren

(1) Der Kontoinhaber hat mittels Online Banking Zugang zum Konto, wenn er zuvor die Benutzerkennung eingegeben hat und sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselements/Authentifizierungselemente ausweist und keine Sperre des Zugangs vorliegt. Nach Gewährung des Zugangs zum Online Banking kann auf Informationen zugegriffen und können Aufträge erteilt werden. Für den Zugriff auf sensible Zahlungsdaten fordert die Bank den Kontoinhaber auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Online Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kontoinhabers und die IBAN sind für den vom Kontoinhaber genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Daten. Der Kontoinhaber muss einem Auftrag zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu ein Authentifizierungselement zu verwenden. Die Bank bestätigt mittels Online Banking den Eingang des Auftrags. Nach der Erteilung der Zustimmung kann der Kontoinhaber den Auftrag nicht mehr widerrufen.

### 4. Bearbeitung von Aufträgen beim Online Banking

(1) Mittels Online Banking erteilte Aufträge werden im Rahmen der Annahme- und Ausführungsfristen im Anschluss an deren Zugang bearbeitet. Der Kontoinhaber muss einem Auftrag zu dessen Wirksamkeit zustimmen (Autorisierung).

(2) Die Bank wird den Auftrag ausführen, wenn

- er gemäß dem vereinbarten Verfahren vom Kontoinhaber autorisiert wurde.
- das Konto einen ausreichenden Verfügungshöchstbetrag gemäß Vereinbarung über die Nutzung des Online Banking aufweist und die finanzielle Nutzungsgrenze eingehalten wird.

(3) Sofern die Voraussetzungen nicht vorliegen, wird die Bank den Auftrag nicht ausführen und den Kontoinhaber darüber und soweit möglich über die Gründe informieren.

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

### 5. Sorgfaltspflichten des Kontoinhabers

(1) Der Kontoinhaber ist verpflichtet, alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (z. B. Online-Banking-Passwort, Mobiltelefon oder mobiles Endgerät, App auf einem mobilen Endgerät) sicher zu verwahren und vor dem Zugriff anderer Personen zu schützen. Anderenfalls besteht die Gefahr, dass das Online Banking missbräuchlich genutzt wird.

(2) Insbesondere ist zum Schutz der Authentifizierungselemente zu beachten, dass

- Authentifizierungselemente aus dem Bereich Wissen (z. B. Online-Banking-Passwort) geheim zu halten sind und nicht mündlich, in Textform (z. B. E-Mail) oder auf sonstige Weise weitergegeben oder ungesichert gespeichert werden dürfen (z. B. darf das Online-Banking-Passwort nicht auf dem PC oder dem mobilen Endgerät gespeichert werden).
- Authentifizierungselemente nicht auf dem mobilen Endgerät notiert oder zusammen mit dem mobilen Endgerät aufbewahrt werden dürfen.
- Authentifizierungselemente aus dem Bereich Besitz (z. B. mobiles Endgerät) vor dem unbefugten Zugriff Dritter sicher zu verwahren sind.
- der Kontoinhaber sicherzustellen hat, dass unberechtigte Personen nicht auf das mobile Endgerät zugreifen können.
- mit dem mobilen Endgerät empfangene Benachrichtigungen nicht mündlich oder per E-Mail weitergegeben werden dürfen.

Weiterhin

- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendungen (z. B. Karten-App, Authentifizierungs-App) nicht nutzen können
- ist die Anwendung (z. B. Karten-App, Authentifizierungs-App) auf dem mobilen Endgerät des Karteninhabers zu deaktivieren, bevor der Karteninhaber den Besitz an diesem mobilen Endgerät

aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons) und

- dürfen die Nachweise des Besitzelements (z. B. TAN, Code) nicht mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden
- dürfen Authentifizierungselemente aus dem Bereich Inhärenz (z. B. der Fingerabdruck des Kontoinhabers) auf einem mobilen Endgerät des Kontoinhabers nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Authentifizierungselemente aus dem Bereich Inhärenz anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, welches für das Online Banking genutzt wird, Authentifizierungselemente aus dem Bereich Inhärenz anderer Personen gespeichert, ist für das Online Banking das von der Bank ausgegebene Wissensselement (z. B. Online-Passwort) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Authentifizierungselement aus dem Bereich Inhärenz.

(3) Der Kontoinhaber muss die im Verkehr erforderliche Sorgfalt bei der Nutzung des Online Banking beachten und insbesondere angemessene Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem) treffen. Soweit dem Kontoinhaber Daten aus seinem Online-Banking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät (z. B. Mobiltelefon) zur Bestätigung angezeigt werden, ist der Kontoinhaber verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen. Bei Abweichungen hat der Kontoinhaber die Transaktion abzubrechen.

(4) Die für das vereinbarte Authentifizierungsverfahren hinterlegte Mobilfunknummer ist auf eine neue Mobilfunknummer zu ändern, wenn der Kontoinhaber diese Telefonnummer nicht mehr für das Online Banking nutzt.

(5) Ungeachtet der Schutzpflichten ist der Kontoinhaber eines Kartenkontos gegenüber Zahlungsauslösediensten und Kontoinformationsdiensten oder sonstigen Drittdiensten zur Verwendung der erforderlichen Authentifizierungselemente berechtigt, wenn diese Zahlungsaufträge über einen Zahlungsauslösedienst auslösen oder Zahlungskontoinformationen über einen Kontoinformationsdienst anfordern. Der Kontoinhaber hat bei der Auswahl sonstiger Drittdienste die im Verkehr erforderliche Sorgfalt einzuhalten.

### 6. Änderung des Online-Banking-Passworts

Der Kontoinhaber ist berechtigt, sein Online-Banking-Passwort unter Verwendung des vereinbarten Verfahrens jederzeit zu ändern. Bei Änderung des Online-Banking-Passworts wird sein bisheriges Online-Banking-Passwort ungültig.

### 7. Sperre des Online-Banking-Angebotes

(1) Stellt der Kontoinhaber den Verlust oder Diebstahl eines Authentifizierungselements aus dem Bereich Besitz, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seiner Authentifizierungselemente fest, muss er die Bank hierüber unverzüglich unterrichten (Sperranzeige).

(2) Der Kontoinhaber hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei anzuzeigen.

(3) Hat der Kontoinhaber den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben und hat sein persönliches Online-Banking-Passwort unverzüglich zu ändern. Der Kontoinhaber hat die Bank unverzüglich nach Feststellen eines nicht autorisierten oder fehlerhaft ausgeführten Auftrages hierüber zu unterrichten.

### 8. Nutzungssperre

(1) Die Hanseatic Bank sperrt auf Veranlassung des Kontoinhabers, insbesondere im Fall der Sperranzeige nach Ziffer 7, den Online-Banking-Zugang.

(2) Die Bank wird den Online-Banking-Zugang sperren,

- wenn der Verdacht einer missbräuchlichen oder betrügerischen Nutzung des Kontos über den Online-Banking-Zugang besteht.
- wenn sachliche Gründe im Zusammenhang mit der Sicherheit eines Authentifizierungselements dies rechtfertigen, oder
- wenn die Bank berechtigt ist, den Vertrag aus wichtigem Grund zu kündigen.

Die Bank wird den Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre, unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber.

(3) Die Bank wird den Online-Banking-Zugang auf Wunsch des Kontoinhabers sperren. Auch diese Sperre kann nicht mittels Online Banking aufgehoben werden.

(4) Die Bank wird eine Sperre aufheben oder das betroffene Authentifizierungselement austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber.

(5) Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zum Konto verweigern, wenn objektive und ausreichend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters zum Konto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Bank wird den Kontoinhaber auf dem vereinbarten Weg möglichst vor, spätestens unverzüglich nach der Verweigerung des Zugangs, unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Pflichten verstoßen würde. Sofern die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Bank die Zugangssperre auf und informiert den Kontoinhaber hierüber unverzüglich.

### 9. Postbox

(1) Im Rahmen der Geschäftsbeziehung zwischen der Hanseatic Bank und dem Kontoinhaber gilt die Nutzung der Postbox als vereinbarter Kommunikationsweg. In der Postbox werden dem Kontoinhaber Nachrichten der Bank online zur Verfügung gestellt.

(2) Der Kontoinhaber verzichtet durch die Nutzung der Postbox ausdrücklich auf den postalischen Versand aller Dokumente und Nachrichten durch die Bank in papiergebundener Form. Dokumente, die aufgrund rechtlicher Anforderungen von der Bank erstellt werden müssen, insbesondere Kontoauszüge und Kontoabschlüsse, sowie Nachrichten, die den Geschäftsverkehr mit der Bank betreffen, werden dem Kontoinhaber

daher grundsätzlich nur in elektronischer Form auf verschlüsselten Seiten in die Postbox im Rahmen des Online-Banking übermittelt. Die Bank ist berechtigt, dem Kontoinhaber die hinterlegten Dokumente und Nachrichten auf dem Postweg oder auf andere Weise zu übermitteln, wenn gesetzliche Vorgaben dies erforderlich machen oder die Bank dies aufgrund anderer Umstände (z. B. technischer Probleme) unter Berücksichtigung des Kundeninteresses als zweckmäßig erachtet.

(3) Die Bank stellt die Dokumente in der Postbox zur Verfügung und benachrichtigt den Kontoinhaber per E-Mail oder auf sonstige Weise, sobald ein neues Dokument online zur Verfügung steht. Der Kontoinhaber kontrolliert die hinterlegten Dokumente auf Richtigkeit und Vollständigkeit. Beanstandungen sind der Bank unverzüglich, spätestens jedoch sechs Wochen nach Zugang der Dokumente, textlich mitzuteilen. Dokumente, die die Bank in die Postbox eingestellt hat, gelten – soweit sie der Kontoinhaber nicht bereits vorher abgerufen hat – drei Kalendertage nach der Einstellung in die Postbox und Zugang der Nachricht über die Einstellung dem Kontoinhaber als zugegangen. Unbeschadet dessen gehen dem Kontoinhaber eingestellte Dokumente spätestens in dem Zeitpunkt zu, in dem dieser die Dokumente abgerufen hat.

## 10. Haftung, Berichtigungs- und Erstattungsansprüche

### 10.1 Haftung der Bank

(1) Im Falle einer nicht autorisierten Online-Banking-Verfügung hat die Bank keinen Anspruch auf Erstattung ihrer Aufwendungen. Die Bank ist verpflichtet, den Betrag unverzüglich zu erstatten und, sofern der Betrag dem Konto belastet worden ist, dieses Konto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung mit der nicht autorisierten Online-Banking-Verfügung befunden hätte. Diese Verpflichtung wird die Bank spätestens bis zum Ende des Geschäftstags erfüllen, an welchem der Kontoinhaber einen nicht autorisierten Zahlungsvorgang angezeigt hat oder die Bank auf andere Weise davon Kenntnis erhalten hat. Hat die Bank einer zuständigen Behörde berechnete Gründe für den Verdacht, dass ein betrügerisches Verhalten des Zahlers vorliegt, schriftlich mitgeteilt, hat die Bank die Verpflichtung zur Erstattung unverzüglich zu prüfen und zu erfüllen, wenn sich der Betrugsverdacht nicht bestätigt.

(2) Im Falle einer nicht erfolgten oder fehlerhaften Ausführung einer autorisierten Online-Banking-Verfügung kann der Kontoinhaber von der Bank die unverzügliche und ungekürzte Erstattung des Betrages insoweit verlangen, als die Zahlung nicht erfolgte oder fehlerhaft war. Wurde der Betrag dem Konto belastet, bringt die Bank dieses wieder auf den Stand, auf dem es sich ohne den nicht erfolgten oder fehlerhaft ausgeführten Zahlungsvorgang befunden hätte. Soweit von dem Betrag von der Bank oder zwischengeschalteten Stellen Entgelte abgezogen worden sein sollten, übermittelt die Bank zu Gunsten des Kontoinhabers unverzüglich den abgezogenen Betrag. Der Kontoinhaber kann darüber hinaus von der Bank die Erstattung derjenigen Entgelte und Zinsen insoweit verlangen, als dem Kontoinhaber diese im Zusammenhang mit der nicht erfolgten oder fehlerhaften Ausführung der Überweisung in Rechnung gestellt oder dem Konto belastet wurden.

(3) Geht die Online-Banking-Verfügung beim Zahlungsdienstleister des Zahlungsempfängers erst nach Ablauf der Ausführungsfrist ein (Verspätung), kann der Kontoinhaber von der Bank verlangen, dass diese den Zahlungsdienstleister des Empfängers darauf in Anspruch nimmt, dass dieser die Gutschrift auf dem Zahlungskonto des Empfängers so vornimmt, als sei die Online-Banking-Verfügung ordnungsgemäß ausgeführt worden.

(4) Der Kontoinhaber kann im Falle einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung verlangen, dass die Bank den Zahlungsvorgang nachvollzieht und den Kontoinhaber über das Ergebnis unterrichtet.

(5) Im Falle einer nicht erfolgten oder fehlerhaften oder verspäteten Ausführung einer autorisierten Online-Banking-Verfügung ist die Haftung der Bank – unabhängig von dem möglicherweise bestehenden gesetzlichen Erstattungsanspruch – für den über den Erstattungsanspruch hinausgehenden Schaden auf 12.500 € begrenzt, sofern die Bank überhaupt ein Verschulden trifft. Diese Haftungsbegrenzung gilt nicht bei Vorsatz und grober Fahrlässigkeit, für den Zinsschaden und für Gefahren, die die Bank besonders übernommen hat.

(6) Die Haftung der Bank ist ausgeschlossen, wenn im Falle einer nicht erfolgten oder fehlerhaften Ausführung der Online-Banking-Verfügung durch die Bank nachgewiesen wird, dass der Betrag ungekürzt eingegangen ist, oder im Falle einer Verspätung durch die Bank nachgewiesen wird, dass der Betrag rechtzeitig

eingegangen ist. Für den Fall, dass eine Online-Banking-Verfügung mit einer vom Kontoinhaber angebenen fehlerhaften Kundenkennung ausgeführt wurde, ist die Haftung der Bank ebenfalls ausgeschlossen. Der Kontoinhaber kann in diesem Fall jedoch verlangen, dass sich die Bank im Rahmen der eigenen Möglichkeiten darum bemüht, den Zahlungsbetrag wieder zu erlangen. Ist dies nicht möglich, teilt die Bank auf Antrag des Kontoinhabers alle verfügbaren Informationen mit, damit der Kontoinhaber einen Anspruch auf Erstattung geltend machen kann.

(7) Der Kontoinhaber hat die Bank unverzüglich zu unterrichten, falls er feststellt, dass eine Online-Banking-Verfügung nicht autorisiert war oder fehlerhaft ausgeführt worden ist. Ein Erstattungsanspruch ist ausgeschlossen, wenn er nicht innerhalb von 13 Monaten ab dem Tag der Belastung des betreffenden Zahlungsvorgangs gegenüber der Bank angezeigt wird. Für andere Ansprüche als die aus §§ 675u und 675y BGB wegen eines nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorgangs kann der Kontoinhaber den Anspruch auch nach Ablauf der Frist geltend machen, wenn er ohne Verschulden an der Einhaltung der Frist verhindert war. Der Lauf der Frist beginnt nur, wenn die Bank den Kontoinhaber entsprechend den vereinbarten Bedingungen über die resultierende Belastungsbuchung mit dem monatlichen Abschluss (Kontoauszug) auf dem vereinbarten Weg unterrichtet hat, anderenfalls ist für den Fristbeginn der Tag der Unterrichtung maßgeblich.

### 10.2 Haftung des Kontoinhabers

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kontoinhaber für den hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob ihn 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 Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung/Zweigstelle eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten der Bank ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Kontoinhaber in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von Absatz (1) und (2) den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Kontoinhabers kann insbesondere dann vorliegen, wenn er eine seiner unter Ziffer 5 aufgeführten Sorgfaltspflichten verletzt hat.

(4) Abweichend von Absatz (1)–(3) ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Bank eine starke Kundenauthentifizierung nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen. Der Kontoinhaber haftet jedoch, wenn er in betrügerischer Absicht gehandelt hat.

(5) Hat die Bank die Möglichkeit eine Sperranzeige gemäß Ziffer 7. vorzunehmen nicht durch geeignete Mittel sichergestellt und konnte der Kontoinhaber eine Sperre aus diesem Grunde nicht durchführen, ist er nicht zum Ersatz des Schadens verpflichtet, es sei denn, der Kontoinhaber hat in betrügerischer Absicht gehandelt.

(6) Sobald die Bank eine Sperranzeige des Kontoinhabers erhalten hat, haftet sie für alle danach durch nicht autorisierte Online-Banking-Verfügungen entstehende Schäden. Die Haftung der Bank ist ausgeschlossen, wenn der Kontoinhaber in betrügerischer Absicht gehandelt hat.

(7) Beruhen die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis, auf das die 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, sind Haftungsansprüche ausgeschlossen.

## 11. Anwendbares Recht

Für die Geschäftsbeziehung zwischen dem Kontoinhaber und der Bank gilt deutsches Recht.