

Datenschutzhinweise der TeamBank AG (Ratenkauf, Rechnungskauf)

Mit diesen Datenschutzhinweisen informiert die TeamBank AG über die Verarbeitung von personenbezogenen Daten im Rahmen des Raten- bzw. Rechnungskaufs.

Personenbezogene Daten in diesem Sinne sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, wie z. B. Name, Telefonnummer oder Adresse.

Die einzelnen Textpassagen erläutern unter anderem, aus welchen Quellen, zu welchen Zwecken und aufgrund welcher Rechtsgrundlagen wir Daten verarbeiten, wie lange wir diese speichern und ob wir Daten weitergeben. Zudem informieren wir Sie über Ihre nach datenschutzrechtlichen Regelungen zustehenden Ansprüche und Rechte.

I. Wer ist für die Datenverarbeitung verantwortlich und an wen können Sie sich wenden?

Verantwortlicher ist die TeamBank AG in der Beuthener Str. 25, 90471 Nürnberg (im Folgenden „Bank“), zu erreichen unter

Telefon: [0911 53 90 2000](tel:091153902000),

Fax: [0911 53 90-2222](tel:091153902222),

E-Mail: service@easycredit.de

Sie erreichen unseren Datenschutzbeauftragten unter der o. g. Anschrift oder unter datenschutz@teambank.de.

II. Wofür verarbeiten wir Ihre Daten und auf welcher Rechtsgrundlage?

Wir verarbeiten personenbezogene Daten im Einklang mit den Bestimmungen der Europäischen Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG):

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

Soweit Sie uns eine Einwilligung zur Verarbeitung personenbezogener Daten für bestimmte Zwecke (z. B. Einwilligung in den Erhalt eines Newsletters, Teilnahme an speziellen Marketing-Maßnahmen) erteilt haben, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis Ihrer Einwilligung gegeben. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

2. Zur Erfüllung von vertraglichen Pflichten (Art. 6 Abs. 1 lit. b DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt zur Erbringung von Bankgeschäften und Finanzdienstleistungen (bspw. Factoring), teilweise schon während der Anbahnung dieser Geschäfte, im Rahmen der Durchführung der Verträge von der Bank oder zur Durchführung banknaher Dienstleistungen, die auf Anfrage von Kunden oder Interessenten hin erfolgen. Die Zwecke, zu denen die Daten verarbeitet werden, sind in der jeweiligen Produktbeschreibung sowie den jeweiligen Allgemeinen Geschäftsbedingungen dargestellt und können unter anderem Bonitäts- und Kreditanalysen, die Beratung sowie die Durchführung von Transaktionen umfassen.

3. Aufgrund gesetzlicher Vorgaben (Art. 6 Abs. 1 lit. c DSGVO) oder im öffentlichen Interesse (Art. 6 Abs. 1 lit. e DSGVO)

Zudem unterliegen wir als Bank diversen rechtlichen Verpflichtungen und Anforderungen (z. B. aus dem Kreditwesengesetz, dem Geldwäschegesetz und Wertpapierhandelsgesetz sowie Steuergesetzen) und bankaufsichtsrechtlichen Vorgaben (z. B. der Europäischen Zentralbank,

der Europäischen Bankenaufsicht, der Deutschen Bundesbank und der Bundesanstalt für Finanzdienstleistungsaufsicht). Zu den Zwecken der Datenverarbeitungen, die auf Basis o. g. Gesetze und Anforderungen erfolgen, gehören unter anderem die Identitätsprüfung, Betrugs- und Geldwäscheprävention, die Erfüllung steuerrechtlicher Kontroll- und Meldepflichten sowie die Bewertung und Steuerung von Risiken.

4. Aufgrund berechtigter Interessen (Art. 6 Abs. 1 f DSGVO)

Soweit erforderlich, verarbeiten wir Ihre Daten zur Wahrung berechtigter Interessen von uns oder Dritten z. B. in folgenden Fällen:

- Konsultation von und Datenaustausch mit Auskunftgebern (z. B. SCHUFA Holding AG) zur Ermittlung von Bonitäts- bzw. Ausfallrisiken;
- Werbung oder Markt- und Meinungsforschung sowie sachbezogene Selektion zur bedarfsorientierten Kundenansprache, soweit sie der Nutzung Ihrer Daten nicht widersprochen haben;
- Prüfung und Optimierung von Verfahren zur Bedarfsanalyse und direkter Kundenansprache;
- Maßnahmen zur Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten, sowie damit in Verbindung stehender Prozesse;
- Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten;
- Videoüberwachung zur Sammlung von Beweismitteln, Wahrnehmung des Hausrechts und zum Schutz von Beschäftigten und Kunden;
- Maßnahmen zur Gebäude- und Anlagensicherheit (z. B. Zutrittskontrollen);
- Gewährleistung der IT-Sicherheit und des IT-Betriebs der Bank, Durchführung von Tests zu Entwicklungszwecken und zur Sicherstellung des IT-Betriebs;
- Maßnahmen zur Sicherstellung des Hausrechts;
- Verhinderung und Aufklärung von Straftaten;
- Validierung des bestehenden Arbeitsverhältnisses zur Minimierung von Ausfallrisiken;
- Entwicklung und Optimierung von Löschkonzepten und Anonymisierungsverfahren.

Bei der Optimierung und Weiterentwicklung der oben genannten Punkte kommen u.a. statistische Verfahren wie Machine Learning und KI-Systeme zum Einsatz.

III. Wie werden Daten konkret im Rahmen der Produkte Ratenkauf und Rechnungskauf verarbeitet?

Die Bank stellt Partnerunternehmen (im Folgenden „Partner“) optional und somit zusätzlich die Zahlungsmethoden Ratenkauf und Rechnungskauf im Rahmen eines Kaufabschlusses zur Verfügung. Die optionale Nutzung der jeweiligen Zahlungsmethode erfolgt gemäß den Bedingungen für den Ratenkauf sowie den Bedingungen für den Rechnungskauf. Macht der Partner hiervon Gebrauch und bietet dies seinen Kunden optional als Zahlungsmöglichkeit an, kann der Kunde im Rahmen des Kaufabschlusses die von der Bank angebotenen Zahlungsmethoden auf den Seiten eines teilnehmenden Partners auswählen. Sofern ein Kaufabschluss zwischen dem Kunden und dem Partner unter Auswahl des Ratenkaufs bzw.

Rechnungskaufs zustande kommt, wird die Bank in beiden Fällen zur Inhaberin der Forderung gegenüber dem Kunden. Zahlungen mit schuldbefreiender Wirkung sind damit seitens des Kunden ausschließlich an die Bank vorzunehmen. Hierfür wird ein Lastschriftmandat zwischen Kunden und Bank vereinbart bzw. stellt die Bank dem Kunden die Zahlungsinformationen nach Kaufabschluss zur Verfügung.

Die Bank verarbeitet die personenbezogenen Daten des Kunden, wie Identifizierungsdaten (insb. Vor- und Nachname, Geburtsdatum, E-Mail-Adresse, Telefonnummer) sowie Daten aus dem Bestellprozess (insb. Bestelldatum, Bestellbetrag, Produktname, Händlername) hauptsächlich, um den Verpflichtungen aus den „Bedingungen für den Ratenkauf“ bzw. den „Bedingungen für den Rechnungskauf“ nachzukommen. Hierbei stützt sich die Bank auf die Vertragserfüllung gem. Art. 6 Abs. 1 lit. b DSGVO. Infolgedessen kommt es zu weiteren zweckgebundenen Verarbeitungen, die in dieser Datenschutzerklärung erläutert werden. Unter anderem verarbeitet die Bank die personenbezogenen Daten des Kunden in diesem Zusammenhang auch zur Bonitätsprüfung und Betrugsrisikoanalyse. Rechtsgrundlage hierfür sind Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 25 h Absatz 2 Kreditwesengesetz (KWG) sowie Art. 6 Abs. 1 lit. f DSGVO. Mit der Verarbeitung der personenbezogenen Daten des Kunden im Rahmen der Betrugsrisikoanalyse und der Bonitätsprüfung schützt die Bank den Kunden vor einer möglichen Überschuldung, vor der betrügerischen Verwendung seiner personenbezogenen Daten sowie sich selbst vor einem Ausfallrisiko. Die Bank behält sich vor auf Basis der Ergebnisse der Betrugsrisikoanalyse und der Bonitätsprüfung die genannten Zahlungsmethoden nicht anzubieten bzw. die Zahlungsmethode bspw. vom Rechnungskauf auf den Ratenkauf abzuändern.

Um die Betrugsrisikoanalyse und Bonitätsprüfung durchführen zu können, übermittelt der Partner personenbezogene Daten des Kunden, insbesondere die Adresse, den vollständigen Namen des Kunden und die Höhe sowie Zusammensetzung des Warenkorbes, an die Bank. Die Bank prüft und bewertet die übermittelten Daten zunächst anhand eigener Vorfilter. Insbesondere prüft die Bank, ob der Kunde das gesetzliche Mindestalter für die Zahlungsmethode erfüllt und ob bereits offene Forderungen gegenüber dem Kunden bestehen. Fehlen Informationen und somit Daten, die für die Vertragserfüllung relevant sind, insbesondere das Geburtsdatum für die Gewährleistung des gesetzlichen Mindestalters sowie für die Bonitätsabfrage bei Auskunftsteilen oder die Mobilfunknummer zur Kontaktaufnahme zum Kunden, so kann die Bank die Bereitstellung dieser Daten per Kundeneingabe auf der TeamBank-Antragsstrecke verlangen. Die Bank leitet die Informationen zur Überprüfung der Identität des Kunden und der Richtigkeit der angegebenen Daten an Unternehmen weiter, die der Identitätsprüfung und Betrugsprävention dienen.

1. Hinweis auf die erforderliche Datenübermittlung an Auskunftsteile und die Befreiung vom Bankgeheimnis

Ferner pflegt die Bank bei berechtigtem Interesse, wie zur Bonitätsprüfung oder Adressermittlung, einen Datenaustausch mit Wirtschaftsauskunftsteilen. Mit den nachfolgenden Auskunftsteilen arbeitet die Bank im Rahmen des Ratenkaufs und des Rechnungskaufs zusammen:

- SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden
- Infoscore Consumer DATA GmbH, Rheinstr. 99, 76532 Baden-Baden
- Creditreform Boniversum, Hellersbergstr. 11, 41460 Neuss

Rechtsgrundlagen dieser Übermittlungen ist Artikel 6 Abs. 1 lit. f der DSGVO. Übermittlungen auf der Grundlage von Artikel 6 Abs. 1 lit. f DSGVO dürfen nur erfolgen, soweit dies zur Wahrung berechtigter Interessen der Bank oder Dritter erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Der Datenaustausch mit den Auskunftsteilen dient insbesondere zur Bonitätsprüfung.

Die Auskunftsteile verarbeiten die erhaltenen Daten und verwenden sie auch zum Zwecke der Profilbildung (Scoring), um ihren Vertragspartnern im Europäischen Wirtschaftsraum (EWR) und in der Schweiz sowie ggf. weiteren Drittländern (sofern zu diesen ein Angemessenheitsbeschluss der Europäischen Kommission besteht) Informationen unter anderem zur Beurteilung der Bonität von natürlichen Personen zu geben. Nähere Informationen zur Tätigkeit der hier aufgeführten Auskunftsteile können Sie unter

<https://www.schufa.de/global/datenschutz/>

<https://finance.arvato.com/icdinfoblatt>

<https://www.boniversum.de/eu-dsgvo/informationen-nach-eu-dsgvo-fuer-verbraucher/>

einsehen.

Als Kunde befreien Sie die Bank zudem vom Bankgeheimnis.

2. Hinweis auf die Verarbeitung und Übermittlung personenbezogener Daten durch die Bank und ihre Kooperationspartner zur Risikobewertung

Zur Vermeidung von Betrugsfällen im Rahmen eines Ratenkaufs bzw. Rechnungsaufs greift die Bank auf die Dienste von folgenden Unternehmen (im Folgenden "Kooperationspartnern zur Risikobewertung") zurück:

- Risk.Ident GmbH, Am Sandtorkai 50, 20457 Hamburg (Deutschland)
- BioCatch Ltd, 136 Menachem Begin Road, Tel Aviv, 6701104 (Israel)
- LexisNexis Risk Solutions (Europe) Ltd., 80 Harcourt St, Saint Kevin's, Dublin, D02 F449 (Irland)
- infoscore Consumer Data GmbH, Rheinstraße 99, 76532 Baden-Baden (Deutschland)
- Tink AB, Vasagatan 11, SE-111 20 Stockholm (Schweden)

2.1 Erhebung und Verarbeitung von Daten zur Betrugsprävention durch die Bank

Zur Vermeidung und Aufklärung von Betrugsfällen bzw. -versuchen im Rahmen eines Raten- bzw. Rechnungsaufs werden die von den "Kooperationspartnern zur Risikobewertung" gemäß den nachstehenden Bedingungen erhobenen und gespeicherten Daten (z.B. Standortdaten und Daten des verwendeten Endgeräts, wie Browserdaten und Bildschirmauflösung, Verhaltensinformationen) in eine Datenbank der Bank übermittelt. Diese Daten werden dort zusammen mit weiteren Daten wie Bestell- und Kontaktdaten gespeichert.

Im Rahmen des Bestellprozesses ruft die Bank aus dieser Datenbank Daten ab, um eine Risikobewertung zu jedem anfragenden Nutzer durchführen zu können. Die Bewertung erfolgt anhand individueller Risikofaktoren (z.B. Art des Eingabeverhaltens, Geo-Referenz oder Entfernung Adresse/Lieferort) und durch einen Abgleich mit früheren Bestellungen. Bei dem Abgleich werden mögliche Verbindungen zu anderen Nutzerdaten bewertet (z.B. Identitätsdiebstahl oder Übereinstimmung mit erkannten Betrugsfällen). Die Bewertung beruht

nicht auf einzelnen Daten, sondern auf einem in der Ausprägung der einzelnen Kriterien variablen Punktesystem. Rechtsgrundlage für die Datenverarbeitung ist unsere rechtliche Verpflichtung zur Verhinderung von Betrug nach Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 25 h Absatz 2 Kreditwesengesetz (KWG) sowie unser berechtigtes Interesse zur Verhinderung von Betrug gem. Art. 6 Abs. 1 lit. f DSGVO.

Als Betroffener der Bank können Sie Auskunft über die Sie betreffenden gespeicherten Daten erhalten und erfahren, aufgrund welcher Daten ein Raten- bzw. Rechnungskauf bewilligt oder abgelehnt wurde. Die betreffenden Daten der Datenbank werden regelmäßig überprüft und nicht mehr erforderliche Daten in der Regel nach vier Jahren gelöscht.

2.2 Erhebung und Verarbeitung von Daten zur Betrugsprävention durch die Risk.Ident GmbH

Die Risk.Ident GmbH erhebt, verarbeitet und nutzt mit Hilfe von Cookies und anderen Tracking-Technologien Daten zur Ermittlung des vom Besucher dieser Website verwendeten Endgeräts (Browserdaten, wie z.B. Browserversion, Auflösung etc.) und weiterer Daten über die Nutzung der Website (wie z.B. Namen bzw. Domain der Website, Durchführung einer Bestellung etc.). Soweit durch den Kooperationspartner IP- Adressen erhoben werden, werden diese Adressen vor der Verarbeitung und Nutzung gekürzt. Die Daten werden vom Kooperationspartner in einer Datenbank zur Betrugsprävention hinterlegt. In diese Datenbank werden auch von der Bank übermittelte Daten zu Endgeräten gespeichert, unter deren Verwendung es bereits zu betrügerischem Verhalten gekommen ist.

Rechtsgrundlage für die Datenverarbeitung ist unsere rechtliche Verpflichtung zur Verhinderung von Betrug nach Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 25 h Absatz 2 Kreditwesengesetz (KWG) sowie unser berechtigtes Interesse zur Verhinderung von Betrug gem. Art. 6 Abs. 1 lit. f DSGVO in Verbindung mit § 25 Abs. 2 Nr. 2 TDDDG. Die Löschfrist für die Datenbank beträgt zwei Jahre.

Im Rahmen eines Anmelde- bzw. Bestellprozesses auf dieser Website ruft die Bank aus dieser Datenbank eine Risikobewertung zum Endgerät des Nutzers ab. Diese Risikobewertung zur Wahrscheinlichkeit eines Betrugsversuchs berücksichtigt u.a., ob das Endgerät sich über verschiedene Service-Provider eingewählt hat, ob das Endgerät eine häufig wechselnde Geo-Referenz aufweist, wie viele Transaktionen über das Endgerät getätigt wurden und ob eine Proxy-Verbindung genutzt wird.

Zwischen der Bank und der Risk.Ident GmbH wurde ein Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO geschlossen. Nähere Informationen zu dem Dienstleister finden Sie auch unter:

<https://riskident.com/de/>

2.3 Erhebung und Verarbeitung von Daten zur Betrugsprävention durch die BioCatch Ltd.

Zur Vermeidung von Betrugsfällen im Rahmen eines Raten- bzw. Rechnungskaufs greift die Bank beim Betrieb dieser Website auf die Dienste der BioCatch Ltd. zurück.

Diese erhebt, verarbeitet und nutzt u.a. mit Hilfe von Cookies und anderen Tracking-Technologien Daten zur Ermittlung des Verhaltens des Besuchers der Website (z.B. Tipverhalten und Mausbewegungen). Die Daten werden von der BioCatch Ltd. ausgewertet und hinsichtlich der Vertrautheit der Eingaben zur Verhinderung von Identitätsdiebstahl bewertet.

Im Rahmen eines Anmelde- bzw. Bestellprozesses auf dieser Website ruft die Bank diese Informationen von der BioCatch Ltd. ab. Diese Risikobewertung wird von der Bank bei der

Berechnung zur Wahrscheinlichkeit eines Identitätsdiebstahls berücksichtigt, indem z.B. geprüft wird, ob Inhalte bei der Eingabe in das Eingabefeld kopiert wurden oder automatisiert bzw. maschinell eingegeben wurden.

Rechtsgrundlage für die Datenverarbeitung ist unsere rechtliche Verpflichtung zur Verhinderung von Betrug nach Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 25 h Absatz 2 Kreditwesengesetz (KWG) sowie unser berechtigtes Interesse zur Verhinderung von Betrug gem. Art. 6 Abs. 1 lit. f DSGVO in Verbindung mit § 25 Abs. 2 Nr. 2 TDDDG.

Die Löschfrist für die Datenbank beträgt 3 Jahre. Zwischen der Bank und der Risk.Ident GmbH wurde ein Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO geschlossen. Israel ist aufgrund eines gültigen Angemessenheitsbeschlusses der Europäischen Kommission ein sog. "sicheres Drittland" und weist ein angemessenes Datenschutzniveau auf. Nähere Informationen zu dem Dienstleister finden Sie auch unter:

<https://www.biocatch.com/>

2.4 Erhebung und Verarbeitung von Daten zur Betrugsprävention durch die LexisNexis Risk Solutions (Europe) Ltd.

Zur Vermeidung von Betrugsfällen im Rahmen eines Raten- bzw. Rechnungsaufs greift die Bank beim Betrieb dieser Website auf die Dienste der LexisNexis Risk Solutions (Europe) Ltd. zurück.

Diese erhebt, verarbeitet und nutzt u.a. Daten, die anhand der im Anmelde- bzw. Bestellprozess verwendeten E-Mail-Adresse und Domain vorliegen. Die Daten werden von der LexisNexis Risk Solutions (Europe) Ltd. ausgewertet und im Hinblick auf Identitätsdiebstahl bewertet.

Im Rahmen eines Anmelde- bzw. Bestellprozesses auf dieser Website ruft die Bank diese Informationen von der LexisNexis Risk Solutions (Europe) Ltd. ab. Diese Risikobewertung wird von der Bank bei der Berechnung der Wahrscheinlichkeit eines Identitätsdiebstahls berücksichtigt.

Rechtsgrundlage für die Datenverarbeitung ist unsere rechtliche Verpflichtung zur Verhinderung von Betrug nach Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 25 h Absatz 2 Kreditwesengesetz (KWG) sowie unser berechtigtes Interesse zur Verhinderung von Betrug gem. Art. 6 Abs. 1 lit. f DSGVO.

Zwischen der Bank und der LexisNexis Risk Solutions (Europe) Ltd. wurde ein Vertrag zur Dienstleistungserbringung geschlossen. Nähere Informationen zu dem Dienstleister finden Sie auch unter:

<https://risk.lexisnexis.com/>

2.5 Hinweis zur Teilnahme am Return-debit Prevention Pool der Infoscore Consumer Data GmbH

Im Rahmen des Antragsverfahrens gleicht die Bank Ihre Bankverbindungsdaten (IBAN und BIC) mit dem Return-debit Prevention Pool (RPP) der infoscore Consumer Data GmbH ab. Der RPP hat die Funktion einer Sperrdatei. Darüber hinaus wird die Bank im Falle der Nichteinlösung der Lastschrift, soweit zulässig, Ihre Bankverbindung (IBAN und BIC) in den RPP der infoscore Consumer Data GmbH einmelden, die diese Sperrung anderen Unternehmen, die am Auskunftsverfahren beteiligt sind, auf Anfrage übermittelt. Nach Bezahlung der Rücklastschrift wird die Bank diese Erledigung in den RPP melden.

2.6 Identitätsprüfung über den Kontoblick durch Tink AB

Bei einzelnen Anträgen ist ein Kontoblick notwendig, um Sie vor der Gefahr eines Identitätsdiebstahls zu schützen. Für den Kontoblick benötigen Sie einen Online-Banking-Zugang für Ihr in der Strecke genanntes Girokonto. Nach Angabe Ihrer Zugangsdaten prüft die Bank einmalig, ob Sie für das genannte Konto zugriffsberechtigt sind. Ihre Umsatzdaten werden nicht angefragt. Für die Identitätsprüfung über den Kontoblick greifen wir auf den Dienstleister Tink AB zurück. Weitergehende Datenschutzhinweise stellt Ihnen Tink AB in der Eingabemaske zur Verfügung.

Zwischen der Bank und Tink AB wurde ein Dienstleistungsvertrag geschlossen. Nähere Informationen zu dem Dienstleister finden Sie auch unter:

<https://tink.com/>

3. Durchführung des mTAN-Verfahrens

mTAN steht für "mobileTAN" und wird oft auch "SMS-TAN" oder "mobil TAN" genannt. Die Erhebung und Verarbeitung personenbezogener Daten im Zusammenhang mit dem mTAN-Verfahren dient dem Schutz vor typischen Gefahren im Online-Bereich wie etwa Identitätsdiebstahl. Dieses Verfahren wird beispielsweise auch im Online-Banking von vielen Kreditinstituten verwendet. Es funktioniert einfach über ein mobiles Endgerät mit SMS-Funktion. mTAN hat den Vorteil, dass die TANs zeitlich nur begrenzt gelten und nur einmalig für die angegebene Transaktion genutzt werden können. Das Verfahren wird grds. nur einmalig verwendet, um den Zugriff auf das Mobiltelefon des Ratenkauf- bzw. Rechnungsaufs-Kunden zu prüfen.

4. Datenübermittlung an den Händler

Ihre Antragsdaten, wie Name, Adresse, Kontaktdaten können dem Händler zur Abwicklung des Kaufes zur Verfügung gestellt werden. Dies dient bspw. zur Abwicklung der Warenauslieferung sowie zur Vermeidung von Betrug. Weiterhin wird dem Händler bei einem Kauf im stationären Ladengeschäft angezeigt, ob evtl. Zusatzkäufe möglich sind. Dies dient dazu, Sie als Kunden optimal beraten zu können. Der Händler ist für die Datenverarbeitung, inkl. der Löschung der an ihn übermittelten Daten, verantwortlich.

IV. Inwieweit werden Ihre Daten zur Profilbildung bzw. zum Scoring genutzt?

Die Bank verarbeitet Daten auch automatisiert mit dem Ziel, bestimmte persönliche Aspekte zu bewerten beispielsweise in folgenden Fällen:

- Gezielte und bedarfsgerechte Kommunikation und Werbung, um Kunden Angebote machen zu können, die interessant und auf ihre Bedürfnisse zugeschnitten sind, sofern kein Werbewiderspruch des jeweiligen Kunden vorliegt.
- Zur Beurteilung der Kreditwürdigkeit sowie zur Bewertung der Geschäftsbeziehung nutzt die Bank Scoring.
- Bekämpfung von Geldwäsche, Terrorismusfinanzierung und anderen vermögensgefährdenden Straftaten, wie Identitätsdiebstahl. Zur Erfüllung dieser gesetzlichen Pflichten werden auch Datenauswertungen (unter anderem im Zahlungsverkehr) vorgenommen, um Kundengelder der Bank zu schützen.

Jeder Kunde oder Interessent hat das Recht, eine persönliche Überprüfung der automatisierten Einzelentscheidung zu verlangen. Das Scoring beruht auf einem mathematisch-statistisch anerkannten und bewährten Verfahren und ist für den Abschluss oder die Erfüllung eines

Produktangebotes erforderlich. Die errechneten Score-Werte unterstützen die Bank bei ihrer Kundensegmentierung und somit bei der Entscheidungsfindung für die Genehmigung eines Produktangebotes und gehen in das laufende Risikomanagement ein.

Hinweise zur Bonitäts- sowie Identitätsprüfung im Rahmen des Angebotsprozesses für den „Ratenkauf“ und den „Rechnungskauf“ Für die Erstellung eines Angebots für den Raten- bzw. Rechnungskauf verwendet die Bank eine automatisierte Bonitätsentscheidung und Identitätsprüfung. Hierbei nutzt die Bank zur Bewertung Ihrer Bonität u.a. einen von der SCHUFA gelieferten Scorewert. Zudem fließen Daten von Auskunftsteilen sowie gegebenenfalls eigene Erfahrungen, die die Bank mit Ihnen als Kunde gemacht hat, ein. Die Bank nutzt in diesem Zusammenhang auch bonitätsrelevante Informationen (Verifizierung der Namensangaben, der E-Mail-Adresse und der Adresse inklusive Prüfung der Zustellbarkeit) zum bisherigen Zahlungsverhalten sowie Informationen zur Beurteilung des Zahlungsausfallrisikos auf Basis mathematisch-statistischer Verfahren unter Verwendung von Anschriftendaten von der Infoscore Consumer Data GmbH.

Das Verfahren ist auf vergangenheitsbezogenen Werten konzipiert. Die Entscheidung beruht somit nicht auf einem einzelnen Merkmal, sondern auf einem in der Ausprägung der einzelnen Kriterien variablen Punktesystem.

Sie haben die Möglichkeit, sich mit Ihren Einwänden gegen das Ergebnis der Prüfungen direkt an die Bank zu wenden. Sie erreichen die Bank unter folgender Adresse: TeamBank AG, Beschwerdemanagement, Beuthener Straße 25, 90471 Nürnberg, E-Mail: service@easycredit.de

V. Wer bekommt Ihre Daten?

Innerhalb der Bank erhalten diejenigen Stellen Zugriff auf Ihre Daten, die diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten brauchen. Auch von uns eingesetzte Auftragsverarbeiter (Art. 28 DSGVO) können zu diesen genannten Zwecken Daten erhalten. Dies sind Unternehmen in den Kategorien kreditwirtschaftliche Leistungen, IT-Dienstleistungen, Logistik, Druckdienstleistungen, Telekommunikation, Inkasso, Beratung und Consulting sowie Vertrieb und Marketing. Stellen, mit denen wir bei der Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten zusammenarbeiten (z. B. Gerichte, Gerichtsvollzieher, Drittschuldner, Rechtsanwälte, Schuldnerberatungen, Betreuer), können zu diesen Zwecken Daten erhalten. Im Hinblick auf die Datenweitergabe an Empfänger außerhalb der Bank ist zunächst zu beachten, dass wir zur Verschwiegenheit über alle kundenbezogenen Tatsachen und Wertungen verpflichtet sind, von denen wir Kenntnis erlangen (Bankgeheimnis). Informationen über Sie dürfen wir nur weitergeben, wenn bspw. gesetzliche Bestimmungen dies gebieten oder Sie Ihre Zustimmung gegeben haben.

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 / behördlichen Verpflichtung
- Andere Kredit- und Finanzdienstleistungsinstitute oder vergleichbare Einrichtungen, an die wir zur Durchführung der Geschäftsbeziehung keine personenbezogenen Daten übermitteln (je nach Vertrag: z. B. Korrespondenzbanken, Auskunftsteile)

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

Einwilligung befreit haben.

Im Rahmen der Leistungserbringung des Raten- bzw. Rechnungsaufschlags können die folgenden konkreten Stellen Ihre Daten erhalten:

- Alle Stellen, die in diesen Datenschutzhinweisen unter III. aufgeführt sind;
- Händler, bei dem der Raten- oder Rechnungsaufschlag als Zahlungsmittel ausgewählt wurde;
- Atos Information Technology GmbH, Otto-Hahn-Ring 6, 81739 München (IT-Dienstleister)
- Deutscher Genossenschafts-Verlag eG, Leipziger Straße 35, 65191 Wiesbaden (IT-Dienstleister)
- Dun & Bradstreet Deutschland GmbH, Robert-Bosch-Str. 11, 64293 Darmstadt (Adressdienstleister)
- DYMATRIX CONSULTING GROUP GmbH (Marketingdienstleister)
- Microsoft Ireland Operations Limited, Leopardstown, Dublin 18 D18 P521, Irland (IT-Dienstleister)
- Noris Network AG, Thomas-Mann-Straße 16-20, 90471 Nürnberg (IT-Dienstleister)
- Schwäbisch Hall Facility Management GmbH, Crailsheimer Straße 52, 74523 Schwäbisch Hall (Druckdienstleister)

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

Soweit die Bank personenbezogene Daten an einen Dienstleister übermittelt und dieser seinen Sitz in ein Drittland i.S.d. DSGVO (d.h. außerhalb der EU/ des EWR) hat, stellt die Bank sicher, dass der/die Empfänger der Daten ein angemessenes Datenschutzniveau gewährleistet/n. Wird eine Datenübermittlung von einem Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO umfasst, bedarf es keinen weiteren Schutzmaßnahmen mehr. Datenübermittlungen an Dienstleister in Drittländer ohne Angemessenheitsbeschluss oder an US-Unternehmen, die nicht nach dem EU-U.S. Data Privacy Framework zertifiziert sind, benötigen geeignete Garantien für die Datenübermittlungen, wie z. B. Standardvertragsklauseln oder Binding Corporate Rules (Art. 46, 47 DSGVO).

VII. Welche Betroffenenrechte haben Sie?

Jeder Betroffene hat das Recht auf Auskunft nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO, das Recht auf Löschung nach Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO sowie das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO. Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Art. 77 DSGVO i.V.m. § 19 BDSG).

1. Einzelfallbezogenes Widerspruchsrecht

Jeder Kunde hat das Recht aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen die Verarbeitung seiner personenbezogenen Daten, die aufgrund einer Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling im Sinne von Art. 4 Nr. 4 DSGVO. Im Falle des Widerspruchs wird die Bank die personenbezogenen Daten nicht mehr verarbeiten, es sei denn, die Bank kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die

Interessen, Rechte und Freiheiten der Kunden oder Interessenten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder die Bank ist zur Datenverarbeitung aufgrund von Gesetzen, Verordnungen oder sonstigen hoheitlichen Maßnahmen dazu verpflichtet. Bis zum Zeitpunkt des Widerspruchs erfolgte Datenverarbeitungen bleiben dabei rechtmäßig. Im Falle eines wirksamen Widerspruchs kann die Bank die Beendigung von einzelnen Verträgen oder der Geschäftsbeziehung insgesamt erwägen.

2. Widerspruchsrecht gegen Verarbeitung von Daten zu Werbezwecken

Die Bank verarbeitet personenbezogene Kundendaten in Einzelfällen, um Direktwerbung zu betreiben. Jeder Kunde hat das Recht, jederzeit Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Widerspricht der Kunde der Verarbeitung für Zwecke der Direktwerbung, so wird die Bank seine personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten. Bis zum Zeitpunkt des Widerrufs erfolgte Datenverarbeitungen bleiben dabei rechtmäßig. Der Widerspruch kann formfrei erfolgen und kann über den Kundenservice der Bank (z. B. über den C24 Bank App Bereich „Meine Nachrichten“) erfolgen.

VIII. Wie lange werden Ihre Daten gespeichert?

Wir verarbeiten und speichern Ihre personenbezogenen Daten grundsätzlich für die Dauer unserer Geschäftsbeziehung, was beispielsweise auch die Anbahnung und die Abwicklung eines Vertrages umfasst.

Darüber hinaus unterliegen wir verschiedenen Aufbewahrungs- und Dokumentationspflichten, die sich unter anderem aus dem Handelsgesetzbuch (§§ 238, 257 Abs. 4 HGB), der Abgabenordnung (§ 147 Abs. 3, 4 AO), dem Kreditwesengesetz (§ 25 a Abs. 1 Satz 6 Nr. 2 KWG) und dem Geldwäschegesetz (§ 8 Abs. 3 GWG) 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 drei Jahre, in gewissen Fällen aber auch bis zu dreißig Jahre betragen können.