Datenschutzerklärung

Mit dieser Datenschutzerklärung informiert die C24 Bank GmbH (im Folgenden „Bank“) über die Erhebung, Nutzung und Verarbeitung von personenbezogenen Daten bei der Nutzung der C24 Bank App und der C24 Bank Webseite c24.de (im Folgenden „Webseite”, gemeinschaftlich bezeichnet: „Dienste”). Soweit Informationen sich ausschließlich auf die C24 Bank App oder Webseite beziehen, weist die Bank ausdrücklich darauf hin.

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 Bank verarbeitet personenbezogene Daten, die sie im Rahmen der Geschäftsbeziehung mit Kunden und Interessenten sowie von Besuchern der Website erhält. Zur Erbringung ihrer Dienstleistung verarbeitet die Bank auch personenbezogene Daten, die sie von Dritten (z. B. SCHUFA) zulässigerweise (z. B. zur Ausführung von Aufträgen, zur Erfüllung von Verträgen oder aufgrund einer erteilten Einwilligung) erhalten hat. Außerdem verarbeitet die Bank personenbezogene Daten, die sie aus öffentlich zugänglichen Quellen (z. B. Schuldnerverzeichnisse, Handels- und Vereinsregister, Presse, Medien, Internet) zulässigerweise bezogen hat und verarbeiten darf.

Bei Abschluss und Nutzung von Bankprodukten oder Produkten von Bankpartnern können zusätzlich zu den vorgenannten Daten weitere personenbezogene Daten erhoben, verarbeitet und gespeichert werden. Details dazu sind unter Gliederungspunkt III. dieser Bedingungen zu finden.

I. Verantwortliche Stelle

Verantwortliche Stelle für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten ist die:

C24 Bank GmbH
Neue Mainzer Straße 14-18
60311 Frankfurt am Main

Die Bank hat einen Datenschutzbeauftragten bestellt, der unter obiger Adresse oder datenschutz@c24.de zu erreichen ist.

Nähere Informationen zur Bank sind im Impressum auf www.c24.de zu finden.

II. Zweck der Datenverarbeitung und Rechtsgrundlage

Die Bank verarbeitet personenbezogene Daten im Einklang mit den Bestimmungen der Verordnung EU 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DSGVO) und dem Bundesdatenschutzgesetz (BDSG).

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

Soweit die Bank eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke erhalten hat, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis der jeweiligen Einwilligung gegeben. Eine erteilte Einwilligung kann jederzeit über den Kundenservice innerhalb der C24 Bank App bzw. unter kundenservice@c24.de widerrufen werden. Der Widerruf wirkt erst für die Zukunft, d. h. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind von dem Widerruf nicht betroffen.

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

Die Verarbeitung personenbezogener Daten erfolgt zur Erbringung von Bankgeschäften und Finanzdienstleistungen, 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. Zu welchem Zweck die Daten verarbeitet werden, ist 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. Gesetzliche Vorgaben (Art. 6 Abs. 1 lit. c DSGVO) oder öffentliches Interesse (Art. 6 Abs. 1 lit. e DSGVO)

Die Bank unterliegt gesetzlichen Anforderungen einschließlich bankaufsichtsrechtlicher Vorgaben, die es zu beachten gilt. So können Datenverarbeitungen z. B. aufgrund des Kreditwesengesetzes, Geldwäschegesetzes oder von Steuergesetzen gerechtfertigt sein. Auch Anforderungen der Europäischen Zentralbank, der Europäischen Bankenaufsicht, der Deutschen Bundesbank und der Bundesanstalt für Finanzdienstleistungsaufsicht berechtigen die Bank zur Datenverarbeitung zur Erfüllung aufsichtsrechtlicher Vorgaben. Die Zwecke der Verarbeitung sind dabei u. a.: Identitäts- und Altersprüfung, Betrugs- und Geldwäscheprävention, Kreditwürdigkeitsprüfung, steuerrechtliche Kontroll- und Meldepflichten und Bewertung von Risiken der Bank.

4. Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO)

Soweit erforderlich, verarbeitet die Bank personenbezogene Daten über die eigentliche Erfüllung des Vertrages hinaus zur Wahrung berechtigter Interessen von der Bank oder Dritten.

Beispiele:

- Einsicht in und Datenaustausch mit Auskunfteien (z. B. SCHUFA) zur Ermittlung von Bonitäts- bzw. Ausfallrisiken und des Bedarfs beim Pfändungsschutzkonto oder Basiskonto
- Prüfung und Optimierung von Verfahren zur Bedarfsanalyse und zu direkter Kundenansprache; inkl. Kundensegmentierungen und Berechnung von Abschlusswahrscheinlichkeiten
- Werbung oder Markt- und Meinungsforschung, soweit der Verarbeitung der Daten nicht widersprochen wurde
- Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten
- Sicherstellung der IT-Sicherheit und des IT-Betriebs
- Abwendung und Aufklärung von Straftaten
- Maßnahmen zur Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten
- Risikosteuerung in der Bank
- Konzerninterne Vertragsverwaltungszwecke

5. Verarbeitung zu anderen Zwecken durch nichtöffentliche Stellen (§ 24 BDSG)

Die Bank kann personenbezogene Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, zur Abwehr von Gefahren, Verfolgung von Straftaten oder zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche verarbeiten sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

6. Auftragsverarbeitung im Auftrag der Bank (Art. 28 DSGVO)

Erfolgt eine Verarbeitung personenbezogener Daten im Auftrag der Bank, schließt die Bank mit dem Auftragsverarbeiter einen gesonderten Vertrag zu dieser Verarbeitung. Dieser Vertrag dient der Einhaltung der Vorgaben der DSGVO und bestimmt hinreichende Garantien zur Durchführung geeigneter technischer und organisatorischer Maßnahmen, welche den Schutz der Rechte der von der Verarbeitung betroffenen Personen gewährleistet.

III. Datenverarbeitung im Rahmen der C24 Produkte (jeweils, soweit anwendbar)

7. Datenerhebung und Verarbeitung bei Eröffnung und Nutzung eines C24 Girokontos sowie weiterer Bankdienstleistungen

Zum Zwecke der Eröffnung und Nutzung eines C24 Girokontos, der Beantragung sowie des Abschlusses von Kreditverträgen, der Entgegennahme von Einlagen (im Folgenden gemeinschaftlich bezeichnet: „Bankprodukte") sowie bei der Nutzung der Dienste der Bank werden bei der Bank unter anderem die folgenden Daten im Sinne des Art. 4 Nr. 2 DSGVO verarbeitet:

- Identifizierungsdaten inkl. Vor- und Nachname, Geburtsdatum, Geburtsort, E-Mail-Adresse, Staatsangehörigkeit, Meldeadresse und Steuer-ID
- Mobilnummer
- Identifikationsdokument inklusive (siehe hierzu ausführlich in Nr. V. dieser Bedingungen), Typ des Ausweisdokuments, Ausstellungsdatum, ID-Nummer und ausstellende Behörde
- Beruflicher Status
- Verschlüsselte Kontodaten, Passwort, PIN und die über das Mobilgerät bereitgestellten verschlüsselten Token zur Authentifizierung durch Gesichtserkennung und/oder Fingerabdruck auf dem jeweiligen Gerät.

Bei Nichtbereitstellung dieser Daten ist eine Nutzung der Bankprodukte nicht möglich.

Darüber hinaus werden weitere personenbezogene oder personenbeziehbare Kategorien von Daten erhoben und verarbeitet:

- Technische Daten des Endgerätes (Mobiltelefon, PC, Tablet), mit dem die C24 Bank App oder die Webseite genutzt wird und die dieses möglichst eindeutig identifizieren („Gerätedaten"), sofern die Übermittlung dieser Gerätedaten seitens des Endgerätes nicht unterbunden oder teilweise eingeschränkt wird. Zu den Gerätedaten gehören insbesondere Seriennummer, Gerätehersteller, Gerätetyp, Geräteeigenschaften wie Speicherplatz oder Displayauflösung, IP-Adresse, Mobilfunkbetreiber, Netzwerkinformationen, Betriebssystem- und Versionsinformationen, Browsertyp und -version, IDFA (Identifier for Advertisers) oder Android-ID und weitere Informationen zu den Einstellungen des Mobilfunkgerätes des Kunden.
- Informationen über die Nutzung und Verwaltung der C24 Bank App und insbesondere des C24 Girokontos sowie die Umstände der Nutzung der C24 Bank App einschließlich der benutzten Version der C24 Bank App
- Einzelheiten der Transaktionen, die der Kunde über die C24 Bank App und die C24 Mastercard ausführt
- Zahlungs- und Bankkontoinformationen
- Daten aus der Erfüllung einer vertraglichen Verpflichtung der C24 Bank (zum Beispiel Umsatzdaten aus dem Einlagen- / Festgeld- und Kreditgeschäft)
- Dokumentationsdaten (z.B. Beratungsprotokolle)
- Hochgeladene Bilder zur Verwendung als Profilbild innerhalb der eigenen App und nach Einwilligung auch als Erkennungsmerkmal in der App von anderen C24 Bank App Nutzern.

Die Verarbeitung von personenbezogenen Daten variiert in den verschiedenen Bankprodukten. Dies gilt insbesondere für die Nutzung der Girokontomodelle C24 Smart-, C24 Plus- und C24 Maxkonto und auch bei der Entscheidung des Kunden zur Nutzung der Produkte von Bankpartnern, z. B. zur optionalen Teilnahme des C24 Punkte Programms als Teil des CHECK24 Smily Treueprogramms (siehe Nr. 8 in diesen Bedingungen). Sofern sich eine Verarbeitung nur auf bestimmte Bankprodukte bezieht, wird darauf gesondert hingewiesen.

Zum Zwecke der Abwicklung von Zahlungsdiensten nimmt die Bank Auftragsdaten entgegen und übermittelt auftragsgemäß (siehe "Bedingungen für den Überweisungsverkehr") und aufgrund des Art. 4 GeldtransferVO Zahlungsverkehrsdaten an Zahler, Zahlungsempfänger und deren Banken.

Die Geldtransferverordnung (GTVO) sieht - abhängig von der Betragshöhe und einem Drittstaatenbezug - vor, dass bei Überweisungen innerhalb der Mitgliedsstaaten der Europäischen Union (EU) von den verfügbaren Auftraggeberdaten zumindest die Kontonummer oder eine kundenbezogene Identifikationsnummer zu übermitteln ist. Sofern es für eine ordnungsgemäße Abwicklung des Auslandszahlungsverkehrs erforderlich ist, wird die Bank im Kundeninteresse die kompletten Auftraggeberdaten weiterleiten. Bei Geldtransfers an einen Begünstigten, dessen Zahlungsverkehrsdienstleister seinen Sitz außerhalb der EU hat, wird der vollständige Auftraggeberdatensatz übermittelt.

8. C24 Punkte Programm als Teil des CHECK24 Treueprogramms Smily

Das C24 Punkte Programm als Teil des CHECK24 Treueprogramms Smily, welches von der CHECK24 GmbH, Erika-Mann-Str. 62-66 in 80636 München (im Folgenden „CHECK24 GmbH") betrieben, ist ein optional wählbarer Vertragsbestandteil für die Kontomodelle C24 Smartkonto, C24 Pluskonto und C24 Maxkonto.

Für Zahlungen mit der C24 Mastercard vergibt die Bank Prämienpunkte, die auf dem CHECK24 Smily Punktekonto des Kunden gesondert gutgeschrieben werden.

Um am C24 Punkte Programm als Teil des CHECK24 Treueprogramms Smily teilnehmen zu können, sind folgende Voraussetzungen unabdingbar erforderlich:

- Ein aktives CHECK24 Kundenkonto (siehe Nr. 11 in diesen Bedingungen), welches von der CHECK24 GmbH verwaltet wird
- Die Zustimmung zu den der Teilnahmebedingungen zum CHECK24 Treueprogramm Smily
- Eine Verknüpfung des CHECK24 Kundenkontos mit der C24 Bank App

Die Anmeldung zum C24 Punkte Programm als Teil des CHECK24 Punkte Programms erfolgt innerhalb der C24 Bank App.

Zur Erfüllung der vertraglichen Pflichten (Art. 6 Abs. 1 lit. b DSGVO) aus den Teilnahmebedingungen zum C24 Punkteprogramm als Teil des CHECK24 Treueprogramms Smily werden persönliche und transaktionsbezogene Daten von der Bank an die CHECK24 GmbH weitergeleitet, u. a. die Verbuchung des Einkaufs mit der C24 Mastercard.

Dies beinhaltet die Übermittlung einer Zuordnungsnummer und den Monatsendsaldo. Verantwortlicher für die dort stattfindende Datenverarbeitung ist die CHECK24 GmbH.

Die Bank übermittelt zudem personenbezogene Daten an Kooperationspartner des C24 Punkte Programms als Teil des CHECK24 Treueprogramms Smily, um eine korrekte Abrechnung der bei dem jeweiligen Partner generierten Punkte zu gewährleisten und nachvollziehen zu können, z. B. im Beschwerdefall. Hierbei werden folgende Daten an den Partner übermittelt: Name, Vorname, Transaktionsdatum, Preis und Referenznummer.

Die Datenübermittlung endet mit der Beendigung der Mitgliedschaft am C24 Punkte Programm als Teil des CHECK24 Treueprogramms Smily.

9. Kontoschutzbrief Plus der ARAG AG

Inhaber eines kostenpflichtigen C24 Plus- oder C24 Maxkontos der Bank partizipieren an einem Gruppenversicherungsvertrag der Bank mit der ARAG Allgemeine Versicherungs-Aktiengesellschaft. Versichert sind Konto- und Kartenverbindungen, die zu Geldinstituten in Deutschland vom Kunden unterhalten werden. Dieser Versicherungsschutz sichert die Kunden in vielen Fällen der Internetkriminalität ab. Es bietet im Kontoschutz zusätzlich Schutz bei Skimming-Betrug und im Käuferschutz bei Einkäufen von Waren im Internet.

Zur Prüfung der Berechtigung und mithin zur Erfüllung des Vertragsverhältnisses (Art. 6 Abs. 1 lit. b DSGVO) übermittelt die Bank an die ARAG monatlich in elektronischer Form ein Verzeichnis der aktivierten Konto- & Käuferschutz Plus Verträge. Dieses Verzeichnis enthält:

- E-Mail-Adresse des Kunden
- Datum der erstmaligen Aktivierung des Konto- & Käuferschutz Plus-Vertrages
- Ablaufdatum des Konto- & Käuferschutz Plus-Vertrages.

Im Schadensfall werden weitere Kontakt- und Kontodaten nach vorheriger Zustimmung des Kunden an die ARAG übermittelt.

10. CHECK24 Treueprogramm Smily Level-3-Mitgliedschaft

Kunden des C24 Maxkontos erhalten automatisch eine Level-3-Mitgliedschaft im CHECK24 Treueprogramm Smily, sofern sie ihr CHECK24 Kundenkonto mit ihrem C24 Girokonto verknüpft haben und den Teilnahmebedingungen für das Treueprogramm Smily haben.

Die Verarbeitung der für die Kundenkonto-Verknüpfung erforderlichen Daten erfolgt zur Erfüllung des Vertrages (Art. 6 Abs. 1 lit. b DSGVO). Die Bank verarbeitet hierbei die Daten, die zur Verknüpfung des CHECK24 Kundenkontos (siehe Nr. 11 dieser Bedingungen) erforderlich sind. Die Verarbeitung und Übermittlung dieser Daten dient der Erfüllung des Vertrages (Art. 6 Abs. 1 lit. b DSGVO).Die zugehörigen Datenschutzhinweise der CHECK24 Vergleichsportal Reise GmbH finden Sie hier.

Mit Kündigung des C24 Maxkontos oder Beendigung der Teilnahme am CHECK24 Treueprogramm Smily endet die durch die Bank begründete Berechtigung auf die Level-3-Mitgliedschaft im CHECK24 Treueprogramm Smily gleichermaßen.

11. Einbindung des CHECK24 Kundenkontos

Für unterschiedliche Funktionen ist eine Einbindung eines aktiven CHECK24 Kundenkontos bei der CHECK24 GmbH erforderlich (insb. das C24 Punkteprogramm als Teil des CHECK24 Treueprogramms Smily und die Vertragserkennung). Für das CHECK24 Kundenkonto gelten eigene Nutzungsbedingungen seitens der CHECK24 GmbH. Die zugehörigen Datenschutzhinweise der CHECK24 GmbH finden Sie hier.

Sofern bereits ein CHECK24 Kundenkonto besteht, ist es möglich, einige der dort vorhandenen Kundendaten für die Girokontoeröffnung zu übertragen. Hierzu findet bei der Eingabe der E-Mail-Adresse während der Kontoeröffnung eine Überprüfung dieser E-Mail-Adresse gegenüber der CHECK24 GmbH statt. Bei einer Übereinstimmung wird der Kunde darauf hingewiesen, dass er sich mit seinen Zugangsdaten für das CHECK24 Kundenkonto anmelden und seine Daten (E-Mail-Adresse, Name, Anschrift und Geburtsdatum) übertragen lassen kann. Die Überprüfung der E-Mail-Adresse dient der Vertragserfüllung zum CHECK24 Kundenkonto (Art. 6 Abs. 1 lit. b DSGVO), so dass der Inhaber eines CHECK24 Kundenkontos seine Stammdaten vorfindet und er weitere Transaktionen einfach durchführen kann. Die Überprüfung der E-Mail-Adresse führt zu keiner Speicherung seitens der CHECK24 GmbH.

Bei der Verknüpfung des CHECK24 Kundenkontos verarbeitet die Bank temporär zur Überprüfung der Existenz des Kundenkontos und zum Abgleich der Daten eine eindeutige, automatisch generierte Zuordnungsnummer.

Die Verantwortung für die Datenverarbeitung innerhalb des CHECK24 Treueprogramms Smily und für das CHECK24 Kundenkonto liegt allein bei der CHECK24 GmbH.

12. Kontowechselservice

Die Bank bietet Kunden einen optional wählbaren Kontowechselservice an, der hauptsächlich über die CHECK24 Vergleichsportal Karten und Konten GmbH, Erika-Mann-Str. 62-66 in 80636 München oder vereinzelt über die finleap connect GmbH, Gaußstraße 190c in 22765 Hamburg (im Folgenden „finleap“) bereitgestellt wird und für die Kunden kostenlos ist. Bestandteil dieses Services ist die Bereitstellung einer Webseite, mithilfe derer die Kunden externe Zahlungskonten verbinden und einen Kontowechsel zur Bank durchführen können.

Um den Kontowechselservice einfacher nutzen zu können, übermittelt die Bank an die CHECK24 Vergleichsportal Karten und Konten GmbH bzw. an finleap hierzu einmalig und nur auf Kundenwunsch bereits vorliegende personenbezogene Daten des jeweiligen Kunden (insbesondere Name, Anschrift, IBAN und BIC des C24 Girokontos) sowie Daten zum CHECK24 Kundenkonto (insbesondere Identifikationsnummer des Kundenkontos).

Diese Datenübermittlung ist Teil der Vertragsanbahnung zwischen der CHECK24 Vergleichsportal Karten und Konten GmbH und dem Kunden bzw. zwischen finleap und dem Kunden und wird über Art. 6 Abs. 1 lit. b DSGVO legitimiert.

Für die Durchführung des Kontowechselservices und die Einbindung der Finanzinformationen von online verfügbaren Zahlungskonten ist ausschließlich die CHECK24 Vergleichsportal Karten und Konten GmbH bzw. finleap verantwortlich. Der Kunde schließt hierzu eine eigenständige Vereinbarung mit der CHECK24 Vergleichsportal Karten und Konten GmbH bzw. finleap ab. Folglich agiert die CHECK24 Vergleichsportal Karten und Konten GmbH bzw. finleap eigenständig als Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO gegenüber dem Kunden.

Die Datenschutzerklärung der CHECK24 Vergleichsportal Karten und Konten GmbH kann unter folgendem Link eingesehen werden: Datenschutzerklärung der CHECK24 Vergleichsportal Karten und Konten GmbH

Die Datenschutzerklärung der finleap connect GmbH ist unter folgendem Link abrufbar: Datenschutzerklärung der finleap connect GmbH

13. Fotoüberweisung

„Fotoüberweisung“ wird gemäß Nr. 3 Abs. (2) der „Bedingungen für den Überweisungsverkehr“ den Kunden als optional wählbare Dienstleistung zur Verfügung gestellt. Hierbei werden Überweisungsdaten (z. B. Zahlungsempfänger, IBAN, BIC, Rechnungsbetrag, Verwendungszweck) vom Kunden als Bild-Datei an die Bank übermittelt und dort mittels einer Texterkennungssoftware automatisiert ausgelesen und in eine Überweisungsmaske eingetragen.

Korrigiert der Kunde die aus der Bilddatei erkannten Überweisungsdaten nachträglich, werden die Erkenntnisse aus diesen Eingaben/Änderungen in nicht personalisierter Weise genutzt, um in Kombination mit den nicht-personalisierten Erkenntnissen aus der vorübergehend gespeicherten Bild-/Textdatei und den ursprünglich ausgelesenen Informationen den automatischen Erkennungsmechanismus zu trainieren und zukünftig Fehler zu vermeiden. Die Bank weist darauf hin, dass sich aus den für die Foto-Überweisung genutzten Text-/Bilddateien möglicherweise Rückschlüsse auf sensible personenbezogene Daten wie religiöse oder weltanschauliche Überzeugungen, politische Meinung, Herkunft, Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung des Kunden ergeben können.

14. Datenverarbeitung im Rahmen von geteilten Konten

Die Verwendung von geteilten Konten ist optional wählbar und erfolgt gemäß den „Bedingungen für geteilte Konten“. Hierfür verarbeitet die Bank gemäß Art. 6 Abs. 1 lit. b DSGVO Daten zur Identifizierung der Mitglieder eines geteilten Kontos sowie Transaktionsdaten.

Zur Nutzung eines geteilten Kontos lädt der Kontoinhaber (im Folgenden „Besitzer“) weitere Personen (im Folgenden „Teilnehmer“) dazu ein, das Hauptkonto oder ausgewählte Pockets des Besitzers gemeinsam zu benutzen.

Die Einladung erfolgt, indem der Besitzer ihm bekannte Mobilfunknummern oder E-Mail-Adressen der eingeladenen Personen in der C24 Bank App erfasst und über diese einen Link oder einen QR-Code generiert bekommt. Dieser Link oder QR-Code kann vom Besitzer über dessen Mobilgerät eigenständig und ohne Mitwirkung der C24 Bank App versendet werden.

Geteilte Konten können ausschließlich von Kunden der Bank verwendet werden.

Nach Annahme der Einladung durch den Teilnehmer und der darauffolgenden Bestätigung durch den Besitzer, kann das geteilte Konto oder Pocket vom Teilnehmer aktiv im Sinne einer Kontovollmacht verwendet werden inkl. der Möglichkeit, Einladungen an weitere Teilnehmer zu versenden.

Aktive Teilnehmer können sowohl alle Transaktionsdetails als auch die Namen aller anderen Teilnehmer einsehen.

Die Teilnahme an einem geteilten Konto kann jederzeit durch den Besitzer oder den Teilnehmer in der C24 Bank App beendet werden. Hierbei verliert der Teilnehmer alle Zugriffsrechte auf dieses geteilte Konto, verbleibt aber weiterhin als Kunde der Bank und kann eventuell vorhandene andere geteilte Konten weiter nutzen.

15. Multibanking

Die optionale Einbindung und der regelmäßige Abruf von Fremdbankkonten in die C24 Bank App erfolgt gemäß den „Bedingungen für das Girokonto“.

Hierbei werden die jeweils aktuellen Konto- und Transaktionsinformationen der eingebundenen Konten (z. B. IBAN, Bankname, Kontostand, Umsätze, Buchungsdatum, Verwendungszweck, Empfänger-/Sendername, Empfänger-/Sender IBAN, Empfänger Gläubiger ID, Mandatsreferenz) erfasst, strukturiert zu einer Vermögensübersicht aufbereitet und in der C24 Bank App dargestellt. Darüber hinaus werden weitere, zwingend für die Bereitstellung dieser Dienstleistung erforderlichen Daten verarbeitet, z. B Einbindungsdatum, Konto-Zugangsdaten, Status der automatischen Aktualisierung.

Zusätzlich zur bereitgestellten Vermögensübersicht werden die abgerufenen Kontoumsätze des Kunden (Einnahmen und Ausgaben) nach Maßgabe von Nr. 3 Abs. 15 und 16 der Bedingungen für das Girokonto in eine Umsatzkategorisierung und Vertragserkennung integriert und dem Kunden in Form einer gesamthaften Analyse nach voreingestellten und individuell durch den Kunden vergebenen Regeln aggregiert zur Verfügung gestellt.

16. Vertragserkennung

Es wird zwischen einfacher und erweiterter Vertragserkennung unterschieden. Die Aktivierung der einfachen Vertragserkennung innerhalb der C24 Bank App erfolgt gemäß den Bedingungen für das Girokonto. Dem Nutzer ist es möglich, die Funktion nachträglich zu deaktivieren. Darüber hinaus kann der Kunde zusätzliche Vertragsfunktionen, genannt erweiterte Vertragserkennung, aktivieren, indem er den „Bedingungen für die erweiterte Vertragserkennung“ zustimmt. Erst in diesem Zuge kommt es bei der Inanspruchnahme zu einem regelmäßigen Datenaustausch mit den Unternehmen innerhalb der CHECK24 Gruppe (siehe „Bedingungen für die erweiterte Vertragserkennung“)
Insbesondere sind folgende Dienstleistungen Teil der einfachen und erweiterten Vertragserkennung:

(1) Einfache Vertragserkennung

Im Rahmen der einfachen Vertragserkennung werden neben dem eigenen C24 Girokonto sämtliche über das Multibanking (siehe Nummer 15 dieser Bedingungen) eingebundenen Fremdkonten auf Verträge/Dauerschuldverhältnisse analysiert und diese bestimmten Vertragstypen (z.B. Strom & Gas, Versicherung, Telekommunikation etc.) zugeordnet. Diese werden dem Kunden in der C24 Bank App in einer Vertragsübersicht angezeigt. Es kommt im Zuge dieser Funktion zu keinem personenbezogenen Datenaustausch mit den Unternehmen innerhalb der CHECK24 Gruppe.

(2) Erweiterte Vertragserkennung

Mit Aktivierung der erweiterten Vertragserkennung erhält der Kunde zusätzlich folgende Dienstleistungen.

Die Bank ruft kontinuierlich mit jedem Abruf der Kontoinformation alle im Kontext des CHECK24 Kundenkontos (siehe Nummer 11 dieser Bedingungen) abgeschlossenen Verträge bei den Unternehmen der CHECK24 Gruppe ab und speichert diese. Dasselbe gilt für den Fall bei aktivem Bestehen eines „VersicherungsCenters“, das von der CHECK24 Versicherungsservice GmbH betrieben wird. Für das „VersicherungsCenter“ gelten die Nutzungsbedingungen der CHECK24 Versicherungsservice GmbH; diese finden Sie hier: Nutzungsbedingungen CHECK24 Versicherungsservice GmbH. Die im „VersicherungsCenter“ hinterlegten und verwalteten Versicherungsverträge werden ebenso abgefragt und gespeichert. In beiden Fällen werden, abgesehen von einer pro Vertrag eindeutigen Referenznummer, lediglich generelle Vertragsinformationen gespeichert, um diese dem Kunden innerhalb der C24 App anzuzeigen und die nachfolgenden Funktionen zu ermöglichen.

Zusätzlich erfolgt bei aktiver erweiterter Vertragserkennung eine technische Verknüpfung der erkannten Verträge mit jenen aus dem CHECK24 Kundenkonto des Nutzers. Verträge, die nicht verknüpft werden konnten, werden dem Nutzer entsprechend gekennzeichnet.

Neben dem Abruf der CHECK24 Verträge werden mit der erweiterten Vertragserkennung die in (a), (b) und (c) aufgelisteten Dienstleistungen bereitgestellt:

(a) Aufzeigen von Spar- und Optimierungspotenzialen

Die Bank wird mit jedem Abruf der Kontoinformation die dabei teilnehmenden Unternehmen der CHECK24 Gruppe anfragen, ob diese Unternehmen, zu den im Kontext der Vertragsübersicht erkannten Verträgen, Alternativ-Vorschläge unterbreiten bzw. mögliche Sparpotenziale aufzeigen können. Es werden nur Daten übermittelt, die zur Abwicklung dieser Dienstleistung zwingend erforderlich sind.

Die Datenempfänger verarbeiten die übermittelten Daten ausschließlich zu diesem festgelegten Zweck. Gegenstand der Verarbeitung sind erkannte Verträge mit gewissen Vertragsinformationen aus den Buchungstexten und infolgedessen auch die aggregierten Kosten hierfür sowie ggf. Verknüpfungen der erkannten Verträge mit einem Unternehmen der CHECK24 Gruppe.

Sollte der Vertrag in der Vergangenheit bereits von einem Unternehmen aus der CHECK24 Gruppe vermittelt worden sein und/oder aktuell betreut werden, wird die Bank lediglich die Referenznummer an das betreffende Unternehmen übermitteln, um Alternativ-Angebote zu erhalten. Das letzte erfolgreiche Ergebnis dieser Anfrage (Angebot) wird die Bank in Form eines Angebotspreises speichern, um so zukünftig dem Nutzer immer zuerst ein entsprechendes Angebot anzeigen zu können, bevor dieses (gegebenenfalls) durch einen neuen Alternativ-Preis ersetzt wird. Sollte hingegen der erkannte Vertrag nicht über ein Unternehmen aus der CHECK24 Gruppe vermittelt worden sein und/oder betreut werden, so wird die Bank einem Unternehmen innerhalb der CHECK24 Gruppe, welches diesen Vertragstypus aktiv vermittelt/betreut, verschiedene

personenbezogene Daten des Nutzers zum Zwecke der Erstellung eines Alternativ-Angebots/-Preises bzw. zum Aufzeigen eines möglichen Sparpotenzials zur Verfügung stellen.

Bei der Auswahl der personenbezogenen Daten des Nutzers wird seitens der Bank strikt darauf geachtet, dass das angefragte Unternehmen innerhalb der CHECK24 Gruppe diese nur zum Zweck der Errechnung von Spar- und Optimierungspotenzialen einsetzt. Dies gilt nicht für den Fall, falls es sich um einen Vertrag handelt, der bereits seitens eines Unternehmens aus der CHECK24 Gruppe vermittelt und/oder betreut wird. In diesem Fall wird die Bank keine zusätzlichen Informationen an das betreffende Unternehmen übermitteln.

(b) Preisaktualisierung

Mit Aktivierung der erweiterten Vertragserkennung wird auch die Funktion „Preisaktualisierung" für jeden aktiv mittels einer Referenznummer verbundenen Vertrag aktiviert. Hierzu werden durch die Bank, sofern das betreffende Unternehmen aus der CHECK24 Gruppe dies technisch unterstützt, die tatsächlich (lt. Kontoinformationen der eingebundenen Bank-Konten) vorhandenen und zugeordneten Abbuchungen und Gutschriften für diesen verbundenen Vertrag an das betreffende Unternehmen innerhalb der Gruppe übermittelt. Folgende Unternehmen nutzen diesen Service:

- CHECK24 Vergleichsportal Energie GmbH
- CHECK24 Vergleichsportal Telekommunikationsdienste GmbH
- CHECK24 Vergleichsportal für Sachversicherungen GmbH

Seitens des empfangenen Unternehmens werden die erhaltenen Umsätze gespeichert, entsprechend aufbereitet und dann dem Nutzer zur Einsichtnahme in seinem CHECK24 Kundenkonto im Rahmen der Vertragsdetailansichten für den betreffenden Vertrag angezeigt, solange diese Verknüpfung besteht.

(c) Kontoschutz

Kunden, die die Funktion Kontoschutz aktivieren, ermächtigen die Bank, Kontobewegungen auf den eingebundenen Bankkonten zu beobachten, die im Zusammenhang mit abgeschlossenen Vergleichsprodukten von einem Unternehmen der CHECK24 Gruppe stehen. Identifizierte Kontobewegungen werden von der Bank an die Unternehmen der CHECK24 Gruppe übermittelt, die verantwortlich für die erkannten Vergleichsprodukte sind. Diese Meldung wird dann von dem entsprechenden Unternehmen inhaltlich geprüft und das Ergebnis dieser Prüfung wiederum an die Bank zurückgespielt. Der Nutzer wird über das Ergebnis dieser Kontoschutz-Prüfung per E-Mail oder Push-Benachrichtigung informiert. Hierbei werden folgende Daten verarbeitet: Kontoschutz-Einstellungen (Art der Kontoalarme, Aktivierungsstatus, Alarmierungsweg (Push-Notification, E-Mail) und Kontoalarm-Daten (z. B. Zeitpunkt des jeweils versendeten Alarms, Art des Alarms, Inhalt des Alarms).

(d) Unternehmen der CHECK24 Gruppe

Eine Auflistung der einzelnen Unternehmen der CHECK24 Gruppe und der jeweiligen Datenschutzbestimmungen kann unter folgendem Link eingesehen werden: https://www.check24.de/unternehmen/impressum/

17. CHECK24 Direktüberweisung

Die optionale Nutzung der CHECK24 Direktüberweisung erfolgt gemäß den „Bedingungen für die CHECK24 Direktüberweisung".

Hierbei werden Daten zwischen verschiedenen Parteien - der Bank, einer vom Kunden ausgewählten Fremdbank (im Folgenden „Fremdbank") und einem Zahlungsempfänger - ausgetauscht.

Für die Durchführung einer Direktüberweisung muss die Bank auf das vom Kunden ausgewählte Fremdbank-konto zugreifen können, von dem die Überweisung ausgeführt werden soll. Der Kunde stellt dazu seine Zugangsdaten (Anmeldename und Online-Banking PIN) zum Online-Banking der Fremdbank über das bereitgestellte Frontend bereit. Die Online-Banking PIN wird von der Bank nicht gespeichert, sondern lediglich über eine den Bankenstandards entsprechende verschlüsselte Verbindung an die Fremdbank übermittelt.

Vor der Einstellung des Überweisungsauftrags bei der Fremdbank sind Prüfschritte erforderlich, z. B., ob die Summe aus Kontostand und Überziehungskreditrahmen den zu überweisenden Betrag abdeckt. Sofern alle Voraussetzungen für eine Direktüberweisung vorliegen, werden die vom Kunden im Überweisungsformular benannten Daten sowie die IP-Adresse des Kunden an die Fremdbank übermittelt.

Je nach Methodik der Fremdbank, wird der Kunde aufgefordert, eine TAN (z.B. mTAN, ChipTAN, iTAN, etc.) zur Bestätigung der Überweisung einzugeben. Die TAN wird verschlüsselt übermittelt und nicht von der Bank

gespeichert. Falls zur Identifizierung gegenüber der Fremdbank ein Zertifikat verwendet wird (Authentifizierungszertifikat), wird dieses von der Bank ausschließlich zur Einstellung der Überweisung verwendet und nicht gespeichert. Sollte zur Einstellung der Überweisung in das Fremdbank-Kundenkonto die Eingabe eines zusätzlichen Sicherheitscodes erforderlich sein (z. B. um einzelne Länder für EU SEPA – Überweisungen freizuschalten), leitet die Bank diesen an die Fremdbank weiter. Eine Speicherung des vom Kunden angegebenen Sicherheitscodes durch die Bank erfolgt nicht. Falls die Fremdbank die Eingabe einer Mobilnummer für die Einstellung einer Überweisung verlangt, leitet die Bank diese an die Fremdbank weiter. Eine Speicherung der vom Kunden angegebenen Mobilnummer durch die Bank erfolgt nicht.

Der Zahlungsempfänger erhält von der Bank eine Bestätigung über die erfolgreiche Einstellung des Überweisungsauftrags. Diese umfasst insbesondere die Daten aus dem Überweisungsformular (Name des Auftraggebers, Bankname, Kontonummer, Bankleitzahl, Betreff, Überweisungsbetrag) sowie das Datum (mit Uhrzeit) und ggf. eine vom Empfänger gewählte Transaktionskennung (z.B. Auftragsnummer). Der Zahlungsempfänger erhält bei der Online-Überweisung keine Information über Kontostände und Umsätze. Bei SEPA-Überweisungen und sofern BIC und IBAN zur Einstellung der Überweisung in das Fremdbank-Konto erforderlich sind (abhängig von der Fremdbank), enthält die Bestätigung an den Zahlungsempfänger auch BIC und IBAN. Diese Daten kann der Zahlungsempfänger grundsätzlich auch seinem Kontoauszug entnehmen.

Der Kunde hat die Möglichkeit, von der Bank eine E-Mail mit einer Transaktionsbestätigung anzufordern. Diese enthält insbesondere folgende Angaben: Name des Inhabers des Empfängerkontos, Name der Absenderbank (Fremdbank), Überweisungszeit (Datum), Betrag, Verwendungszweck und Transaktions-ID. Die E-Mail mit der Transaktionsbestätigung (einschließlich der E-Mail-Adresse des Kunden) wird ausschließlich zum Zwecke der Erfüllung gesetzlicher Aufbewahrungsfristen gespeichert und genutzt.

Die Datenverarbeitung im Rahmen der Direktüberweisung erfolgt basierend insbesondere auf den folgenden Rechtsgrundlagen:

- Verarbeitungstätigkeiten von personenbezogenen Daten auf Grundlage des Art. 6 Abs. 1 Satz 1 lit. b DSGVO (Vertragserfüllung): Kontodeckungsprüfung, Missbrauchsrisikoprüfung, Übermittlung der Überweisungsdaten an den Händler, Speicherung der Überweisungsdaten, Information des Nutzers bei gescheiterter Überweisung, Zusendung der Transaktionsbestätigung.
- Verarbeitungstätigkeiten von personenbezogenen Daten auf Grundlage des Art. 6 Abs. 1 Satz 1 lit. c DSGVO (rechtliche Pflicht): Speicherung der Überweisungsdaten

18. Abschluss von externen Anlageprodukten über CHECK24

Die Bank bietet ihren Kunden die Möglichkeit, über die C24 Bank App Anlageprodukte wie Tages- und Festgelder von Fremdbanken (nachfolgend „externe Anlageprodukte“) abzuschließen. Die technische und organisatorische Bereitstellung der Angebote und der Möglichkeit des Abschlusses erfolgt in Kooperation mit der CHECK24 Vergleichsportal Geldanlage GmbH, Erika-Mann-Str. 62–66, 80636 München.

Für die Vermittlung und Verwaltung der externen Anlageprodukte verarbeiten die Bank und die CHECK24 Vergleichsportal Geldanlage GmbH (CHECK24 Geldanlage) bestimmte personenbezogene Daten als gemeinsam Verantwortliche im Sinne von Art. 26 DSGVO.

Die gemeinsame Verarbeitung betrifft insbesondere:

- Bereitstellung der Angebote und der Möglichkeit zum Abschluss externer Anlageprodukte in der C24 Bank App
- Erhebung und Übermittlung von Kunden- und Antragsdaten an Fremdbanken
- Sofern erforderlich, Übermittlung von für Identifikations- und Legitimationsprozesse erforderliche Daten
- Technische Unterstützung bei der Abwicklung des Kontoeröffnungsprozesses (inkl. Eröffnung eines Verrechnungskontos („Anlagekonto“) bei der C24 Bank) sowie Einzahlung des Anlagebetrags
- Kundenkommunikation
- Technische Unterstützung bei der Verwaltung von Anlageprodukten innerhalb der C24 Bank App (insbesondere Anzeige von Status-, Konto- und steuerrelevanten Informationen sowie Abwicklung von Self-Service-Funktionen wie Freistellungsaufträgen oder Verlängerungen).

Nicht von der gemeinsamen Verantwortlichkeit umfasst sind bankaufsichtsrechtliche Kernprozesse wie Identifikations-, Legitimations-, Kontoeröffnungs-, Zahlungsabwicklungs- oder Kontoführungsprozesse. Diese

liegen ausschließlich im Verantwortungsbereich der C24 Bank GmbH bzw. der jeweiligen Fremdbank. Die Bank ist hierbei verantwortlich für:

- Bereitstellung der C24 Bank App und der Darstellung der Angebote in der App sowie der Produktstrecke für den Abschluss dieser Angebote
- Durchführung von Identifikations- und Legitimationsprozessen
- Übermittlung der Daten an CHECK24 Geldanlage
- Eröffnung des Anlagekontos, sofern noch nicht vorhanden
- Umbuchung des Anlagebetrags vom C24 Girokonto (oder einem Unterkonto (Pocket)) auf das Anlagekonto und anschließend weiter auf das Festgeld-/Tagesgeldkonto der Fremdbank
- Kundenkommunikation innerhalb der C24 Bank App

CHECK24 Geldanlage ist verantwortlich für:

- Betrieb der Einlagenplattform
- Anbindung der Fremdbanken und deren Produktangebote
- Weiterleitung der Antragsdaten an die jeweilige Fremdbank
- Abwicklung der Abrechnungs- und Provisionsprozesse mit der jeweiligen Fremdbank

Im Rahmen der Antragsstrecke erhält der Kunde eine Übersicht über verfügbare Angebote verschiedener Fremdbanken. Wählt der Kunde ein Angebot einer Fremdbank aus, ist die Abfrage bankenindividueller Fragen (darunter KYC – „Know Your Customer“) zur Erfüllung regulatorischer und aufsichtsrechtlicher Vorgaben zwingend erforderlich.

Die Bereitstellung dieser Fragen erfolgt durch CHECK24 Geldanlage. Damit die jeweils relevanten Fragen angezeigt werden können, ist eine vorherige Übermittlung personenbezogener Daten durch die C24 Bank erforderlich. Ohne diese Datenübermittlung ist ein Fortschreiten im Abschlussprozess nicht möglich, da die Fragen nicht abgerufen werden können und somit ein Vertragsabschluss mit der Fremdbank ausgeschlossen ist.

Folgende personenbezogene Daten werden zu diesem Zweck an CHECK24 Geldanlage übermittelt:

- Identifikationsdaten (z.B. Vorname, Nachname, Geburtsdatum, Geburtsort, Geburtsland, Staatsangehörigkeit und weitere)
- Demografische Daten (z.B. Geschlecht und weitere)
- Kontaktdaten (z.B. Anschrift, Mobilfunknummer, E-Mail-Adresse und weitere)
- Finanz- und steuerrelevante Daten (z.B. Steueridentifikationsnummer, FATCA-Status und weitere)
- Berufliche Daten (z.B. Beruf, Branche und weitere)
- Besondere Statusinformationen (z.B. Status als politisch exponierte Person und weitere)

Neben der Beantwortung der Fragen der jeweiligen Fremdbank, kann es auch notwendig sein, dass ein Kunde sich über die C24 Bank erneut legitimiert. Die Notwendigkeit hängt dabei davon ab, wann sich ein Kunde letztmals für die C24 Bank legitimiert hat und ob sein für die letztmalige Legitimation genutztes Ausweisdokument zum Zeitpunkt des Abschlusses eines externen Anlageprodukts noch gültig ist. Ist eine Legitimation notwendig, erhält der Kunde eine entsprechende Information in der C24 Bank App. Über einen Link kann der Kunde dann in den Legitimationsprozess einsteigen.

Im Fall einer erneuten Legitimation des Kunden in der C24 Bank App speichert die C24 Bank diese Legitimation zur Erfüllung gesetzlicher Pflichten. Zudem reicht die C24 Bank die Legitimationsdaten an die Fremdbank weiter, bei der der Kunde ein externes Anlageprodukt abschließen möchte. Dies erfolgt zum Zweck der Erfüllung des Vertrags sowie regulatorischer Vorgaben auf Seiten der Fremdbank.

Eine zwingende Voraussetzung für die erfolgreiche Abwicklung des externen Anlageprodukts ist das Anlagekonto. Das Anlagekonto ist ein Verrechnungskonto, das für die Abwicklung der vorliegenden sowie zukünftigen Anlagen über die C24 Bank App oder CHECK24 Geldanlage genutzt wird. Weitere Details zum Anlagekonto sind den „CHECK24 Anlagekonto Bedingungen“ zu entnehmen.

Sobald die Voraussetzungen (Fragen der Fremdbank vollständig beantwortet, Legitimation vorhanden, Anlagekonto vorhanden) erfüllt sind, wird der Anlagebetrag vom C24 Girokonto bzw. einem Unterkonto (Pocket) der C24 Bank auf das Anlagekonto umgebucht und dort für die Auszahlung auf das Festgeld-/ Tagesgeldkonto bei der entsprechenden Fremdbank vorgemerkt. Sobald alle notwendigen Schritte des Kunden-Onboardings und der Kontoeröffnung auf Seiten der Fremdbank abgeschlossen sind, wird dieser Anlagebetrag vom Anlagekonto auf das Festgeld-/Tagesgeldkonto der Fremdbank weitertransferiert.

Die Kundenkommunikation bzgl. über die C24 Bank App abgeschlossener externer Anlageprodukte erfolgt in der C24 Bank App durch die C24 Bank. Die Kommunikation kann dabei über unterschiedliche Wege erfolgen. Dazu zählen beispielsweise E-Mails, Push Notifications, Benachrichtigungen im Notfication Center oder spezifische Ausspieler auf der Startseite der C24 Bank App.

Kunden können post-sale Services im Sinne eines Self-Services direkt in der C24 Bank App nutzen. Zu solchen Self-Services gehört die Möglichkeit der Beantragung, Bearbeitung und Löschung eines Freistellungsauftrags bei einer Fremdbank, die Möglichkeit zur Beantragung, Bearbeitung und Löschung einer Verlängerung (Prolongation) eines abgeschlossenen externen Anlageprodukts sowie die Möglichkeit zur Einsicht und zum Download sämtlicher im Abschlussprozess zur Verfügung gestellter Dokumente.

Dafür ruft die Bank fortlaufend alle bei CHECK24 Geldanlage hinterlegten konto- und steuerrelevanten Informationen ab, um diese innerhalb der C24 Bank App anzuzeigen. Dies sind neben dem erforderlichen Anlagekonto sowie Informationen zu Freistellungsaufträgen, Verlängerungen und Dokumente auch sämtliche über die C24 Bank App oder CHECK24 Geldanlage abgeschlossenen Anlageprodukte. Der Abruf erfolgt über die Laufzeit der Anlageprodukte hinaus und bleibt auch bei einer späteren Trennung eines verknüpften CHECK24 Kundenkontos bestehen. Der Datenabruf endet mit Schließung des Anlagekontos.

Sämtliche dem Kunden in der C24 Bank präsentierten externen Anlageprodukte werden von Partnerbanken von CHECK24 Geldanlage bereitgestellt. Diese Partnerbanken sind Teil der Einlagenplattform von CHECK24 Geldanlage. Durch die technische Anbindung der Partnerbanken an CHECK24 Geldanlage erfolgt sämtliche Kommunikation bzgl. externer Anlageprodukte an die Partnerbanken durch CHECK24 Geldanlage. CHECK24 Geldanlage leitet dabei beispielsweise für die Kontoeröffnung benötigten Antrags- und Identifikationsdaten an die Partnerbanken weiter.

Aufgrund der technischen Anbindung von Partnerbanken an CHECK24 Geldanlage leisten die Partnerbanken auch fällige Provisionszahlungen für die Vermittlungsleistung direkt an CHECK24 Geldanlage. Eine Weiterverrechnung von Provisionen an die C24 Bank erfolgt im Innenverhältnis zwischen CHECK24 Geldanlage und der Bank.

Einschränkungen bei der Datenverarbeitung:

Sofern der Antrag auf ein externes Anlageprodukt nicht abgeschlossen wird, speichert CHECK24 Geldanlage die übermittelten Daten für bis zu 28 Tage als nicht finalisierte Anfrage, um eine Wiederaufnahme des Prozesses zu ermöglichen. Danach werden die Daten automatisch gelöscht.

Die Datenübermittlung endet mit Abschluss oder Abbruch des Antragsprozesses für das jeweilige externe Anlageprodukt. Eine Speicherung der Daten durch die C24 Bank erfolgt ausschließlich im Rahmen gesetzlicher Aufbewahrungspflichten.

Betroffenenrechte können gegenüber **beiden Verantwortlichen** geltend gemacht werden. Primäre Anlaufstelle ist die C24 Bank: datenschutz@c24.de.

Weitere Details finden Sie im „Informationsblatt zur gemeinsamen Verantwortlichkeit nach Art. 26 Datenschutz-Grundverordnung (DSGVO)“.

19. Freunde einladen

Die Bank stellt Kunden eine optional nutzbare Funktion „Freunde einladen“ zur Verfügung.

Der Kunde kann Dritte (Empfehlungsempfänger) dazu einladen, ein Girokonto bei der Bank zu eröffnen – also aktiv selbst einen Dritten werben. Im Rahmen der „Freunde einladen“-Funktion erhält jeder Kunde einen persönlichen Einladungscode, den er in der C24 Bank App einsehen und mit Freunden teilen kann. Dieser Einladungscode dient ausschließlich dazu, um der Bank eine eindeutige Zuordnung zwischen Werber (Kunde der Bank) und Dritten als Empfehlungsempfänger zu ermöglichen und im Falle der erfolgreichen Werbung, eine Prämie auszahlen zu können.

Dem Kunden stehen zwei Optionen zur Verfügung, um Freunde aus der App heraus einladen zu können: „Einladungscode teilen“ oder „Kontakte einladen“. Dem Kunden steht es vollkommen frei, welche dieser Funktionen er nutzen möchte. Seitens der Bank wird weder eine Vorgabe gemacht noch besteht ein entsprechender monetärer Anreiz, die eine oder die andere Funktion zu nutzen.

(1) Auszahlung der Prämie

Eröffnet der eingeladene Freund erfolgreich ein Konto und erfüllt alle erforderlichen Bedingungen gemäß den „Bedingungen zum Programm Freunde einladen“, wird dem Werber und damit Einladenden, eine Prämie auf sein C24 Girokonto gutgeschrieben.

(2) Einladungscode teilen

Entscheidet sich der Kunde für die Option „Einladungscode teilen“, greift die App auf die nativ seitens des Betriebssystems (Android oder iOS) bereitgestellte Funktionalität zum Teilen von Informationen zurück. In diesem Zuge stellt die Bank dem Kunden und damit dem Betriebssystem lediglich eine vorgefertigte Nachrichtenvorlage bereit, die dieser dann eigenhändig und damit auch eigenverantwortlich, direkt selbst mit anderen Apps teilen kann und muss, um so Dritte einladen zu können. Das bedeutet, nicht die Bank verschickt die Information und damit den Einladungscode, sondern ausschließlich der Kunde selbst. Da hier ausschließlich auf die native, seitens des jeweiligen Betriebssystems zur Verfügung gestellte Funktionalität zum Teilen von Informationen zurückgegriffen wird, hat die Bank zu keiner Zeit Zugriff auf die entsprechenden Daten und somit erfolgt auch keine Verarbeitung der Daten seitens der Bank. Der Kunde allein ist für Versand und letztendlich auch den Inhalt der Einladung verantwortlich.

(3) Kontakte einladen

Möchte der Kunde die Option „Kontakte einladen“ nutzen, ist der Zugriff auf die Kontaktdaten des Telefons und das Auslesen der Kontaktdaten unabdingbar. Jedoch wird dazu neben der aktiven Zustimmung durch den Kunden in der App zum Zugriff auf das Adressbuch und damit der Kontaktdaten des Telefons, zusätzlich systemseitig durch das Betriebssystem (Android oder iOS) eine weitere Zustimmung benötigt, damit überhaupt erstmalig der Zugriff auf diese Daten autorisiert werden kann.

In beiden Fällen kann der Kunde den Zugriff erlauben oder verweigern. Der Kunde muss aktiv die Kontakte auswählen, die er einladen möchte. Die ausgewählten Kontakte sowie die Nachrichtenvorlage der Bank werden infolgedessen lediglich in das SMS-Programm des Telefons übertragen. Der Kunde muss dann jede einzelne Nachrichtenvorlage wiederum selbst versenden. Das heißt, die Bank befüllt auch in diesem Fall lediglich die Nachrichten vor. Der Kunde muss aber auch hier, wie bei der Funktion „Einladungscode teilen“, selbst aktiv die Versendung vornehmen. Zu keiner Zeit speichert die Bank die Kontaktdaten aus dem Adressbuch oder die vom Kunden ausgewählten Kontakte. Die gesamte Verarbeitung findet ausschließlich in Memory und damit lokal innerhalb der App statt. Zu keiner Zeit findet eine Übermittlung der Daten an einen zentralen Server der Bank statt. Darüber hinaus hat der Kunde jederzeit die Möglichkeit, die Zugriffsmöglichkeit der App auf die Kontaktdaten, die im Telefon gespeichert sind, in den Einstellungen des Betriebssystems (Android oder iOS) zu widerrufen. Rechtsgrundlage für die Verarbeitung der Daten aus dem Adressbuch des Kunden ist Art. 6 Abs. 1 lit. f DSGVO.

20. Geld an Kontakte

Die Funktion „Geld an Kontakte“ wird dem Kunden als optional wählbare Dienstleistung gemäß Nr. 3 Abs. (3) der „Bedingungen für den Überweisungsverkehr“ zur Verfügung gestellt. Bei aktiver Auswahl durch den Kunden, steht diese Dienstleistung fortan im Rahmen der Nutzung des Girokontos zur Verfügung. Mit der Funktion „Geld an Kontakte“ kann der Kunde von seinem mobilen Endgerät entweder Geld an seine Kontakte senden oder von diesen anfragen, ohne deren Bankverbindung zu kennen. Grundvoraussetzungen für die Nutzung dieser Leistung ist, dass erstens sowohl der Kunde als auch die Kontakte des Kunden unabdingbar Kunden der Bank sein müssen, zweitens beide diese Funktion aktiv nutzen und drittens alle Beteiligten „sichtbar“ sein müssen.

Damit der Kunde die Funktion aktiv nutzen kann, ist der Zugriff auf die Kontaktdaten des mobilen Endgeräts des Kunden und das Auslesen und Abgleichen dieser Kontakte unabdingbar. Bei der erstmaligen Nutzung dieser Funktion muss der Kunde der Bank aktiv diesen Zugriff gewähren. Zusätzlich kann der Kunde ein weiteres Mal systemseitig durch das Betriebssystem (Android oder iOS) aufgefordert werden, diesen Zugriff ausdrücklich zu autorisieren, wenn die App entweder bis dato keine Berechtigung hat, hierauf zugreifen zu können, oder dieser Zugriff widerrufen wurde. In beiden Fällen kann der Kunde den Zugriff erlauben oder verweigern oder zu einem späteren Zeitpunkt in den Einstellungen des Betriebssystems widerrufen oder wieder gewähren. Sollte der Zugriff nicht gewährt werden, kann die Bank diese Funktion dem Kunden nicht anbieten.

Mit Gewährung des Zugriffs liest die Bank zuerst einmal initial sämtliche Kontaktdaten aus dem Adressbuch des mobilen Endgeräts aus und generiert für jeden Eintrag, basierend auf Namen und Mobilfunknummer, ausschließlich in Memory, und damit lokal innerhalb der App, einen eindeutigen Hash. Danach wird ausschließlich dieser Hash dazu genutzt, um auf den Systemen der Bank abgleichen zu können, ob dieser Kontakt, der hinter dem Hash steht, auch die Funktion „Geld an Kontakte" nutzt. Sollte das der Fall sein, wird dem Kunden diese Treffer in seiner App angezeigt; im Negativfall werden sowohl Hash als auch Kontaktdaten sofort verworfen.

Bei jeder folgenden Nutzung/Aufruf dieser Funktion liest die Bank wieder die Kontaktdaten des Adressbuchs neu aus, generiert daraus wieder ausschließlich in Memory diesen Hash und gleicht diesen wieder mit den Systemen der Bank ab. Im Fall eines neuen Treffers wird dieser dem Kunden in der App angezeigt; im Negativfall werden sowohl Hash als auch Kontaktdaten sofort verworfen oder aus der Trefferliste entfernt. Intention dieser Wiederholung ist, um feststellen zu können, ob entweder die bestehenden positiven Treffer noch weiterhin diese Funktion nutzen oder ob neue Treffer vorhanden sind.

Des Weiteren ist über die Funktion „Geld an Kontakte" möglich, Chat-Nachrichten an andere Kontakte zu schicken, die diese Funktion aktiviert haben. Die Chat-Nachrichten werden verschlüsselt übertragen und gespeichert.

Im Rahmen der Funktion „Geld an Kontakte" werden folgende Daten verarbeitet:

- Mobilfunknummern: Zur Ermittlung von gemeinsamen Kontakten, die ebenfalls Kunden der Bank sind und die Funktion „Geld an Kontakte" nutzen. Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten ist Art. 6 Abs. 1 lit. f DSGVO.
- Chat-Nachrichten: Die Verarbeitung der Nachrichten erfolgt auf Grundlage von Art. 6 Abs. 1 lit. a DSGVO im Rahmen der durch den Kunden erteilten Einwilligung bei Aktivierung der Funktion. Im Rahmen der Weiterentwicklung/Fehleranalyse (vgl. Art. 6 Abs. 1 lit. f DSGVO) sowie gesetzlichen oder regulatorischen Verpflichtungen (vgl. Art. 6 Abs. 1 lit. e DSGVO) behält sich die Bank jedoch den vereinzelten Zugriff auf die Chat-Nachrichten vor.

21. Profilbild

Die Verwendung eines Profilbildes wird dem Kunden als optional wählbare Dienstleistung zur Verfügung gestellt.

Die Rahmenbedingungen hinsichtlich der Verwendung eines Profilbildes sind im folgenden Dokument festgehalten und gelten, sofern diese seitens des Nutzers vor Speicherung eines Bildes bestätigt werden: Bedingungen zur Verwendung eines Profilbildes.

Das Profilbild des Kunden wird ausschließlich dem Kunden selbst in seiner C24 Bank App und anderen Kunden der Bank an ausgewählten Stellen innerhalb der C24 Bank App (nachfolgend „Verwendungsbereich") angezeigt. Dritte, die nicht Kunden der Bank sind, verfügen über keinen Zugriff auf das Profilbild des Kunden.

Verwendungsbereiche des Profilbildes für andere Kunden sind dabei insbesondere:

- Transaktionsübersicht, Transaktionshistorie,
- Zahlungszusammenfassung,
- Überweisungsvorlagen,
- Geld an Kontakte oder
- geteilte Konten bzw. geteilte Pockets.

Der Kunde kann jederzeit die Anzeige des eigenen Profilbildes und Sichtbarkeit für andere Kunden innerhalb der C24 Bank App in den Datenschutzeinstellungen der C24 Bank App verwalten.

22. Gemeinschaftskonto

Die Verwendung des Gemeinschaftskontos ist optional wählbar und erfolgt gemäß den „Bedingungen für Gemeinschaftskonten". Hierfür verarbeitet die Bank gemäß Art. 6 Abs. 1 lit. b DSGVO Daten zur Identifizierung der Inhaber eines Gemeinschaftskontos sowie Transaktionsdaten.

Zur Erstellung eines Gemeinschaftskontos muss ein Kunde eine weitere Person, die ihrerseits unabdingbar Kunde der Bank sein muss, (nachfolgend „Eingeladener") mittels Einladungslinks einladen. Dieser Link kann vom Kunden über dessen Mobilgerät eigenständig und somit ohne Mitwirkung der Bank oder der C24 Bank App versendet werden. Wenn der Kunde eine andere Person, also den Eingeladenen, zur Eröffnung eines

Gemeinschaftskontos einlädt, werden dessen Kontaktdaten als zusätzliche Sicherheitsmaßnahme gegen Betrug an den Eingeladenen weitergegeben; gleiches gilt umgekehrt, wenn der Kunde eine erhaltene Einladung zu einem Gemeinschaftskonto annimmt. Die Erhebung und Verarbeitung dieser Daten sind für die Durchführung des Vertrages zwischen der Bank und dem Kunden erforderlich (Art. 6 Abs. 1 lit. b DSGVO). Ferner entspricht diese Handlung und damit diese Verarbeitung auch dem berechtigten Interesse der Bank, um ihrerseits den gesetzlich auferlegten Pflichten in Zusammenhang mit Geldwäsche- und Betrugsprävention nachkommen zu können (Art. 6 Abs. 1 lit. f DSGVO).

Beide Personen, also Kunde, und damit ursprünglicher Besitzer des Kontos als auch Eingeladener, der jetzt die Einladung des Besitzers aktiv angenommen hat, sind fortan gleichberechtigte Inhaber dieses Kontos. Folglich sind beide Personen berechtigt, individuell auf alle personenbezogenen Daten und Transaktionen im Zusammenhang mit diesem Gemeinschaftskonto zuzugreifen; einschließlich der Transaktionen der jeweils anderen Person, aber ausschließlich in Bezug auf das Gemeinschaftskonto und nicht in Bezug auf deren weiterhin bestehenden individuellen Einzelkonten.

Die zugehörigen Daten werden im Rahmen der Betroffenenrechte (insb. Art. 15 und 17 DSGVO) allen Betroffenen gemeinschaftlich zugeordnet.

IV. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

Innerhalb der Bank erhalten nur diejenigen Personen Zugriff auf Kundendaten, die diese zur Erfüllung der vertraglichen und gesetzlichen Pflichten benötigen.

Für die technische Bereitstellung der Dienste der Bank wird die Bank von verschiedenen Dienstleistern weisungsgebunden unterstützt. Bezüglich der Datenerhebung, -nutzung und -verarbeitung im Rahmen dieser Dienste existieren zwischen der Bank (Auftraggeberin) und den Dienstleistern der Bank (Auftragnehmern) schriftliche Vereinbarungen über die Auftragsverarbeitung nach Art. 28 DSGVO.

Die Bank gibt die personenbezogenen Daten der Kunden an Dritte generell nur dann gemäß folgender Regeln an Dritte, einschließlich CHECK24 Gruppe verbundenen Unternehmen und an Dienstleister weiter und das unabhängig davon, ob diese weisungsgebunden oder eigenverantwortlich handeln.

- Empfänger der Daten können Unternehmen der CHECK24 Gruppe (siehe Ziffer 16 lit. d welche Unternehmen zur „CHECK24 Gruppe“ gehören) sein, die im Auftrag der Bank Dienstleistungen, wie z. B. Helpdesk, Support oder Betrieb der IT-Infrastruktur, erbringen. Dabei gewährt die Bank den beauftragten und mit der Bank in der CHECK24 Gruppe verbundenen Unternehmen, soweit erforderlich, Zugriff auf Kundendaten, z. B. zur Identitätsprüfung.
- Empfänger der Daten können auch Unternehmen sein, die Leistungen zur Bonitätsprüfung sowie Missbrauchs- und Betrugsverhinderung für die Bank erbringen (siehe Gliederungspunkt VI dieser Bedingungen). Die fraglichen Unternehmen können Ihre Daten sowie die vorgenommenen Suchen aufzeichnen, selbst wenn der Antrag erfolglos ist oder nicht fortgeführt wird. Diese Unternehmen können bei der Prüfung von Kundendaten unter anderem auch mathematisch-statistische Verfahren zur Berechnung von Zahlungswahrscheinlichkeiten unter Verwendung von Anschriftendaten (Scoring) einsetzen. Die Entscheidung erfolgt im Rahmen eines automatisierten Verfahrens. In die Entscheidung fließen insbesondere die vom Kunden eingeholten Informationen, Score-Werte der Unternehmen selbst sowie Zahlungserfahrungen auf Basis von Personen-, Kontakt-, Bankverbindungs- und ggfs. Kartendaten des Kunden ein.
- Die Bank ist als ausgebendes Finanzinstitut von Girokonten und Krediten für Kunden gesetzlich dazu verpflichtet, die Identität zu überprüfen (sog. „Know-Your-Customer“ oder KYC-Prozess). Die Bank ist entsprechend den Vorgaben im Geldwäschegesetz (GwG) dazu verpflichtet, die unter Gliederungspunkt II. Nr. 6 dieser Bedingungen genannten Daten zu erheben und zu verifizieren.
- Bei der Zahlung mit der C24 Mastercard werden die für die Zahlung notwendigen personenbezogenen Daten an Mastercard als Kartennetzwerk und Zahlungssystem weitergeleitet, um die Zahlung durchzuführen, einschließlich Informationen zu der Transaktion und Karteninformationen.
- Wenn die C24 Mastercard zu einem Wallet eines Drittanbieters wie unter anderem Apple Pay, Google Pay und Mastercard Click-to-Pay hinzugefügt wird, können die Kartendaten und der Kundenname an

den Drittanbieter übertragen werden. Die Verarbeitung der Kundendaten durch den Drittanbieter erfolgt in alleiniger Verantwortung des Drittanbieters.

- Zur Erstellung einer physischen Karte empfängt der Dienstleister, der im Auftrag der Bank die physische Karte herstellt und prägt, die dafür erforderlichen Kundendaten.
- Empfänger können auch Strafverfolgungsbehörden, Aufsichtsorganisationen, Gerichte oder andere Behörden sein, jedoch nur soweit die Bank dazu aufgrund gesetzlicher Bestimmungen oder auf gesetzlicher Grundlage erlassener behördlicher Maßnahmen oder in Verbindung mit Gerichtsverfahren verpflichtet ist oder wenn dies in Fällen von Missbrauchs- oder Betrugsaktivitäten zur zivilrechtlichen oder strafrechtlichen Verfolgung notwendig ist. Übermittlungen zu anderen Zwecken – insbesondere für den Adressenhandel – sind ausgeschlossen.
- Bei der Einbindung eines oder mehrerer Fremdbankkonten (siehe Nummer 15 dieser Bedingungen) werden mit jedem Abruf von Kontoumsätzen die Zugangsdaten für das jeweilige Konto sowie ggf. eine entsprechende TAN an die kontoführende Bank übermittelt. Diese Übermittlung ist unabdingbar, damit die Bank aktuelle Kontoinformationen bezüglich des jeweils eingebundenen Fremdbankkontos erhalten, anzeigen und die darauf bezogenen Funktionen im Rahmen der „Bedingungen für das Girokonto“ erbringen kann.
- Für den Fall, dass der Kunde offene Rechnungen oder Raten trotz wiederholter Mahnung nicht begleicht, kann die Bank die für die Durchführung eines Treuhandinkassos erforderlichen Daten an einen Inkassodienstleister übermitteln. Alternativ kann die Bank die offenen Forderungen stattdessen auch an einen Inkassodienstleister veräußern (Forderungsverkauf). Dieser wird dann Forderungsinhaber und macht die Forderungen im eigenen Namen und auf eigene Rechnung geltend. Die Bank arbeitet mit dem folgenden Inkassodienstleistern zusammen: PAIR Finance GmbH, Hardenbergstraße 32, 10623 Berlin; VR Inkasso GmbH, Hannoversche Straße 149, 30627 Hannover, Rechtsgrundlage für die Übermittlung der Daten im Rahmen des Treuhandinkasso ist Artikel 6 Absatz 1 lit. b DSGVO; die Übermittlung der Daten im Rahmen des Forderungsverkaufs erfolgt auf Basis von Artikel 6 Absatz 1 lit. f DSGVO.
- Für die Erfüllung gesetzlicher Verpflichtungen nach dem Common Reporting Standard (CRS) und dem Foreign Account Tax Compliance Act (FATCA), meldet die Bank bestimmte personenbezogene Daten von Kunden (insb. zur Identifizierung sowie für die Berechnung der Steuer notwendigen Daten) an das Bundeszentralamt für Steuern zu Zwecken der Übermittlung an den Ansässigkeitsstaat des Kontoinhabers. Diese Meldungen dienen der internationalen Zusammenarbeit zur Bekämpfung von Steuerhinterziehung gemäß dem Finanzkonten-Informationsaustauschgesetz (FKAustG).
- Für das Thema Datenübermittlungen in Drittländer wird auf den Gliederungspunkt VIII. dieser Bedingungen verwiesen.

23. Datenübermittlung im Rahmen der Nutzung von Google Pay, Apple Pay und Mastercard Click-to-Pay

Zur Nutzung der mobilen Zahlungsdienste von Google, Apple und Mastercard Click-to-Pay, werden hierzu Kontoinformationen der Bank an den Prozessor Mastercard MPTS übermittelt und dort in einen verschlüsselten Token zur Zahlungsautorisierung und -durchführung umgewandelt. Google, Apple und Mastercard Click-to-Pay stellen die technologische Grundlage der Datenverarbeitung zur Verfügung. Zur Erfüllung des Vertrages, den der Kunde mit Google, Apple und/oder Mastercard Click-to-Pay eingeht, wird die Bank die notwendigen personenbezogenen Daten des Kunden mit Alphabet Inc. (Google), Apple Inc. oder Mastercard Europe S.A. teilen; Rechtsgrundlage hierfür ist demnach Art. 6 Abs. 1 lit. b DSGVO. Sollte der Kunde die Dienste wieder deaktivieren, wird der von Mastercard MPTS generierte Token automatisch deaktiviert und gelöscht.

(1) Datenverarbeitung bei Google Pay

Die Datenverarbeitung innerhalb von Google Pay richtet sich grundsätzlich nach den Datenschutzhinweisen/-richtlinien für Google Payments sowie der Datenschutzerklärung von Google.

Google werden dabei von der Bank folgende personenbezogene Daten zur Verfügung gestellt:

- Namen, Anschrift und Telefonnummer sowie Kartenart, -nummer und Gültigkeitsdauer des Zahlungsmittels
- Informationen über durch Google Pay ausgelöste Zahlungsvorgänge (Transaktionsdaten). Transaktionsdaten sind u. a. Datum, Uhrzeit, Art und Betrag der Transaktion, Händlername/-

anschrift, Händlerstandort, Waren- bzw. Dienstleistungskategorie, Transaktionsstatus, Autorisierungsdaten der Transaktion, Händlerrabatte und verwendetes Endgerät.

(2) Datenverarbeitung bei Apple Pay

Die Datenverarbeitung innerhalb von Apple Pay richtet sich grundsätzlich nach den Datenschutzhinweisen/-richtlinien für Apple Pay sowie der Datenschutzerklärung von Apple. Diese können auf der Webseite von Apple nachgelesen werden.

Apple werden dabei von der Bank folgende personenbezogene Daten zur Verfügung gestellt:

- Namen, Anschrift und Telefonnummer sowie Kartenart, -nummer und Gültigkeitsdauer des Zahlungsmittels
- Informationen über durch Apple Pay ausgelöste Zahlungsvorgänge (Transaktionsdaten). Transaktionsdaten sind u. a. Datum, Uhrzeit, Art und Betrag der Transaktion, Händlername/-anschrift, Händlerstandort, Waren- bzw. Dienstleistungskategorie, Transaktionsstatus, Autorisierungsdaten der Transaktion, Händlerrabatte und verwendetes Endgerät.

(3) Datenverarbeitung bei Mastercard Click-to-Pay

Die Datenverarbeitung innerhalb von Mastercard Click-to-Pay richtet sich grundsätzlich nach den Nutzungsbedingungen sowie der Datenschutzerklärung von Mastercard Click-to-Pay. Diese können auf der Webseite von Mastercard nachgelesen werden.

Mastercard Click-to-Pay werden dabei von der Bank folgende personenbezogene Daten zur Verfügung gestellt:

- Namen, Anschrift und Telefonnummer sowie Kartenart, -nummer und Gültigkeitsdauer des Zahlungsmittels
- Informationen über durch Mastercard Click-to-Pay ausgelöste Zahlungsvorgänge (Transaktionsdaten). Transaktionsdaten sind u. a. Datum, Uhrzeit, Art und Betrag der Transaktion, Händlername/-anschrift, Händlerstandort, Waren- bzw. Dienstleistungskategorie, Transaktionsstatus, Autorisierungsdaten der Transaktion, Händlerrabatte und verwendetes Endgerät.

24. Datenübermittlung im Rahmen von Push-Benachrichtigungen über Google Firebase Cloud Messaging und Apple Push Notifications

Die C24 Bank App hat die technische Möglichkeit vorgesehen, Push-Benachrichtigungen zur Nutzung der C24 Bank App und der Erbringung der Dienste zu übermitteln (Art. 6 Abs. 1 lit. b DSGVO).

Bei einer Push-Benachrichtigung handelt es sich um eine über die C24 Bank App verwaltete Mitteilung an den Kunden, dass neue Kontoinformationen vorliegen. Der Kunde kann die Entscheidung treffen, diese anzusehen oder zu ignorieren.

Um Push-Benachrichtigungen empfangen zu können, muss der Kunde Benachrichtigungen der C24 Bank App auf seinem Mobiltelefon oder Tablet-Computer zulassen. Hierbei erfolgt eine Weitergabe von Gerätedaten an das Push-Benachrichtigungssystem des Mobiltelefons oder Tablet-Computers des Kunden.

Zur eindeutigen Weiterleitung von Informationen an den Kunden verwendet die Bank ein sogenanntes Push-Token (eine individuelle, zufallsgenerierte Nummer), welches sie von den Betreibern der App-Stores übermittelt bekommt. Der Transport der Nachrichten erfolgt verschlüsselt und ist nur der Bank und dem Kunden bekannt. Die Betreiber der App-Stores können Push-Benachrichtigungen nicht einsehen.

(1) Google Firebase Cloud Messaging

Google Firebase Cloud Messaging ist ein Dienst von Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. Die Datenspeicherung erfolgt in Dublin, Irland.

Die Daten werden im Rahmen eines Auftragsverarbeitungsvertrags https://firebase.google.com/terms/data-processing-terms von Google Firebase für die Bank verarbeitet und in einer Weboberfläche aufbereitet.

Sollte der Kunde keine Push-Benachrichtigung zukünftig von der Bank erhalten wollen, kann der Kunde dies in den Einstellungen seines Mobiltelefons oder Tablet-Computers für die C24 Bank App jederzeit wie folgt festlegen.

Android: Einstellungen/Apps/<Name der C24 Bank App>/Benachrichtigungen

(2) Apple Push Notifications

Bei einem Mobiltelefon mit dem Betriebssystem iOS wird der Apple Push Notification Service der Apple, Inc. verwendet. Die Datenschutzrichtlinie von Apple ist hier einsehbar.

Sollte der Kunde keine Push-Benachrichtigung zukünftig von der Bank erhalten wollen, kann der Kunde dies in den Einstellungen seines Mobiltelefons oder Tablet-Computers für die C24 Bank App jederzeit wie folgt festlegen.

iOS: Einstellungen/<Name der C24 Bank App >/Mitteilungen

(3) SMS Versand

Die Bank wird in einigen Fällen Informationen an den Kunden mittels SMS verschicken z. B. einen Sicherheitscode bei der Kontoeröffnung oder einen Einladungslink für den Download der C24 Bank App.

25. Marketingmitteilungen

Abhängig des Umfangs der Einwilligungserklärungen erhält der Kunde Werbung sowohl per E-Mail als auch als Push-Mitteilung seitens der C24 Bank. Diese Mitteilungen können Personalisierungen enthalten, die auf Basis folgender Daten hinsichtlich der Relevanz bestimmt wird:

- Transaktionsdaten Ihres Kontos,
- Persönliche Daten (z.B. Alter, Adresse) und
- Nutzungsdaten (z.B. welche Funktionen Sie verwenden).

Die Personalisierung der Mitteilungen erfolgt ausschließlich durch die C24 Bank. Es erfolgt keine Weitergabe von Daten an Partnerunternehmen, es sei denn, diesem Vorgang wurde an anderer Stelle ausdrücklich zugestimmt oder ist anderweitig vertraglich geregelt.

Rechtsgrundlage für die Verarbeitung ist Art. 6 Abs. 1 lit. a) DSGVO.

Der werblichen Kontaktaufnahme können Sie jederzeit in den App-Einstellungen widerrufen. Alternativ enthält jede E-Mail einen Link am Ende oder Sie können sich an unseren Kundenservice (kundenservice@c24.de) wenden, um dem Erhalt jederzeit widersprechen zu können.

26. Datenverarbeitung im Rahmen der Nutzung von künstlicher Intelligenz

Zur Unterstützung ausgewählter automatisierter Prozesse im Rahmen der Kundenkommunikation, der Ausgabenanalyse und Transaktionssuche sowie interner Abläufe kommen cloudbasierte KI-Dienste über Microsoft Azure sowie Google Cloud / Vertex AI zum Einsatz. Hierfür werden ausschließlich Server innerhalb der Europäischen Union seitens der jeweiligen Anbieter genutzt. Diese Datenverarbeitung umfasst insbesondere Funktionen zur automatisierten Bearbeitung von Nutzeranfragen (zum Beispiel in einem Chatbot) sowie zur strukturellen Analyse, Klassifikation und/oder Validierung von Eingaben. Im Rahmen der Nutzung von Google Cloud / Vertex AI kann eine Datenübermittlung in Drittländer nicht ausgeschlossen werden. Durch den Einsatz einer auf die Europäische Union beschränkten Verarbeitungsumgebung wird eine solche Übermittlung auf das technisch und vertraglich unvermeidbare Minimum reduziert.

Im Rahmen dieser von uns eingesetzten KI-Dienste, können folgende Kategorien von personenbezogenen Daten verarbeitet werden: Stammdaten (z.B. Nachname, Vorname, Adresse, E-Mail, Telefonnummer), Kontoinformationen (z.B. IBAN, Kontonummer, Pocketinformationen, etc.), Karteninformationen (z.B. Kartennummer, Kartentyp, Status etc.), Transaktionsdaten (z.B. Betrag, Buchungsdatum, Counterpart, Verwendungszweck sowie weitere transaktionsbezogene Angaben), Kommunikationsdaten: (z.B. Inhalte der Chatnachrichten (freie Texteingaben der Kunden), Zeitpunkt der Anfrage, Metadaten der Anfrage (z.B. IP-Adresse für Logging) etc.

Die Verarbeitung dieser personenbezogenen Daten erfolgt im Rahmen einer Auftragsverarbeitung gemäß Art. 28 DSGVO mit Microsoft Ireland Operations Ltd. auf deren Azure-Plattform bzw. mit Google Cloud EMEA Limited auf deren Vertex-AI-Plattform. Die jeweiligen Anbieter agieren hier als Hosting- und Plattformanbieter und stellen in diesem Zusammenhang eine integrierte, ausschließlich EU-basierte Systemarchitektur. Eine Datenübermittlung in Drittländer ist bei der Nutzung von Microsoft Ireland Operations Ltd. ausgeschlossen.

Zudem ist durch entsprechende technische und organisatorische Maßnahmen diesseitig sichergestellt, dass die übermittelten personenbezogenen Daten nicht zu Trainingszwecken verwendet werden.

Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO. Das berechtigte Interesse liegt in der effizienten, sicheren und skalierbaren Ausgestaltung digitaler Serviceprozesse, der operativen Unterstützung interner Abläufe sowie der Verhinderung von Geldwäsche und Betrug im Sinne der §§ 10 ff. GwG.

V. Identifikationsverfahren

Die Bank ist aufgrund des Geldwäschegesetzes (GwG) gesetzlich verpflichtet, die Identität des Interessenten insbesondere im Rahmen der Kontoeröffnung oder der Kreditvergabe durch ein gültiges Ausweisdokument zu überprüfen und bestimmte Angaben des Ausweisdokuments zu speichern. Hierzu bietet die Bank das Video-Ident-Verfahren, das POSTIDENT-Verfahren, das SofortIdent-Verfahren und das Legitimierungsverfahren mit dem Personalausweis mit Online-Ausweisfunktion (eID) an. Darüber hinaus haben Kunden die Möglichkeit, mithilfe des SmartIdent-Verfahrens eigenständig Sicherheitssperren innerhalb der C24 Bank App aufzulösen sowie den Besitz eines Aufenthaltstitels nachzuweisen.

(1) Video-Ident

Die Durchführung der Videoidentifikation erfolgt im Auftrag der Bank durch einen externen Dienstleister. Die Identität wird durch ein internetbasiertes Video-Identifikationsverfahren über einen verschlüsselten Übertragungsweg ermittelt. Die Bank wird dafür personenbezogene Daten an externe Dienstleister zum Zwecke der Überprüfung der Identität übermitteln. Für das Video-Ident-Verfahren erfolgt die Identifikation direkt per Live-Video. Während der Video-Identitätsbestätigung muss der Anbieter die Authentizität des vorgelegten Personalausweises oder Reisepasses sicherstellen. Zu Beweiszwecken werden die Fotos sowie das Live-Video aufgezeichnet und so lange aufbewahrt, wie es die jeweiligen einschlägigen Gesetze vorschreiben.

(2) POSTIDENT

Die Durchführung des POSTIDENT-Verfahrens erfolgt im Auftrag der Bank durch die Deutsche Post AG, Charles-de-Gaulle-Straße 20 in 53113 Bonn (im Folgenden „Deutsche Post AG“). Dem Kunden wird von der Bank ein sogenannter POSTIDENT Coupon zur Verfügung gestellt, mit dem er sich in Deutschland in einer Filiale der Deutsche Post AG mit Hilfe eines gültigen Ausweisdokuments identifizieren lassen kann. Zur Feststellung der Identität des Kunden werden personenbezogene Daten, insbesondere Angaben zur Person und Ausweisdaten, zwischen der Bank und der Deutsche Post AG über einen verschlüsselten Übertragungsweg ausgetauscht. Zu Beweiszwecken werden die verarbeiteten Daten so lange aufbewahrt, wie es die jeweiligen einschlägigen Gesetze vorschreiben.

(3) AutoIdent

Die Durchführung der AutoIdent-Funktion zu den Zwecken der Auflösung von Sicherheitssperren innerhalb der C24 Bank App und zum Nachweis eines Aufenthaltstitels erfolgt im Auftrag der Bank durch einen externen Dienstleister. Die Identität wird durch ein internetbasiertes Identifikationsverfahren über einen verschlüsselten Übertragungsweg ermittelt. Die Bank wird dafür personenbezogene Daten an externe Dienstleister zum Zwecke der Überprüfung der Identität übermitteln. Für das AutoIdent-Verfahren erfolgt die Identifikation durch Live-Fotoaufnahmen von Ausweisdokumenten, z. B. Personalausweis oder Reisepass bzw. dem elektronischen Aufenthaltstitel. Während der Identitätsbestätigung muss der Anbieter die Authentizität der vorgelegten Ausweisdokumente sicherstellen. Zu Beweiszwecken werden die Fotos aufgezeichnet und so lange aufbewahrt, wie es die jeweiligen einschlägigen Gesetze vorschreiben.

(4) SofortIdent

Die Durchführung des SofortIdent-Verfahrens erfolgt im Auftrag der Bank durch die IdentityCheck GmbH, Erika-Mann-Str. 62-66 in 80636 München. Die Identität wird durch ein internetbasiertes Identifikationsverfahren über einen verschlüsselten Übertragungsweg ermittelt. Die Bank wird dafür personenbezogene Daten an die IdentityCheck GmbH übermitteln. Für das SofortIdent-Verfahren erfolgt die Identifikation durch eine Referenzüberweisung zusammen mit einer QES (qualifizierte elektronische Signatur). Zu Beweiszwecken werden die verarbeiteten Daten so lange aufbewahrt, wie es die jeweiligen einschlägigen Gesetze vorschreiben.

(5) Legitimierung mit dem Personalausweis mit Online-Ausweisfunktion (eID)

Die Durchführung des Legitimierungsverfahrens mit dem Personalausweis mit Online-Ausweisfunktion (eID) erfolgt im Auftrag der Bank durch die IdentityCheck GmbH, Erika-Mann-Str. 62-66 in 80636 München. Die Identität wird durch ein internetbasiertes Identifikationsverfahren über einen verschlüsselten Übertragungsweg ermittelt. Die Bank wird dafür personenbezogene Daten an die IdentityCheck GmbH übermitteln. Für das Legitimierungsverfahren mit eID erfolgt die Identifikation durch den Ausweisscan, das Auslesen der persönlichen Daten aus dem Personalausweis mit Online-Ausweisfunktion (eID), und Live-Fotoaufnahmen von dem Personalausweis. Zu Beweiszwecken werden die verarbeiteten Daten so lange aufbewahrt, wie es die jeweiligen einschlägigen Gesetze vorschreiben.

(6) SmartIdent

Die Durchführung des SmartIdent-Verfahrens dient zur Auflösung von Sicherheitssperren innerhalb der C24 Bank App sowie zum Nachweis eines deutschen Aufenthaltstitels und erfolgt im Auftrag der Bank durch die IdentityCheck GmbH, Erika-Mann-Str. 62-66 in 80636 München. Die Identität wird durch ein internetbasiertes Identifikationsverfahren über einen verschlüsselten Übertragungsweg ermittelt. Die Bank wird dafür personenbezogene Daten an die IdentityCheck GmbH zum Zwecke der Überprüfung der Identität übermitteln. Die Identifikation erfolgt durch automatisierte Prüfschritte anhand von Aufnahmen gültiger Ausweisdokumente, z. B. Personalausweis oder Reisepass bzw. elektronischer Aufenthaltstitel, sowie ggf. ergänzende Verifikationsverfahren. Während der Identitätsbestätigung stellt der Anbieter die Authentizität der vorgelegten Ausweisdokumente sicher. Zu Beweiszwecken werden die im Rahmen des Verfahrens verarbeiteten Daten so lange aufbewahrt, wie es die jeweiligen einschlägigen Gesetze vorschreiben.

VI. Bonitätsüberprüfung und Datenübermittlung an die SCHUFA

Die Bank übermittelt im Rahmen des jeweiligen Vertragsverhältnisses erhobene personenbezogene Daten über die Beantragung, die Durchführung und die Beendigung dieser Geschäftsbeziehung (insb. bei Giro-, Basis-, Pfändungsschutz- und Gemeinschaftskonten sowie Ratenkrediten) sowie Daten über nicht vertragsgemäßes Verhalten oder betrügerisches Verhalten an die SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden (im Folgenden „SCHUFA“).

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 und den Datenschutzhinweisen der SCHUFA können unter www.schufa.de/datenschutz eingesehen werden.

Rechtsgrundlagen dieser Übermittlungen ist das berechtigte Interesse der Bank an der Verarbeitung gemäß Art. 6 Abs. 1 lit. f DSGVO. Die 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. Sofern die Datenübermittlung zur Erfüllung einer vertraglichen Verpflichtung mit der betroffenen Person erfolgt, gilt als Rechtsgrundlage Art. 6 Abs. 1 lit. b DSGVO. Der Datenaustausch mit der SCHUFA dient auch der Erfüllung gesetzlicher Pflichten zur Durchführung von Kreditwürdigkeitsprüfungen von Kunden (§ 505a des Bürgerlichen Gesetzbuches, § 18a des Kreditwesengesetzes).

Der Kunde befreit die Bank insoweit auch vom Bankgeheimnis.

VII. Verwendung von Cookies

Informationen zur Verwendung der Cookies werden in einer separaten Cookie Policy bereitgestellt, die vor Abschluss eines Girokontovertrages zwischen Kunde und Bank und über die Webseite der Bank www.c24.de zur Verfügung gestellt wird.

VIII. Übertragung von personenbezogenen Daten in Drittländer gem. Art 44 bis 49 DSGVO

Soweit die Bank personenbezogene Daten in ein Drittland i.S.d. DSGVO (d.h. außerhalb der EU) übermittelt, stellt die Bank sicher, sofern kein entsprechender Angemessenheitsbeschluss gemäß Art. 45 DSGVO der Kommission vorliegt, dass der/die Empfänger der Daten ein angemessenes Datenschutzniveau gewährleistet/n. Sollte kein Angemessenheitsbeschluss für das betreffende Drittland vorliegen, wird die Bank zur Sicherstellung eines angemessenen Schutzniveaus beim Empfänger geeignete Garantien einholen bzw. wirksame Vereinbarungen mit dem Empfänger treffen. Hierzu zählen u.a. der Abschluss von Musterverträgen der Europäischen Union für die Übermittlung von Daten ins EU-/EWR-Ausland in der jeweils aktuellen Fassung (Art. 46 Abs. 2 lit. c DSGVO) oder die verbindlichen internen Datenschutzvorschriften gemäß Art. 47 DSGVO.

IX. Automatisierte Entscheidungsfindung und Profiling

Die Bank verarbeitet Daten teilweise automatisiert mit dem Ziel, bestimmte persönliche Aspekte zu bewerten (Profiling) beispielsweise in folgenden Fällen:

- Zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und anderen vermögensgefährdenden Straftaten. Bei Erfüllung dieser gesetzlichen Pflichten werden auch Datenauswertungen (unter anderem im Zahlungsverkehr) vorgenommen, um Kundengelder der Bank zu schützen.
- Zu gezielter und bedarfsgerechter 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 (siehe Nr. 27 dieser Bedingungen) sowie zur Bewertung der Geschäftsbeziehung nutzt die Bank Scoring.
- Zur automatisierten Risikoprüfung werden im Rahmen unserer Sorgfaltspflichten im Sinne des § 15 GwG KI-gestützte Recherchearbeiten durchgeführt. Hierbei werden zur Verhinderung von Geldwäsche und Betrug im Sinne der §§ 10 ff. GwG öffentlich verfügbare Informationen geprüft. Dies wird durch die in 26. genannten Systeme unterstützt und dient ausschließlich der Erfüllung aufsichtsrechtlicher Anforderungen. Die abschließende Beurteilung erfolgt durch autorisierte Mitarbeitende der Bank; eine automatisierte Entscheidung mit Rechtswirkung gegenüber dem Kunden findet nicht statt.

Jeder Kunde oder Interessent hat das Recht, eine persönliche Überprüfung der automatisierten Einzelentscheidung zu verlangen.

27. Überprüfung der Kreditwürdigkeit

Bei der Vergabe eines Kredites sowie während der Laufzeit des Kredites ist die Bank dazu verpflichtet, die Kreditwürdigkeit des Kunden zu überprüfen. Rechtsgrundlage ist bei der Überprüfung der Kreditwürdigkeit im Rahmen der Eröffnung die Verarbeitung aufgrund rechtlicher Verpflichtung Art. 6 Abs. 1 lit. c DSGVO i.V.m § 505 a BGB sowie im Rahmen der Laufzeit Art. 6 Abs. 1 lit. b Verarbeitung aufgrund der Vertragserfüllung.

Bei der Eröffnung eines Girokontos wird die Bonität des jeweiligen Kunden anhand von dessen SCHUFA Bonitätsdaten überprüft. Ob und in welcher Höhe im Zuge der Eröffnung eines Girokontos ein Dispokredit eingeräumt wird, hängt u.a. von dem sog. SCHUFA Score sowie von weiteren eventuell vorhandenen SCHUFA-Merkmalen ab (siehe VI. dieser Bedingungen). Die zugehörigen Datenschutzerklärungen der SCHUFA finden Sie hier: www.schufa.de/datenschutz

Sofern automatisiert kein Angebot zu einem Dispokredit erstellt werden konnte, hat der Kunde jederzeit die Möglichkeit eine individuelle Prüfung seines Anliegens beim Kundenservice anzufragen.

Neben dem Dispokredit bei Girokontoeröffnung kann der Kunde einen individuell zu seinem jeweiligen Risikoscore angepassten Dispokredit abschließen. Sofern ein Kunde die Möglichkeit eines individuellen Dispokredits oder eines Ratenkredits nutzt, findet im Vergabeprozess eine erneute Bonitätsüberprüfung anhand von SCHUFA-Bonitätsdaten und mittels eines bankinternen Risiko-Scores statt.

Der bankinterne Risiko-Score setzt sich insbesondere aus der Höhe des sog. SCHUFA Scores sowie Transaktionsdaten des Girokontos zusammen. Dabei wird die Wahrscheinlichkeit berechnet, mit der ein Kunde seinen Zahlungsverpflichtungen vertragsgemäß nachkommt. Berücksichtigt werden in der

Berechnung die Einnahmen- und Ausgabenverhältnisse des Kunden sowie Informationen über bestehende Vertragsbeziehungen.

Im Rahmen des Angebotsprozesses für den „Ratenkauf“ und den „Kauf auf Rechnung“ wird die Bonität des Kunden ebenfalls anhand eines Scorings überprüft.

Das Scoring beruht auf einem mathematisch-statistisch anerkannten und bewährten Verfahren und ist für den Abschluss oder die Erfüllung des Kreditvertrags (Dispokredit und auch Ratenkredit) erforderlich (Art. 22 Abs. 2 lit. a und Abs. 3 DSGVO und § 31 Abs. 1 BDSG). 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.

Nach Erteilung eines individuellen Dispokredits als auch eines Ratenkredits überprüft die Bank in regelmäßigen Abständen automatisiert, ob der jeweilige Kunde noch die Bonitätsbedingungen des Dispokredits erfüllt, oder ob die Möglichkeit einer Dispoerhöhung besteht.

X. Widerspruchsrecht

28. 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.

29. 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.

XI. Rechte der betroffenen Person

Es bestehen die folgenden Rechte im Zuge der Verarbeitung von personenbezogenen Daten:

- Recht auf Auskunft nach Art. 15 DSGVO,
- Berichtigung nach Art. 16 DSGVO,
- Löschung nach Art. 17 DSGVO,
- Einschränkung der Verarbeitung nach Art. 18 DSGVO sowie
- Datenübertragbarkeit aus Art. 20 DSGVO.

Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach Art. 12 und 15 DSGVO i. V. m. § 34 BDSG und Art. 17 DSGVO i. V. m. § 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Artikel 77 DSGVO i. V. m § 19 BDSG).

Anfragen können an den Kundenservice innerhalb der C24 Bank App oder an den Datenschutzbeauftragten der Bank (datenschutz@c24.de) gestellt werden.

XII. Aufbewahrungs- und Löschfristen

Grundsätzlich verarbeitet und speichert die Bank personenbezogene Daten nur solange es für die Erfüllung von vertraglichen, vorvertraglichen und gesetzlichen Pflichten erforderlich ist. Das heißt, sind die Daten für die Erfüllung dieser Pflichten nicht mehr erforderlich, z. B. bei Kündigung eines Girokontos, der Deaktivierung optional aktivierbarer Funktionalitäten innerhalb der C24 Bank App oder einer 30-tägigen Inaktivität im Rahmen der Antragstellung zur Kontoeröffnung, werden diese regelmäßig gelöscht, es sei denn, ihre (befristete) Weiterverarbeitung ist z. B. zu folgenden Zwecken erforderlich:

- Erfüllung handels- und steuerrechtlicher Aufbewahrungsfristen, die sich aus folgenden Gesetzen ergeben: Handelsgesetzbuch, Abgabenordnung, Kreditwesengesetz, Geldwäschegesetz und Wertpapierhandelsgesetz. Die dort vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen zwei bis zehn Jahre.
- Wurden Kontoanträge über einen Marketing-Partner der C24 Bank initiiert (z. B. über Vergleichsportale oder sonstige Kooperationspartner), werden die im Rahmen des Antragsprozesses erhobenen Daten für eine Dauer von bis zu 90 Tagen aufbewahrt. Dies ist erforderlich, um die Vermittlungsleistung des Partners nachzuweisen. Die Rechtsgrundlage hierfür ergibt sich aus Art. 6 Abs. 1 lit. f DSGVO (berechtigte Interessen der Bank bzw. des Partners). Nach Ablauf dieser Frist werden die Daten gelöscht, sofern keine anderweitigen gesetzlichen Aufbewahrungspflichten entgegenstehen.
- Mit Verweis auf § 8 GwG ist die Bank verpflichtet, im Falle jeder Einbindung eines Bank-Kontos im Rahmen des Multibankings (siehe Nummer 15 dieser Bedingungen), die zugehörige IBAN des Nutzers, verbunden mit dem Zeitpunkt der ersten Einbindung, für mindestens 5 Jahre zu speichern. Diese Frist beginnt mit dem Schluss des Kalenderjahres, in dem die Geschäftsbeziehung endet bzw. in dem der Kunde die Option „Multibanking“ (siehe Nummer 15 dieser Bedingungen) deaktiviert.
- Im Falle von Krediten und Anlagen ist zu beachten, dass die Geschäftsbeziehung zwischen Kunde und Bank ein Dauerschuldverhältnis darstellt, dessen Dauer in erster Linie durch die vom Kunden gewählte Laufzeit bestimmt wird, zum Beispiel:
    - Ratenkredit 24 bis 84 Monate oder
    - Anlagedauer im Einlagengeschäft
- Erhaltung von Beweismitteln im Rahmen der Verjährungsvorschriften. Nach den §§ 195 ff. des Bürgerlichen Gesetzbuches (BGB) können diese Verjährungsfristen bis zu 30 Jahre betragen, wobei die regelmäßige Verjährungsfrist drei Jahre beträgt. Die Rechtsgrundlage hierzu ergibt sich aus Art. 17 Abs. 3 lit. e DSGVO, Art. 6 Abs. 1 lit. f DSGVO.