Frankfurter Bankgesellschaft
PRIVATBANK I Zürich I Frankfurt

Datenschutzhinweise

Informationen nach Artikeln 13, 14 und 21 Datenschutz-Grundverordnung – EU-DSGVO

Stand: Oktober 2022

Mit den nachfolgenden Informationen möchten wir Ihnen (nachfolgend: Kundin bzw. Kunde) einen Überblick über die Verarbeitung ihrer personenbezogenen Daten durch uns (nachfolgend: Bank) und ihrer Rechte aus dem Datenschutzrecht geben. Welche Daten im Einzelnen verarbeitet und in welcher Weise genutzt werden, richtet sich maßgeblich nach den jeweils von Ihnen beantragten bzw. mit Ihnen vereinbarten Dienstleistungen.

Wer ist für die Datenverarbeitung verantwortlich und an wen kann sich die Kundin bzw. der Kunde wenden?

Verantwortliche Stelle ist:

Frankfurter Bankgesellschaft (Deutschland) AG

Junghofstraße 26

60311 Frankfurt am Main

Deutschland

Sie erreichen unsere/n Datenschutzbeauftragte/-n unter:

Frankfurter Bankgesellschaft (Deutschland) AG

Datenschutzbeauftragter

Junghofstraße 26

60311 Frankfurt am Main

E-Mail: datenschutz.de@frankfurter-bankgesellschaft.com

Welche Quellen und Daten nutzt die Frankfurter Bankgesellschaft?

Die Bank verarbeitet personenbezogene Daten, die sie im Rahmen der Geschäftsbeziehung von Kundinnen und Kunden oder anderen Betroffenen erhält. Zudem verarbeitet die Bank – soweit für die Erbringung ihrer Dienstleistung erforderlich – personenbezogene Daten, die sie von anderen Unternehmen der Sparkassen-Finanzgruppe oder von sonstigen Dritten zulässigerweise (z. B. zur Ausführung von Aufträgen, zur Erfüllung von Verträgen oder aufgrund einer erteilten Einwilligung)

erhalten hat. Zum anderen verarbeitet die Bank personenbezogene Daten, die sie aus öffentlich zugänglichen Quellen (z. B. Schuldnerverzeichnissen, Grundbüchern, Handels- und Vereinsregistern, Presse, Medien) zulässigerweise gewonnen hat. Relevante personenbezogene Daten im Interessentenprozess, bei der Eröffnung einer Vertragsbeziehung, im Zuge einer Bevollmächtigung (Depot-/ Kontovollmacht) oder als Verfügungsberechtigte eines Depots/Vertrages können sein:

Name, Adresse und andere Kontaktdaten (z.B. Telefon, E-Mail-Adresse), Geburtsdatum/-ort, Geschlecht, Staatsangehörigkeit, Sprache, Familienstand, Geschäftsfähigkeit, Berufsgruppenschlüssel, wirtschaftliche und steuerliche Angaben (z.B. unselbständig/selbständig, Steuerdomizil), Legitimationsdaten (z. B. Bild, Ausweisdaten/-kopie), Authentifikationsdaten (z. B. Unterschriftprobe), Steuer-ID, FATCA-Status. Bei Nutzung des Diensts S-Videolegitimation werden weitere Daten wie z.B. Audio- und Videomitschnitte im Legitimationsvorgang durch unseren Kooperationspartner S-Markt & Mehrwert GmbH & Co. KG erhoben. Die vollständigen Datenschutzhinweise sind im Absatz zur S-Videolegitimation beschrieben.

Bei Abschluss und Nutzung von Produkten/Dienstleistungen aus den im Folgenden aufgelisteten Produktkategorien können zusätzlich zu den vorgenannten Daten weitere personenbezogene Daten erhoben, verarbeitet und gespeichert werden. Diese umfassen im Wesentlichen:

Vermögensverwaltung /Anlageberatung/Beratungsfreies Geschäft

Gegenwärtiger oder früherer Beruf, detaillierte Angaben zu Kenntnissen und/oder Erfahrungen mit Wertpapieren (MiFID-Status), Anlageverhalten/-strategie (Umfang, Häufigkeit, Risikobereitschaft), finanzielle Situation (Vermögen, Verbindlichkeiten, Einkünfte, Ausgaben), absehbare Änderungen in den Vermögensverhältnissen (z. B. Eintritt in den Ruhestand), steuerliche Informationen (z. B. US-Quellensteuer-Zwecke), Dokumentationsdaten (z. B. frühere Beratungsprotokolle bzw. Geeignetheitsberichte), Auftragsdaten (z. B. Zahlungsauftrag, Wertpapierauftrag).

Weitere Korrespondenz- und Kommunikationsdaten

Im Rahmen der Geschäftsbeziehung, insbesondere durch persönliche, telefonische oder schriftliche Kontakte, durch die Kundin bzw. den Kunden oder durch die Bank initiiert, entstehen weitere personenbezogene Daten, z. B. Informationen über Kontaktkanäle, Datum, Anlass und Ergebnis, (elektronische) Kopien des Schriftverkehrs sowie Informationen im Rahmen von Werbemaßnahmen.

Sofern Sie sich zur telefonischen Annahme, Übermittlung oder Ausführung von Aufträgen in Zusammenhang mit Wertpapier(neben)-dienstleistungen entscheiden, speichern wir auch Tonaufnahmen von Telefongesprächen. Dies erfolgt dabei auf Grundlage von gesetzlichen Vorgaben. Bei der Aufzeichnung werden neben dem Gesprächsinhalt auch technische Informationen gespeichert (z.B. Verbindungsdauer, Rufnummern).

Wofür verarbeitet die Bank die Daten der Kundin bzw. des Kunden (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage?

Die Bank verarbeitet personenbezogene Daten im Einklang mit den Bestimmungen der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) und dem Bundesdatenschutzgesetz (BDSG):

(1) Zur Erfüllung von vertraglichen Pflichten (Art. 6 Abs. 1 Buchst. b EU-DSGVO)

Die Verarbeitung personenbezogener Daten (Art. 4 Nr. 2 EU-DSGVO) erfolgt zur Erbringung und Vermittlung von Geschäften und Finanzdienstleistungen zur Durchführung der Verträge oder vorvertraglichen Maßnahmen mit der Kundin bzw. dem Kunden und der Ausführung ihrer Aufträge sowie aller mit dem Betrieb und der Verwaltung eines Kredit- oder Finanzdienstleistungsinstituts erforderlichen Tätigkeiten.

Die Zwecke der Datenverarbeitung richten sich in erster Linie nach dem konkreten Produkt (z. B. Konto, Kredit, Wertpapiere, Einlagen, Vermittlung) und können unter anderem Bedarfsanalysen, Beratung, Vermögensverwaltung und -betreuung sowie die Durchführung von Transaktionen umfassen.

(2) Im Rahmen der Interessenabwägung (Art. 6 Abs. 1 Buchst. f EU-DSGVO)

Soweit erforderlich, verarbeitet die Bank die Daten der Kundin bzw. des Kunden über die eigentliche Erfüllung des Vertrages hinaus zur Wahrung berechtigter Interessen der Bank oder Dritter. Beispiele:

- Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten;
- Gewährleistung der IT-Sicherheit und der Aufrechterhaltung sowie Weiterentwicklung des IT-Betriebs der Bank;
- Verhinderung und Aufklärung von Straftaten;
- Wahrung der Bank vor Reputationsschäden;
- Maßnahmen zur Gebäude- und Anlagensicherheit (z. B. Zutrittskontrollen);
- Videoüberwachung zur Wahrung des Hausrechts und Sammlung von Beweismitteln für besonders schutzbedürftige Räume;
- Maßnahmen zur Geschäftssteuerung und zur Weiterentwicklung von Dienstleistungen und Produkten;
- Risikosteuerung im Konzern;
- Bereitstellung der Webseite.

(3) Aufgrund der Einwilligung der Kundin bzw. des Kunden (Art. 6 Abs. 1 Buchst. a EU-DSGVO)

Soweit die Kundin bzw. der Kunde der Bank eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke (z. B. Vermittlung an Kooperationspartner, Weitergabe von Daten im Verbund/Konzern) erteilt hat, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis der Einwilligung gegeben. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Dies

gilt auch für den Widerruf von Einwilligungserklärungen, die vor Geltung der EU-DSGVO der Bank gegenüber erteilt worden sind.

Die Bank bittet die Kundin bzw. den Kunden zu beachten, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

(4) Aufgrund gesetzlicher Vorgaben (Art. 6 Abs. 1 Buchst. c EU-DSGVO)

Zudem unterliegt die Bank diversen rechtlichen Verpflichtungen, das heißt gesetzlichen Anforderungen (z. B. Kreditwesengesetz, Geldwäschegesetz, Wertpapierhandelsgesetz, Steuergesetze) sowie bankenaufsichtsrechtlichen Vorgaben (z. B. der Europäischen Zentralbank, der Europäischen Bankenaufsicht, der Deutschen Bundesbank und der Bundesanstalt für Finanzdienstleistungsaufsicht). Zu den Zwecken der Verarbeitung gehören unter anderem die Identitätsprüfung, Betrugs- und Geldwäscheprävention, die Erfüllung steuerrechtlicher Kontroll- und Meldepflichten sowie die Bewertung und Steuerung von Risiken in der Bank und im Konzern.

Wer bekommt die Daten der Kundin bzw. des Kunden?

Innerhalb der Bank erhalten diejenigen Stellen Zugriff auf die Daten der Kundin bzw. des Kunden, die diese zur Erfüllung der vertraglichen und gesetzlichen Pflichten brauchen. Auch durch die Bank eingesetzte Auftragsverarbeiter (Art. 28 EU-DSGVO) können zu diesen genannten Zwecken Daten erhalten, wenn diese die Vertraulichkeit und die datenschutzrechtlichen Weisungen wahren. Im Hinblick auf die Datenweitergabe an Empfänger außerhalb der Bank ist zunächst zu beachten, dass die zwischen der Kundin bzw. dem Kunden und der Bank vereinbarten Allgemeinen Geschäftsbedingungen die Bank zur Verschwiegenheit über alle die Kundin bzw. den Kunden bezogenen Tatsachen und Wertungen verpflichten, von denen sie Kenntnis erlangt (Bankgeheimnis). Informationen über die Kundin bzw. den Kunden dürfen durch die Bank nur weitergeben werden, wenn vertragliche oder gesetzliche Bestimmungen dies gebieten oder die Kundin bzw. der Kunde eingewilligt hat.

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, Bundeszentralamt für Steuern, Staatsanwaltschaft) bei Vorliegen einer gesetzlichen oder behördlichen Verpflichtung.
- Andere Kredit- und Finanzdienstleistungsinstitute oder vergleichbare Einrichtungen und Auftragsverarbeiter, die zur Durchführung der Geschäftsbeziehung personenbezogene Daten erhalten (je nach Vertrag: z. B. Korrespondenzbanken, Depotbanken, Börsen und sonstige Dienstleister).

Weitere Datenempfänger können diejenigen Stellen sein, für die die Kundin bzw. der Kunde der Bank eine Einwilligung zur Datenübermittlung erteilt hat (z. B. Kooperationspartner) bzw. für die die

Kundin bzw. der Kunde die Bank vom Bankgeheimnis gemäß Vereinbarung oder Einwilligung befreit hat.

Zwecke der Datenweitergabe sind unter anderen:

- Abwicklung von Behördenanfragen,
- Unterstützung/Betrieb/Wartung von EDV-/IT-Anwendungen,
- Archivierung,
- Belegbearbeitung,
- Controlling,
- Datenscreening für Anti-Geldwäsche-Zwecke,
- Datenvernichtung,
- Einkauf/Beschaffung,
- Kundenverwaltung,
- Marketing,
- Research,
- Risikocontrolling,
- Telefonie,
- Webseitenmanagement,
- Wertpapierdienstleistungen,
- Aktienregister,
- Fondsverwaltung,
- Wirtschaftsprüfungsdienstleistung,
- Zahlungsverkehr.

Wie lange werden die Daten der Kundin bzw. des Kunden gespeichert?

Soweit erforderlich, verarbeitet und speichert die Bank personenbezogene Daten für die Dauer der gemeinsamen Geschäftsbeziehung, was beispielsweise auch die Anbahnung und die Abwicklung eines Vertrages umfasst. Dabei ist zu beachten, dass die Geschäftsbeziehung ein Dauerschuldverhältnis ist, welches auf Jahre angelegt ist. Darüber hinaus unterliegt die Bank verschiedenen Aufbewahrungs- und Dokumentationspflichten, die sich unter anderem aus dem Handelsgesetzbuch (HGB), der Abgabenordnung (AO), dem Kreditwesengesetz (KWG), dem Geldwäschegesetz (GwG) und dem Wertpapierhandelsgesetz (WpHG) ergeben. Die dort

vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen bis zu 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 30 Jahre betragen können.

Für die Aufzeichnung telefonischer und elektronischer Kommunikation, die im Rahmen der Erbringung von Wertpapier(neben)-dienstleistungen erfolgt, gilt eine gesetzliche Aufbewahrungsfrist von fünf Jahren, bei aufsichtsbehördlicher Anordnung im Einzelfall auch für bis zu sieben Jahre.

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

Eine Datenübermittlung in Drittstaaten (Staaten außerhalb des Europäischen Wirtschaftsraums – EWR[1]) findet nur statt, soweit dies zur Ausführung der Aufträge (z. B. Zahlungs- und Wertpapieraufträge) erforderlich ist, gesetzlich vorgeschrieben ist (z. B. steuerrechtliche Meldepflichten), die Kundin bzw. der Kunde eine Einwilligung erteilt hat oder im Rahmen einer Auftragsdatenverarbeitung erfolgt. Werden Dienstleister im Drittstaat eingesetzt, sind diese durch die Vereinbarung der EU-Standardvertragsklauseln zur Einhaltung des Datenschutzniveaus in Europa verpflichtet.

Welche Datenschutzrechte hat die Kundin bzw. der Kunde?

Jede betroffene Person hat das Recht auf Auskunft nach Art. 15 EU-DSGVO, das Recht auf Berichtigung nach Art. 16 EU-DSGVO, das Recht auf Löschung nach Art. 17 EU-DSGVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 EU-DSGVO sowie das Recht auf Datenübertragbarkeit aus Art. 20 EU-DSGVO. Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Art. 77 DS-GVO i. V. m. § 19 BDSG) oder dem Datenschutzbeauftragten der Bank.

Besteht für die Kundin bzw. den Kunden eine Pflicht zur Bereitstellung von Daten?

Im Rahmen der Geschäftsbeziehung müssen nur diejenigen personenbezogenen Daten bereitgestellt werden, die für die Aufnahme und Durchführung einer Geschäftsbeziehung und die Erfüllung der damit verbundenen vertraglichen Pflichten erforderlich sind oder zu deren Erhebung die Bank gesetzlich verpflichtet ist. Ohne diese Daten wird die Bank in der Regel den Abschluss des Vertrages oder die Ausführung des Auftrages ablehnen müssen oder einen bestehenden Vertrag nicht mehr durchführen können und ggf. beenden müssen. Insbesondere ist die Bank nach den geldwäscherechtlichen Vorschriften verpflichtet, die Kundin bzw. den Kunden vor der Begründung

der Geschäftsbeziehung, beispielsweise anhand des Personalausweises, zu identifizieren und dabei den Namen, den Geburtsort, das Geburtsdatum, die Staatsangehörigkeit sowie die Wohnanschrift zu erheben und festzuhalten. Damit die Bank dieser gesetzlichen Verpflichtung nachkommen kann, hat die Kundin bzw. der Kunde der Bank die nach dem Geldwäschegesetz notwendigen Informationen und Unterlagen zur Verfügung zu stellen und sich im Laufe der Geschäftsbeziehung ergebende Änderungen unverzüglich anzuzeigen. Sollte die Kundin bzw. der Kunde der Bank die notwendigen Informationen und Unterlagen nicht zur Verfügung stellen, darf die Bank die von der Kundin bzw. dem Kunden gewünschte Geschäftsbeziehung nicht aufnehmen oder fortsetzen.

S-Videolegitimation: Die Bereitstellung der Legitimationsdaten kann auch online durch die Nutzung des Dienstes S-Videolegitimation erfolgen. Die S-Videolegitimation wird dabei im Auftrag der Bank durch die S-Markt & Mehrwert GmbH & Co. KG (Auftragsverarbeiter) mit Sitz in Halle durchgeführt. Für die technische Umsetzung kooperiert die S-Markt & Mehrwert GmbH & Co. KG mit dem IT-Systembetreiber IDnow GmbH in München. Die Datenerhebung und -speicherung erfolgt dabei ausschließlich in Deutschland und wird ausschließlich zum Zweck der Identifizierung der Betroffenen, auf Grund der gesetzlichen Verpflichtung zur Legitimationsprüfung sowie zur weiteren Vertragserfüllung vorgenommen. Für die Durchführung der Online-Legitimationsprüfung benötigt die Bank zusätzlich die Einwilligung der betroffenen Person nach Art. 6 Abs. 1 lit. a) EU-DSGVO, aufgrund der Erhebung weiterer persönlicher Daten durch Aufzeichnung (z. B. Video, Ton und Bild). Vor Beginn der S-Videolegitimation wird die betroffene Person deshalb aufgefordert, ihre Einwilligung in die Aufzeichnung zu geben. Sofern sie nicht einwilligt, wird die Legitimationsprüfung durch eine Beraterin bzw. einen Berater der Bank durchgeführt. Eine erteilte Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Aus rechtlichen Gründen ist bei Widerruf eine erneute Legitimationsprüfung durch die Bank notwendig.

Im Rahmen des Online-Legitimationsvorgangs werden folgende personenbezogene Daten verarbeitet:

Identifizierungsdaten, wie z. B. Name, Vorname, Adresse, E-Mail-Adresse, Mobilfunknummer, Geburtsdatum und -ort. Des Weiteren werden Legitimationsdaten der betroffenen Person wie z. B. Bilder des Ausweisdokuments und der Sicherheitsmerkmale, Bild der Person, Ausweisnummer, Ausstellungsbehörde und -datum, Audio- und Videomitschnitte, TAN sowie die Kommunikationsdaten des Videolegitimationsvorgangs (IP-Adresse, Dauer und Datum der Verbindung) erhoben und verarbeitet. Die erhobenen Identifizierungs- und Legitimationsdaten werden bis zu zehn Jahren nach der Beendigung der Geschäftsbeziehung aufbewahrt. Die Speicherfrist beginnt mit Ablauf des Kalenderjahres, in dem die Geschäftsbeziehung endet. Die TAN wird unmittelbar nach dem Vorgang, die Kommunikationsdaten werden 15 Tage nach dem Legitimationsvorgang gelöscht. Der Auftragsverarbeiter löscht die Daten unmittelbar nach Abruf der Daten durch die Bank. Die Datenübertragung erfolgt auf Grundlage aktueller Sicherheitsstandards (Verschlüsselung). Bei Abbruch des Legitimationsprozesses werden alle im Verfahren erhobenen Daten gelöscht.

Nutzung des elektronischen Kundenportals: Sofern sich die Kundin bzw. der Kunde zur Nutzung des elektronischen Kundenportals mit dem Elektronischen Postfach entscheidet, verarbeitet die

Bank nachfolgende personenbezogene Daten zur Registrierung, Anmeldung und Nutzung des Kundenportals: Login-User, Passwort, E-Mail-Adresse sowie Name und Vorname.

Die Bank verarbeitet die personenbezogenen Daten von Kundinnen, Kunden und Geschäftspartnern nur zum Zweck der elektronischen Bereitstellung von Vertrags-, Vermögens-, Kundeninformations- und Geschäftsunterlagen. Die Datenverarbeitung erfolgt zur Erfüllung gesetzlicher Vorgaben auf Basis des bestehenden Vertrags gem. Art. 6 Abs. 1 lit. b EU-DSGVO. Zum Zweck der Bereitstellung des elektronischen Kundenportals bietet die Bank eine Kundenportal-Hotline über die KPMG AG Wirtschaftsgesellschaft an. Bei Inanspruchnahme der Kundenportal-Hotline wird technischer Support zur Einrichtung und Bedienung des Kundenportals erbracht. Die Kundenportal- Hotline verarbeitet dazu lediglich den Namen der anrufenden Person sowie ggf. ihre E-Mail-Adresse, sofern der Austausch weiterer Informationen notwendig ist. Eine Datenweitergabe an Dritte - bei Nutzung der Kundenportal-Hotline - erfolgt nicht.

Jeder Nutzerin und jedem Nutzer wird im Rahmen der Registrierung ein Profil eingerichtet (Login-User, Passwort), mit dem der die Nutzerin bzw. der Nutzer sich am Kundenportal anmelden kann. Für eine sichere Authentifizierung der Nutzerin bzw. des Nutzers am Kundenportal wird zusätzlich ein zweiter Faktor benötigt, der über eine eigene Authentifizierungs-App erzeugt wird. Diese App generiert einen sechsstelligen PIN-Code, der im Rahmen der Anmeldung für eine erfolgreiche Authentifizierung durch die Nutzenden des Kundenportals zusätzlich eingetragen werden muss. Zur Zustellung des PIN-Codes muss die App auf einem Endgerät der Nutzerin bzw. des Nutzers installiert sein und der bei der Erstregistrierung zugestellte QR-Code einmalig gescannt werden. Der QR-Code enthält eine einmalige individuelle Kennung (ID), die eine Verbindung zum Kundenportal herstellt, welche nach Verwendung gelöscht wird. Die Bank speichert die Anmelde- und Registrierungsdaten sowie die zugehörigen Dokumente der Nutzenden in eigenen Rechenzentren in Deutschland und nur zum Zweck der Bereitstellung der oben beschriebenen Dienstleistung. Eine Weitergabe dieser Daten erfolgt nicht. Das Kundenportal ist durch die Zwei-Faktor-Anmeldung und eine verschlüsselte Datenübertragung sicher geschützt. Einen Zugriff auf diese Daten und die zugehörigen Informationen und Dokumente im Kundenportal haben lediglich die Nutzenden selbst sowie die entsprechend autorisierten Mitarbeitenden der Bank. Sofern die Nutzerin bzw. der Nutzer das Kundenportal nicht mehr benötigen, werden die Nutzerdaten zum Kundenportal umgehend gelöscht und die bereitgestellten Unterlagen im Rahmen der Aufbewahrungsfristen gespeichert.

Inwieweit gibt es eine automatisierte Entscheidungsfindung im Einzelfall?

Zur Begründung und Durchführung der Geschäftsbeziehung nutzt die Bank grundsätzlich keine automatisierte Entscheidungsfindung gemäß Art. 22 EU-DSGVO. Sollten diese Verfahren in Einzelfällen eingesetzt werden, wird die Bank die Kundin bzw. den Kunden hierüber gesondert informieren, sofern dies gesetzlich vorgegeben ist.

Inwieweit werden die Daten der Kundin bzw. des Kunden für die Profilbildung (Scoring) genutzt?

Die Bank verarbeitet die Daten der Kundin bzw. des Kunden teilweise automatisiert mit dem Ziel, bestimmte persönliche Aspekte zu bewerten (Profiling). Die Bank setzt Profiling beispielsweise in folgenden Fällen ein:

Aufgrund gesetzlicher und regulatorischer Vorgaben ist die Bank zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und vermögensgefährdenden Straftaten verpflichtet. Dabei werden auch Datenauswertungen (u. a. im Zahlungsverkehr) vorgenommen. Diese Maßnahmen dienen zugleich auch dem Schutz der Kundin bzw. des Kunden.

Informationen über das Widerspruchsrecht der Kundin bzw. des Kunden nach Art. 21 Datenschutz-Grundverordnung (EU-DSGVO)

(1) Einzelfallbezogenes Widerspruchsrecht

Die Kundin bzw. der Kunde hat das Recht, aus Gründen, die sich aus der besonderen Situation der Kundin bzw. des Kunden ergeben, jederzeit gegen die Verarbeitung der personenbezogenen Daten, die aufgrund von Artikel 6 Absatz 1 Buchstabe f der EU-DSGVO (Datenverarbeitung auf der Grundlage einer Interessenabwägung) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling im Sinne von Art. 4 Nr. 4 EU-DSGVO, das die Bank zur Bonitätsbewertung oder für Werbezwecke einsetzt.

Legt die Kundin bzw. der Kunde Widerspruch ein, wird die Bank die personenbezogenen Daten nicht mehr verarbeiten, es sei denn, die Bank kann zwingende berechtigte Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der Kundin bzw. des Kunden überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(2) Widerspruchsrecht gegen eine Verarbeitung von Daten für Werbezwecke

In Einzelfällen verarbeitet die Bank personenbezogene Daten, um den Kundinnen bzw. den Kunden individuelle Angebote zu unterbreiten. Die Kundin bzw. der Kunde haben das Recht, jederzeit Widerspruch gegen die Verarbeitung der betreffenden personenbezogenen Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

Widerspricht die Kundin bzw. der Kunde der Verarbeitung für Zwecke der Direktwerbung, so wird die Bank die personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten.

Der Widerspruch kann formfrei erfolgen und sollte möglichst gerichtet werden an:

Frankfurter Bankgesellschaft (Deutschland) AG

Datenschutzbeauftragter

Junghofstraße 26

60311 Frankfurt am Main

Hinweise

1 Zum Europäischen Wirtschaftsraum gehören derzeit: Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich (einschließlich Französisch-Guayana, Guadeloupe, Martinique, Mayotte, Réunion), Griechenland, Irland, Island, Italien, Kroatien, Lettland, Liechtenstein, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich von Großbritannien und Nordirland, Zypern.