

Unser Umgang mit Ihren Daten und Ihre Rechte
Informationen nach Artikeln 13, 14 und 21 der EU-Datenschutz-Grundverordnung –
(DSGVO)
Stand: Mai 2025

A. Datenverarbeitung im Allgemeinen

Mit den nachfolgenden Informationen geben wir Ihnen einen Überblick über die Verarbeitung Ihrer personenbezogenen Daten durch uns und Ihre Rechte aus dem Datenschutzrecht. 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.

1. Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich 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
Datenschutzbeauftragte/r
Junghofstraße 26
60311 Frankfurt am Main
Deutschland
E-Mail-Adresse: datenschutz.de@frankfurter-bankgesellschaft.com

2. Welche Quellen und Daten nutzen wir?

Wir verarbeiten personenbezogene Daten, die wir im Rahmen unserer Geschäftsbeziehung von Ihnen erhalten. Zudem verarbeiten wir – soweit für die Erbringung unserer Dienstleistung erforderlich – personenbezogene Daten, die wir von anderen Unternehmen der Sparkassen-Finanzgruppe oder von sonstigen Dritten zulässigerweise (z.B. zur Ausführung von Aufträgen, zur Erfüllung von Verträgen oder aufgrund einer von Ihnen erteilten Einwilligung) erhalten haben. Zum anderen verarbeiten wir personenbezogene Daten, die wir aus öffentlich zugänglichen Quellen (z.B. Schuldnerverzeichnisse, Grundbücher, Handels- und Vereinsregister, Presse, Medien) zulässigerweise gewonnen haben.

Relevante personenbezogene Daten im Interessentenprozess, bei der Eröffnung einer Vertragsbeziehung, im Zuge einer Bevollmächtigung (Depot-/Kontovollmacht) oder einer Verfügungsberechtigung können sein:

Name, Adresse und andere Kontaktdaten (Telefon, E-Mail-Adresse, Geburtsdatum/-ort, Geschlecht, Staatsangehörigkeit, Sprache, Familienstand, Geschäftsfähigkeit/Handlungsfähigkeit, Berufsgruppenschlüssel, wirtschaftliche und steuerliche Angaben (z.B. unselbständig/selbständig, steuerlicher Wohnsitz, Steuerdomizil), Legitimationsdaten (z.B. Ausweisdaten/-kopie), Herkunft von Vermögenswerten, ggf. Einfluss auf und Kontrolle von juristischen Personen, Authentifikationsdaten (z.B. Unterschriftprobe), Steuer-ID, FATCA-Status.

Bei Nutzung des Dienstes S-Videolegitimation werden weitere Daten wie z.B. Bild, Audio- und Videomitschnitte im Legitimationsvorgang durch unseren Auftragsverarbeiter S-Markt & Mehrwert GmbH & Co. KG, Grenzstr. 21, 06112 Halle, erhoben. Die vollständigen Informationen finden Sie auch unter Punkt 8 beschrieben.

Zur Identifizierung der Kunden/Interessenten kann auch der Service der Deutsche Post AG, Charles-de-Gaulles-Str. 20, 53113 Bonn, als Auftragsverarbeiter genutzt werden. Die Deutsche Post AG übernimmt für die Frankfurter Bankgesellschaft (Deutschland) AG die Bereitstellung und den Betrieb des POSTIDENT-Portals, die Datenbereitstellung, den technischen Support und das POSTIDENT-Verfahren in einer Postfiliale.

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), Anlageverhalten/-strategie (Umfang, Häufigkeit, Risikobereitschaft), finanzielle Situation (Vermögen, Verbindlichkeiten, Einkünfte, Ausgaben), absehbare Änderungen in den Vermögensverhältnissen (z.B. Eintritt Rentenalter), steuerliche Informationen (z.B. für US-Quellensteuer-Zwecke), Dokumentationsdaten (z.B. Geeignetheitserklärungen), Auftragsdaten (z.B. Zahlungsauftrag, Wertpapierauftrag).

Weitere Korrespondenz- und Kommunikationsdaten können im Rahmen der Geschäftsbeziehung, insbesondere durch persönliche, telefonische oder schriftliche Kontakte, durch Sie oder von der Bank initiiert, entstehen, z.B. Informationen über Kontaktkanäle, Datum, Anlass und Ergebnis, (elektronische) Kopien des Schriftverkehrs sowie Informationen im Rahmen von werblichen Maßnahmen. 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).

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

Wir verarbeiten personenbezogene Daten im Einklang mit den Bestimmungen der DSGVO und dem Bundesdatenschutzgesetz (BDSG)

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

Die Verarbeitung personenbezogener Daten erfolgt zur Erbringung und Vermittlung von Bankgeschäften und Finanzdienstleistungen zur Durchführung unserer Verträge oder vorvertraglichen Maßnahmen mit Ihnen und der Ausführung Ihrer Aufträge sowie aller mit dem Betrieb und der Verwaltung eines Kreditinstituts 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.

3.2 Im Rahmen der Interessenabwägung (Art. 6 Abs. 1 Buchst. f DSGVO)

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

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 Weiterentwicklung von Dienstleistungen und Produkten
- Risikosteuerung im Konzern
- Bereitstellung der Webseite

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

Soweit Sie uns eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke (z.B. werbliche Ansprache, Vermittlung an Kooperationspartner, Weitergabe von Daten im Verbund/Konzern) erteilt haben, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis Ihrer Einwilligung gegeben. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der DSGVO uns gegenüber erteilt worden sind.

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

3.4 Aufgrund gesetzlicher Vorgaben (Art. 6 Abs. 1 Buchst. c DSGVO)

Zudem unterliegen wir als 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 Identitätsüberprüfung, Betrugs- und Geldwäscherprävention, die Erfüllung steuerrechtlicher Kontroll- und Meldepflichten sowie die Bewertung und Steuerung von Risiken in der Bank und im Konzern.

4. Wer erhält meine Daten?

Innerhalb der Bank erhalten diejenigen Stellen Zugriff auf Ihre personenbezogenen Daten, die diese zur Erfüllung der Verarbeitungszwecke benötigen. Auch von uns eingesetzte Dienstleister und Auftragsverarbeiter können hierzu Ihre personenbezogenen Daten erhalten.

Im Hinblick auf die Datenweitergabe an weitere Empfänger außerhalb der Bank ist zunächst zu beachten, dass wir als Bank zur Verschwiegenheit über alle kundenbezogenen Tatsachen und Wertungen verpflichtet sind, von denen wir Kenntnis erlangen (Bankgeheimnis). Informationen über Sie dürfen wir grundsätzlich nur weitergeben, wenn eine Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO (Einwilligung) vorliegt, wir zur Erteilung einer Bankauskunft befugt sind und/oder von uns beauftragte Auftragsverarbeiter gleichgerichtet die Vorgaben der DSGVO garantieren. Unter diesen Voraussetzungen können Empfänger personenbezogener Daten z.B. sein:

- Öffentliche Stellen und Institutionen (z.B. Deutsche Bundesbank, Bundesanstalt für Finanzdienstleistungsaufsicht, Europäische Bankenaufsichtsbehörde, Europäische Zentralbank, Finanzbehörden, Bundeszentralamt für Steuern, Strafverfolgungsbehörden, Familiengerichte, Grundbuchämter) bei Vorliegen einer gesetzlichen oder behördlichen Verpflichtung
- Andere Kredit- und Finanzdienstleistungsinstitute oder vergleichbare Einrichtungen sowie Auftragsverarbeiter, an die wir zur Durchführung der Geschäftsbeziehung mit Ihnen personenbezogene Daten übermitteln (z.B. Korrespondenzbanken, Depotbanken, Börsen,)
- Unternehmen in den Kategorien IT-Dienstleistungen, Logistik, Druckdienstleistungen und Telekommunikation

Zur Wahrung des betrieblichen Interesses können zum Zweck der Konzernsteuerung und der Betriebssicherheit ihre personenbezogenen Daten auch an die Konzerngesellschaften der FBG-Gruppe sowie an die Konzernmutter weitergegeben werden (z.B. zum Zweck des IT-Betriebs und IT-Sicherheit, Gebäudesicherheit, Geschäfts- und Risikosteuerung). Diese sind:

- Frankfurter Bankgesellschaft Holding AG
- Family Office der Frankfurter Bankgesellschaft AG
- Frankfurter Bankgesellschaft (Schweiz) AG
- IMAP M&A Consulting AG
- Landesbank Hessen-Thüringen (Helaba/Konzernmutter)

5. Wie lange werden meine Daten gespeichert?

Soweit erforderlich, verarbeiten und speichern wir Ihre personenbezogenen Daten für die Dauer unserer Geschäftsbeziehung, was beispielsweise auch die Anbahnung und die Abwicklung eines Vertrages umfasst. Dabei ist zu beachten, dass unsere Geschäftsbeziehung ein Dauerschuldverhältnis ist, welches auf Jahre angelegt ist. Darüber hinaus unterliegen wir verschiedenen Aufbewahrungs- und Dokumentationspflichten, die sich unter anderem aus dem Handelsgesetzbuch

(HGB), der Abgabenordnung (AO), dem Kreditwesengesetz (KWG), dem Geldwäschegesetz (GwG) und dem Wertpapierhandelsgesetz (WpHG) ergeben. Die dort vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen zwei bis zehn Jahre.

Schließlich beurteilt sich die Speicherdauer auch nach den gesetzlichen Verjährungsfristen, die zum Beispiel nach den §§ 195 ff. des Bürgerlichen Gesetzbuches (BGB) in der Regel 3 Jahre, in gewissen Fällen aber auch bis zu dreißig 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 5 Jahren, bei aufsichtsbehördlicher Anordnung im Einzelfall auch für bis zu sieben Jahre.

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

Eine Datenübermittlung von personenbezogenen Daten an Drittstaaten (Staaten außerhalb der EU/EWR) findet nur statt, soweit dies zur Ausführung Ihrer Aufträge (z.B. Zahlungs- und Wertpapieraufträge) erforderlich, gesetzlich vorgeschrieben ist (z.B. steuerrechtliche Meldepflichten), Sie uns Ihre Einwilligung erteilt haben oder im Rahmen einer Auftragsdatenverarbeitung. Mit den Auftragsverarbeitern schließen wir einen entsprechenden Vertrag auf Grundlage von Art. 44ff DSGVO ab.

7. Welche Datenschutzrechte habe ich?

Sie haben das **Recht auf Auskunft** nach Artikel 15 DSGVO, das **Recht auf Berichtigung** nach Artikel 16 DSGVO, das **Recht auf Löschung** nach Artikel 17 DSGVO, das **Recht auf Einschränkung** der Verarbeitung nach Artikel 18 DSGVO, das **Recht auf Widerspruch** aus Artikel 21 DSGVO sowie das **Recht auf Datenübertragbarkeit** aus Artikel 20 DSGVO. Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein **Beschwerderecht** bei einer zuständigen Datenschutzaufsichtsbehörde (Artikel 77 DSGVO i. V.m. § 19 BDSG).

Die für die Frankfurter Bankgesellschaft (Deutschland) AG zuständige Aufsichtsbehörde ist:

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
Gustav-Stresemann-Ring 1
65189 Wiesbaden
Referat Kreditinstitute
Telefon: +49-0611-1408-0
Fax: +49-0611-1408-900-901
E-Mail: poststelle@datenschutz.hessen.de

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

8. Besteht für mich eine Pflicht zur Bereitstellung von Daten?

Sollten Sie der Bank im Rahmen der Geschäftsbeziehung personenbezogene Daten von Drittpersonen zur Verfügung stellen, so haben Sie die Drittperson vorgängig über deren Rechte aus dem Datenschutz aufzuklären. Im Rahmen unserer Geschäftsbeziehung müssen Sie nur diejenigen personenbezogenen Daten bereitstellen, die für die Aufnahme und Durchführung einer Geschäftsbeziehung und der Erfüllung der damit verbundenen vertraglichen Pflichten erforderlich sind oder zu deren Erhebung wir gesetzlich verpflichtet sind. Ohne diese Daten werden wir 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 sind wir nach den geldwäscherechtlichen Vorschriften verpflichtet, Sie vor der Begründung der Geschäftsbeziehung beispielsweise anhand Ihres amtlichen Lichtbildausweises zu identifizieren und dabei eine Kopie des amtlichen Lichtbildausweises inkl. Ihres Namens, Ihres Geburtsortes, Ihres Geburtsdatums, Ihrer Staatsangehörigkeiten sowie Ihrer Wohn- und Versandanschriften zu erheben und festzuhalten. Damit wir dieser gesetzlichen Verpflichtung nachkommen können, haben Sie uns aufgrund der vorgenannten Grundlagen die notwendigen Informationen und Unterlagen zur Verfügung zu stellen und sich im Laufe der Geschäftsbeziehung ergebende Änderungen unverzüglich anzuzeigen. Sollten Sie uns die notwendigen Informationen und Unterlagen nicht zur Verfügung stellen, dürfen wir die von Ihnen gewünschte Geschäftsbeziehung nicht aufnehmen oder fortsetzen.

Die Bereitstellung der Legitimationsdaten kann auch online, durch Nutzung des Diensts S-Videolegitimation, erfolgen. Die S-Videolegitimation wird dabei im Auftrag der Bank durch die S-Markt & Mehrwert GmbH & Co.KG, (Auftragsverarbeiter) durchgeführt. Für die technische Umsetzung kooperiert die S-Markt & Mehrwert mit dem IT-Systembetreiber IDnow GmbH, Auenstr. 100, 80469 München. Die Datenerhebung und -speicherung erfolgt dabei ausschließlich in Deutschland und erfolgt ausschließlich zum Zweck Ihrer Identifizierung, auf Grund der gesetzlichen Verpflichtung zur Legitimationsprüfung sowie zur weiteren Vertragserfüllung. Für die Online-Legitimationsprüfung benötigen wir zusätzlich auch Ihre Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO da wir weitere persönliche Daten durch Aufzeichnung (z.B. Video, Ton und Bild) erheben. Sofern Sie dieser Erhebung nicht zustimmen möchten, können wir natürlich die Legitimationsprüfung auch persönlich durchführen. 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-Mailadresse, Mobilfunknummer, Geburtsdatum und -ort. Des Weiteren werden

Legitimationsdaten des Betroffenen wie z.B. Bilder des Ausweisedokuments und der Sicherheitsmerkmale, Bild der Person, Ausweisnummer, Ausstellungsbehörde und -datum, Audio- und Videomitschnitte, TAN-Nummer sowie die

Kommunikationsdaten des Videolegitimationsvorgangs (IP-Adresse, Dauer und Datum der Verbindung) erhoben und verarbeitet. Die erhobenen Identifizierungs- und

Legitimationsdaten werden bis zu 10 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 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 erhobene Daten gelöscht.

9. Inwieweit gibt es eine automatisierte Entscheidungsfindung im Einzelfall?

Zur Begründung und Durchführung der Geschäftsbeziehung nutzen wir grundsätzlich keine automatisierte Entscheidungsfindung. Sollten wir diese Verfahren in Einzelfällen einsetzen, werden wir Sie hierüber gesondert informieren, sofern dies gesetzlich vorgegeben ist.

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

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

Aufgrund gesetzlicher und regulatorischer Vorgaben sind wir zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und vermögensgefährdenden Straftaten verpflichtet. Dabei werden auch Datenauswertungen (u. a. im Zahlungsverkehr) vorgenommen. Diese Maßnahmen dienen zugleich auch Ihrem Schutz.

B. Internetnutzung im Speziellen

11. Wie gehen wir mit Ihren Internetdaten um?

Wir nehmen den Schutz Ihrer personenbezogener Internetdaten sehr ernst und behandeln Ihre personenbezogenen Daten vertraulich und entsprechend der gesetzlichen Vorschriften.

Eine Datenverarbeitung findet nur statt, als dies zur Durchführung der angebotenen Dienste erforderlich ist.

Personenbezogene Daten werden nicht an Dritte weitergeleitet, außer wenn dies zuvor von Ihnen kenntlich gemacht wurde und Sie der Übertragung durch eine eindeutige und bewusste Handlung elektronisch zugestimmt haben.

Mit der Registrierung und dem Besuch auf unseren Internetseiten erklären Sie sich einverstanden, dass die nutzungsbezogenen Daten von uns erfasst, gespeichert und genutzt werden dürfen.

Bedenken Sie dennoch: eine Datenübertragung im Internet kann grundsätzlich mit Sicherheitslücken bedacht sein. Ein vollumfänglicher Schutz vor dem Zugriff durch Fremde ist nicht realisierbar.

Um Ihre übermittelten Daten bestmöglich zu schützen, nutzen wir eine SSL-Verschlüsselung. Sie erkennen derart verschlüsselte Verbindungen an dem Präfix "https://" im Seitenlink in der Adresszeile Ihres Browsers. Unverschlüsselte Seiten sind durch „http://" gekennzeichnet. Sämtliche Daten, welche Sie an diese Website übermitteln – etwa bei Anfragen oder Logins – können dank SSL-Verschlüsselung nicht von Dritten gelesen werden.

11.1 Beschreibung und Umfang der Datenverarbeitung

Bei jedem Aufruf unserer Internetseite erfasst unser System automatisiert Daten und Informationen vom System des aufrufenden Rechners.

Folgende Daten werden hierbei unter anderem erhoben (Beispiele):

- IP-Adresse des von Ihnen genutzten Endgerätes
- Name der abgerufenen Datei
- Datum und Uhrzeit des Abrufs
- übertragene Datenmenge
- Status des Abrufs (erfolgreich / nicht erfolgreich)
- Browsertyp nebst Version sowie das Betriebssystem, das Sie nutzen
- URL der jeweils vorher aufgerufenen Seite (sogenannte „Referrer URL“)

Diese Daten sind für uns keiner bestimmten Person zuordenbar und erlauben uns keine Rückschlüsse auf die Identität des Nutzers. Eine Speicherung zusammen mit anderen personenbezogenen Daten des Nutzers findet nicht statt.

11.2 Rechtsgrundlage für die Datenverarbeitung

Die Verarbeitung der Daten erfolgt zur Wahrung berechtigter Interessen auf Grundlage einer Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO.

11.3 Zweck der Datenverarbeitung

Die vorübergehende Speicherung der IP-Adresse durch das System ist notwendig, um eine Auslieferung der Website an Ihren Rechner zu ermöglichen. Hierfür muss Ihre IP-Adresse für die Dauer der Sitzung gespeichert bleiben. Im Übrigen erfolgt die Speicherung der Daten, um die Funktionsfähigkeit der Website sicherzustellen.

12. Welche Daten können bei der Nutzung unserer Internetseiten anfallen und werden allenfalls von uns oder Dritten gespeichert?

12.1 Cookies und Session IDs

Verschiedentlich werden auf unseren Internetseiten Cookies und Session IDs eingesetzt, um Ihnen gezielt Informationen zur Verfügung zu stellen, um Ihre Sucheinstellungen zu speichern und zu Analysezwecken. Sofern Sie der Nutzung von Cookies im Hinweis-Banner widersprechen, werden solche Cookies, welche wir zu Marketing- und Analysezwecken erheben, nicht verwendet. Technisch zwingend notwendige Cookies, die wir z.B. zur Bereitstellung unserer vertraglich vereinbarten Dienstleistungen benötigen, werden nicht deaktiviert. Durch den Einsatz der Cookies werden weder persönliche Daten gespeichert, noch solche mit Ihren persönlichen Nutzerdaten verbunden. Cookies sind kleine Textdateien, die von unserem Webserver an Ihren PC verschickt und dort meist auf Ihrer Festplatte abgespeichert werden. Sie werden nicht Bestandteil Ihres Systems und können auch keinen Schaden anrichten.

Die meisten Browser sind so eingestellt, dass sie Cookies automatisch akzeptieren. Sie können das Speichern von Cookies jedoch deaktivieren oder Ihren Browser so einstellen, dass er Sie auf die Sendung eines Cookies hinweist.

12.2 Matomo

Auf unserer Internetseite werden mit Matomo, einem Open-Source Web-Analyse-Tool (<https://matomo.org>), auf Basis unseres berechtigten Interesses an der statistischen Analyse zu Optimierungs- und Marketingzwecken gemäß Art. 6 Abs. 1 f DSGVO Daten gesammelt und gespeichert. Aus diesen Daten können unter einem Pseudonym Nutzungsprofile erstellt werden. Hierzu können Cookies eingesetzt werden. Bei Cookies handelt es sich um kleine Textdateien, die lokal im Zwischenspeicher des Internet-Browsers des Seitenbesuchers gespeichert werden. Die Cookies ermöglichen die Wiedererkennung des Internet-Browsers. Unsere Internetseite verwendet Matomo mit der Privacy Einstellung „Anonymisierung der IP-Adresse“. Dadurch werden IP-Adressen gekürzt weiterverarbeitet, ein direkter Personenbezug wird dadurch ausgeschlossen. Die mittels Matomo von Ihrem Browser übermittelte IP-Adresse wird außerdem nicht mit anderen von uns erhobenen Daten zusammengeführt. Sie haben die Möglichkeit, zu verhindern, dass Cookies von Matomo auf Ihrem Computer gespeichert werden, in dem Sie im Cookie Banner bei Aufruf dieser Webseite der Nutzung von Cookies widersprechen, oder die entsprechenden Einstellungen an Ihrem Internetbrowser modifizieren. Dies kann dazu führen, dass Sie nicht den gesamten Umfang unserer Internetseite verwenden können.

12.3 Google Maps

Unsere Webseiten verwenden die Google Maps API, um geographische Informationen visuell darzustellen, z.B. beim Filialfinder. Bei der Nutzung von Google Maps werden von Google (Google Inc., 1600 Amphitheatre Parkway, Mountain View, California, 94043) auch Daten über die Nutzung der Maps-Funktionen durch Besucher der Webseiten erhoben, verarbeitet und genutzt. Nähere Informationen über die Datenverarbeitung durch Google können Sie den Datenschutzhinweisen von Google entnehmen, die Sie unter <http://www.google.com/privacypolicy.html> abrufen können. Durch die Nutzung von Google Maps API werden Informationen über die Nutzung der Webseite der einschließlich Ihrer anonymisierten und gekürzten IP-Adresse an einen Server von Google in den USA übertragen und dort gespeichert. Wir weisen an dieser Stelle explizit auf die unterschiedlichen Datenschutzniveaus in Europa und den USA hin. Wünschen Sie die Nutzung von Google Maps API nicht, so deaktivieren Sie dazu JavaScript in Ihrem Browser. Wir weisen Sie jedoch darauf hin, dass Sie in diesem Fall die Kartenanzeige z.B. Filialfinder nicht nutzen können. Mit der Nutzung der Dienste stimme ich der Datenübermittlung zu Google zu.

12.4 Versand Newsletter

Sofern Sie sich für den Bezug eines Newsletters der Frankfurter Bankgesellschaft (Deutschland) AG entscheiden, benötigen wir zum Zweck des Versands des Newsletters eine E-Mail-Adresse, die wir aufgrund Ihrer Einwilligung gemäß Art. 6 Abs. 1 a DSGVO speichern. Sofern Ihr Email-Provider die Transport Layer Security (TLS) unterstützt, erfolgt der Versand verschlüsselt. Sie haben jederzeit das Recht

Ihre Einwilligung zum Bezug des Newsletters zu widerrufen, Ihre Daten werden dann gelöscht und der Versand eingestellt.

12.5 Anmeldung VVS Portal

Bei Nutzung des VVS Portals der Frankfurter Bankgesellschaft (Deutschland) AG werden Ihre Daten (Name, Email, Telefon, Adresse, Zugangsdaten) zum Zweck der Erfüllung von vertraglichen Pflichten erhoben und durch uns gespeichert. Die Verarbeitung Ihrer Daten erfolgt auf Grund der vertraglich vereinbarten Leistungen gemäß Art. 6 Abs. 1 b DSGVO. Bei Beendigung der Vertragsbeziehung werden Ihre Daten umgehend gelöscht.

12.6 Kontaktformular

Durch die Nutzung des Kontaktformulars werden lediglich die zum Zweck der Kontaktaufnahme notwendigen Daten durch uns erhoben. Ihre persönlichen Kontaktdaten (Name und E-Mail-Adresse) speichern wir aufgrund unseres berechtigten Interesses nach Art. 6 Abs. 1 f DSGVO zur Erfüllung unserer angebotenen Dienstleistung und Ihrer Kontaktanfrage.

Bei der Kontaktaufnahme nutzt die Frankfurter Bankgesellschaft (Deutschland) AG aus Sicherheitsgründen den Dienst Friendly Captcha des Auftragsverarbeiters „Friendly Captcha GmbH“, Am Anger 3-5, 82237 Wörthsee. Der Auftragsverarbeiter bietet eine Schutzlösung, um die Nutzung unserer Webseite durch automatische Programme und Skrypte (sog. „Bots“) zu erschweren.

12.7 Online-Meetings, Video- und Telefonkonferenzen

Wir verwenden die Anwendung Webex der Firma Cisco Systems Inc., USA, um Telefonkonferenzen, Online-Meetings, Videokonferenzen oder Webinare durchzuführen (nachfolgend: „Online-Meetings“).

Wir bieten Online-Meetings zum Zweck von Informationsgesprächen für unsere Kunden und Kundinnen und Geschäftspartner an, um flexibel und trotzdem persönlich erreichbar zu sein. Dies erfolgt aufgrund unserer vertraglichen Beziehung nach Art. 6 Abs. 1 lit. b) DSGVO. Soweit personenbezogene Daten von uns verarbeitet werden, ist § 26 BDSG die Rechtsgrundlage der Datenverarbeitung.

Wertpapieraufträge nehmen wir mittels eines Online-Meetings nicht entgegen. Hierzu nutzen Sie bitte den persönlichen Kontakt zu Ihrem Kundenberater. Online-Meetings werden grundsätzlich nicht aufgezeichnet. Sofern dies trotzdem erfolgen soll, werden

wir Ihnen das im Vorfeld transparent mitteilen und – soweit erforderlich – um eine Einwilligung bitten.

Bei der Nutzung der Anwendung für Online-Meetings werden insbesondere Anmeldedaten verarbeitet. Um an einem Online-Meeting teilzunehmen müssen Sie mindestens Angaben zu Ihrem Namen oder Ihrer E-Mailadresse machen. Bei der Teilnahme an einem Online-Meeting werden die Metadaten der Verbindung, nicht aber die Kommunikationsinhalte, gespeichert. Folgende personenbezogene Daten können Gegenstand der Verarbeitung sein:

Vorname, Nachname, Telefon (optional), E-Mail-Adresse, Passwort (optional) sowie die Verbindungsdaten wie z.B. IP-Adressen oder Geräte-/Hardware-Informationen.

Bei einer optionalen Aufzeichnung des Online-Meetings wird auch die MP4-Datei mit den Video- und Audioinhalten gespeichert. Bei einer Einwahl per Telefon werden die Angabe zur eingehenden und ausgehenden Rufnummer, Dauer sowie zugehörige Ländercodes verarbeitet. Bei Audio- und Videonutzung können Sie optional die Kamera oder das Mikrophon selbständig über die Applikation abschalten bzw. stumm stellen.

Die im Zusammenhang mit Ihrer Teilnahme an Online-Meetings erhobenen personenbezogenen Daten werden grundsätzlich nicht an Dritte weitergegeben. Notwendigerweise verarbeitet der Anbieter für Online-Meetings Ihre Daten, um die Anwendung Webex zur Nutzung bereitstellen zu können. Ihre Daten können dabei auch außerhalb der EU verarbeitet werden.

Cisco verpflichtet sich zum Schutz Ihrer Daten durch die Einhaltung von Datenschutzstandards und bestätigt durch den Abschluss von Binding Corporation Rules (BCR) und EU-Standardvertragsklauseln, die Einhaltung der europäischen Datenschutzstandards.

Weiterführende Informationen zum Datenschutz werden Ihnen durch Cisco unter dem Link https://www.cisco.com/c/de_de/about/legal/privacy-full.html und der E-Mailadresse privacy@cisco.com erteilt.

12.8 Nutzung des elektronischen Kundenportals

Sofern Sie sich für die Nutzung unseres elektronischen Kundenportals mit dem elektronischen Postfach entscheiden, verarbeitet die Frankfurter Bankgesellschaft (Deutschland) AG nachfolgende personenbezogene Daten zur Registrierung, Anmeldung und Nutzung des Kundenportals: Login-User, Passwort, E-Mail-Adresse sowie Name und Vorname. Wir verarbeiten Ihre personenbezogenen Daten dabei nur zum Zweck der elektronischen Bereitstellung von Vertrags-, Vermögens-, Kundeninformations- und Geschäftsunterlagen. Die Datenverarbeitung erfolgt zur Erfüllung gesetzlicher Vorgaben auf Basis des mit Ihnen bestehenden Vertrags gem. Art. 6 Abs. 1 lit. b DSGVO.

Für den Zugang zum Kundenportal verwenden wir ein Zwei-Faktor-Legitimierungsverfahren. Jedem Nutzenden des elektronischen Postfachs wird dazu im Rahmen der Registrierung ein Profil eingerichtet (Login-User, Passwort), mit dem der Nutzende sich am Kundenportal anmelden kann. Der zweite Authentifizierungsfaktor wird über die FBG Access App der Schweizer Firma Futuræ Technologies AG erzeugt. Futuræ Technologies AG, Eichstr. 23, 8045 Zürich, erfasst und verarbeitet die Daten in Übereinstimmung mit Art. 6 Abs. 1 lit. b DSGVO im Auftrag der Frankfurter Bankgesellschaft (Deutschland) AG. Hierbei handelt es sich um installationsspezifische Kennungen, IP Adressen, Zugriffszeiten und Geräteinformationen (wie Betriebssystem, Smartphone-Modell, u.a.). Bei Verwendung des «signal-based zero-touch» Verfahrens wertet die App zudem lokal auf dem Gerät anonymisierte Sensor Daten, wie zum Beispiel WLAN und Bluetooth Scans aus. Diese App generiert einen sechsstelligen PIN Code, der im Rahmen der Anmeldung für eine erfolgreiche Authentifizierung durch den Nutzenden am

Kundenportal zusätzlich eingetragen werden muss. Zur Zustellung des PIN Codes muss die App auf einem Endgerät des Nutzens 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 und nach Verwendung gelöscht wird.

Die Frankfurter Bankgesellschaft (Deutschland) AG 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 hat lediglich der Nutzende selbst sowie die entsprechend autorisierten Mitarbeitenden der Frankfurter Bankgesellschaft (Deutschland) AG.

Sofern Sie das Kundenportal nicht mehr nutzen möchten, werden die Nutzerdaten zum Kundenportal umgehend gelöscht und die bereitgestellten Unterlagen im Rahmen der Aufbewahrungsfristen gespeichert.

C. Datenschutzhinweise für Bewerbende und Mitarbeitende

1. Welche Quellen und Daten nutzen wir?

Wir verarbeiten personenbezogene Daten (Art. 4 Nr. 2 DSGVO), die wir von Ihnen im Rahmen des Auswahl- und Einstellungsverfahrens oder während des Beschäftigungsverhältnisses erhalten. Zudem verarbeiten wir – soweit für das Beschäftigungsverhältnis erforderlich – personenbezogene Daten, die wir auf gesetzlicher Grundlage bei anderen Stellen erheben (z. B. anlassbezogene Abfragen von steuerrelevanten Daten beim zuständigen Finanzamt, Informationen über Arbeitsunfähigkeitszeiten bei der Krankenkasse). Zum anderen verarbeiten wir personenbezogene Daten nur, soweit wir diese zulässigerweise

- von Dritten (z. B. Personalvermittlern) erhalten oder
- aus öffentlich zugänglichen Quellen (z. B. beruflichen sozialen Netzwerken oder Suchmaschinen) gewonnen haben

Relevante personenbezogene Daten sind vor allem Ihre Stammdaten (z.B. Name, Personalnummer, Adresse und andere Kontaktdaten), die bei der Nutzung der IT-Systeme anfallenden Protokolldaten sowie weitere Daten aus dem Beschäftigungsverhältnis (z. B. Beschäftigungsverlauf, Zeiterfassungsdaten, Urlaubszeiten, Arbeitsunfähigkeitszeiten, Beurteilungen, Aus- und Fortbildungen, Sozialdaten, Bankverbindung, Sozialversicherungsnummer, Krankenversicherung/ Krankenversicherungsnummer Gehaltsdaten sowie die Steueridentifikationsnummer, Nachweise und Unterlagen, die Teil der Personalakte werden) sowie andere mit den genannten Kategorien vergleichbare Daten. Hierunter können auch besondere Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DSGVO (z.B. Gesundheitsdaten) fallen. Darüber hinaus werden personenbezogene Daten (z.B. Namen und andere Kontaktdaten, ggf. Depotnummern) von Ehe- bzw. Lebenspartnern, Lebensgefährten und Kindern erhoben, um den gesetzlichen Verpflichtungen aus den Sozialversicherungen, den betrieblichen Regelungen, insbesondere den Dienstvereinbarungen zur Altersversorgung und den Vorgaben

des Art. 2 Abs. 1 und Art. 29 Delegierte Verordnung (EU) 2017/565 gerecht werden zu können.

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

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

2.1 Zur Erfüllung von vertraglichen Pflichten (Anbahnung, Begründung, Durchführung, Änderung oder Beendigung des Beschäftigungsverhältnisses - Art. 6 Abs. 1 Buchst. b DSGVO i.v. m. § 26 Abs. 1 BDSG; Art. 88 Abs. 1 DSGVO i. V. m. § 26 Abs. 4 BDSG)

Die Verarbeitung personenbezogener Daten erfolgt in erster Linie im Beschäftigungskontext, d. h. insbesondere für Zwecke der Anbahnung, Änderung, Durchführung und Beendigung des Vertragsverhältnisses, einschließlich der Erfüllung von durch individuellen (Arbeitsvertrag) oder kollektiven Rechtsvorschriften (Dienst- bzw. Betriebsvereinbarungen und Tarifvertrag) festgelegten Pflichten sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen.

Beispiele:

- zur Erfassung von An- und Abwesenheitszeiten (z. B. Fortbildungen, Urlaub, Arbeitsunfähigkeit)
- zur Entgeltabrechnung sowie zur Reisekostenerstattung
- zur Personalverwaltung (z.B. innerbetriebliche Organisation und Aufgabenverteilung, Dienstwagenabwicklung, Versicherungen, betriebliche Altersversorgung)
- zur Personalaktenführung
- zum Austrittsmanagement (z.B. Zeugniserstellung)

2.2 Im Rahmen der Interessenabwägung (Art. 6 Abs. 1 Buchst. f DSGVO)

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

Beispiele:

- für die Durchführung und Dokumentation rechtlich oder betrieblich notwendiger rechtlicher, technischer oder wirtschaftlicher Prüfungen (z.B. Wirtschaftsprüfer, Innenrevision, Zuverlässigkeitsprüfung nach dem GwG, internes Kontrollsystem)
- zur Sicherstellung ordnungsgemäßer Datenverarbeitung gemäß IT-sicherheitstechnischer und datenschutzrechtlicher Anforderungen (z.B. Protokolldateien)
- Kundenberatung, Kundenbetreuung, Vertrieb und zur Durchführung von Veranstaltungen

- Verhinderung und Aufklärung von Straftaten oder schwerwiegenden Pflichtverletzungen
- Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten
- Maßnahmen zur Gebäude- und Anlagensicherheit (z.B. Zutrittskontrollen)
- zur Datenschutzkontrolle / für den Datenschutz- und Datensicherheitszwecke
- zur Personalplanung und Personalcontrolling
- zum Personalberichtswesen
- Telefonnummern/E-Mail-Adressen zur Aktivierung/Durchführung des Citrix-Zugangs
- Gewährleistung der IT-Sicherheit und Aufrechterhaltung und Weiterentwicklung des IT-Betriebs
- Interne Kommunikation und sonstige Verwaltungszwecke

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

Soweit Sie uns eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke erteilt haben, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis Ihrer Einwilligung gegeben.

Beispiele für bestimmte Zwecke:

- Durchführung eines betrieblichen Eingliederungsmanagements
- Durchführung von Mitarbeiterbefragungen auf freiwilliger Basis
- Verarbeitung und Veröffentlichung von Fotos auf der Website, den Social-Media-Kanälen (LinkedIn/Xing), in Präsentationen und Newslettern sowie in Printmedien (insbesondere im Kundenmagazin CREDUM und in Einladungsunterlagen) der Frankfurter Bankgesellschaft Gruppe sowie im Nachgang zu Veranstaltungen in geschützten Online-Galerien und in gedruckten Handouts für den Kreis der Teilnehmenden an der jeweiligen Veranstaltung

Eine erteilte Einwilligung kann jederzeit widerrufen werden. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der DSGVO, also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

2.4 Aufgrund gesetzlicher Vorgaben (Art. 6 Abs. 1 Buchst. c DSGVO i.V.m. § 26 BDSG)

Zudem unterliegen wir als Arbeitgeber diversen rechtlichen Verpflichtungen, das heißt gesetzlichen Anforderungen (z.B. aus dem Sozialversicherungsrecht, Arbeitssicherheitsgesetz, Arbeitszeitgesetz, Teilzeit- und Befristungsgesetz, Kreditwesengesetz, Geldwäschegesetz, Wertpapierhandelsgesetz, Steuergesetze). Zu den Zwecken gehören u.a. die Identitätsprüfung, die Mitarbeiterzuverlässigkeitsprüfung, die Betrugs- und Geldwäschrävention, die Erfüllung sozialversicherungs- und steuerrechtlicher Kontroll-, Melde- und Dokumentationspflichten und die Steuerung von Risiken in der FBG D und zur

Erfüllung gesetzlicher Auskunftspflichten (z.B. gegenüber öffentlichen Stellen wie Jobcenter, Polizei, Staatsanwaltschaft, Gerichten)

2.5 Verarbeitung besonderer Kategorien personenbezogener Daten zur Erfüllung gesetzlich/kollektivvertraglich vorgesehener Rechte/Pflichten im Bereich des Arbeitsrechts, des Rechts der sozialen Sicherheit oder des Sozialschutzes (Art. 9 Abs. 2 Buchst. b DSGVO, Art. 9 Abs. 2 Buchst. h DSGVO)

Soweit wir besondere Kategorien personenbezogener Daten im Rahmen des Beschäftigungsverhältnisses oder im Rahmen des Bewerbungsprozesses verarbeiten, dient dies der Ausübung von Rechten oder Erfüllung von rechtlichen Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und dem Sozialschutz (z.B. Angabe von Gesundheitsdaten gegenüber der Krankenkasse, Erfassung der Schwerbehinderung wegen Zusatzurlaub und Ermittlung der Schwerbehindertenabgabe) bzw. zur Beurteilung der Arbeitsfähigkeit.

Daneben kann die Verarbeitung besonderer personenbezogener Daten auf einer Einwilligung nach Art. 9 Abs. 2 a DSGVO i.V.m. § 26 Abs.2 BDSG beruhen (z.B. betriebliches Gesundheitsmanagement).

Sofern Sie im Bewerbungsschreiben oder im Laufe des Bewerbungsverfahrens auch besondere Kategorien personenbezogener Daten (wie Gesundheitsdaten, Religionszugehörigkeit, Grad einer Behinderung) freiwillig mitgeteilt haben, findet eine Verarbeitung aufgrund Ihrer Einwilligung statt.

3. Wer erhält meine Daten?

Zur Wahrung des betrieblichen Interesses können zum Zweck der Konzernsteuerung und der Betriebssicherheit ihre personenbezogenen Daten auch an die Konzerngesellschaften der FBG-Gruppe sowie an die Konzernmutter weitergegeben werden (z.B. zum Zweck des IT-Betriebs und IT-Sicherheit, Gebäudesicherheit, Geschäfts- und Risikosteuerung). Diese sind:

- Frankfurter Bankgesellschaft Holding AG
- Family Office der Frankfurter Bankgesellschaft AG
- Frankfurter Bankgesellschaft (Schweiz) AG
- IMAP M&A Consulting AG
- Landesbank Hessen-Thüringen (Helaba)

Im Hinblick auf die Datenweitergabe an weitere Empfänger außerhalb der FBG D ist zunächst zu beachten, dass wir als Arbeitgeber Informationen über unsere Beschäftigten grundsätzlich nur weitergeben, wenn gesetzliche Bestimmungen dies gebieten, der Beschäftigte eingewilligt hat, wir zur Weitergabe anderweitig befugt sind und/oder von uns beauftragte Auftragsverarbeiter gleichgerichtet die Vorgaben der DSGVO garantieren.

Unter diesen Voraussetzungen können weitere Empfänger personenbezogener Daten außerhalb der FBG D z. B. sein:

- Öffentliche Stellen und Institutionen (z. B. Europäische Zentralbank, Europäische Bankenaufsicht, Deutsche Bundesbank, Bundesanstalt für Finanzdienstleistungsaufsicht, Finanzbehörden, Strafverfolgungsbehörden, Familiengerichte) bei Vorliegen einer gesetzlichen oder behördlichen Verpflichtung, Wirtschafts- und Lohnsteuerprüfer
- Bank des Mitarbeitenden (SEPA-Zahlungsträger)
- Annahmestellen der Krankenkassen
- Stellen, um Ansprüche aus der betrieblichen Altersversorgung gewährleisten zu können
- Stellen, um die vermögenswirksamen Leistungen ausbezahlen zu können
- Drittschuldner im Falle von Lohn- und Gehaltspfändungen
- Insolvenzverwalter im Falle einer Privatinsolvenz
- Abrechnung der Beihilfe
- Unternehmen, die bei der Durchführung einer Mitarbeiterbefragung unterstützen
- Auftragsverarbeiter entsprechend dem geschlossenen Vertrag nach Art. 28 DSGVO):
 - Personio GmbH & Co. KG, Rundfunkplatz 4, 80335 München. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Rahmen von Personalverwaltung und Bewerbendenmanagement
 - Netcloud AG, Schlachthofstrasse 19, 8406 Winterthur, Schweiz. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Rahmen von Protokollierung und Monitoring zur Gewährleistung der IT-Sicherheit

4. Wie lange werden meine Daten gespeichert?

Kommt nach einem Bewerbungsverfahren ein Beschäftigungsverhältnis nicht zustande, löschen bzw. vernichten wir Ihre Daten und Unterlagen regelmäßig innerhalb von sechs Monaten nach Beendigung des Bewerbungsverfahrens. Dies gilt nicht, wenn Sie einer längeren Speicherdauer zugestimmt haben oder gesetzliche Regelungen einer Löschung entgegenstehen. Wurden im Rahmen des Bewerbungsverfahrens Kosten für Sie übernommen oder wurden Ihnen Auslagen erstattet, so gelten hierfür die unten genannten Aufbewahrungs- bzw. Nachweispflichten.

Sofern ein Arbeitsverhältnis begründet wird, verarbeiten und speichern wir Ihre personenbezogenen Daten für die oben genannten Zwecke für die Dauer Ihres Arbeitsverhältnisses, was beispielsweise auch die Anbahnung und die Abwicklung des Arbeitsvertrages umfasst. Dabei ist zu beachten, dass das Arbeitsverhältnis ein Dauerschuldverhältnis ist, welches auf Jahre angelegt ist.

Darüber hinaus unterliegen wir verschiedenen Aufbewahrungs- und Nachweispflichten, die sich unter anderem aus dem Handelsgesetzbuch (HGB) und der Abgabenordnung (AO) ergeben. Die Speicherfristen betragen danach bis zu zehn Jahre. Für Wertpapier-Gesprächsaufzeichnungen und Eigenhandelsgespräche beträgt die Frist 5 Jahre, in besonderen Ausnahmefällen bis zu 7 Jahren.

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

Sofern Sie im Rahmen der betrieblichen Altersversorgung eine unverfallbare Anwartschaft erlangt haben, werden Ihre personenbezogenen Daten auch über das Ende Ihres Arbeitsverhältnisses hinaus zu diesem Zweck verarbeitet. .

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

Personenbezogene Daten von Mitarbeitenden werden im Rahmen der Geschäftstätigkeit an die Frankfurter Bankgesellschaft (Schweiz) AG in der Schweiz übermittelt und an Auftragsverarbeiter übermittelt, mit denen ein Vertrag auf Grundlage von Art. 44ff DSGVO geschlossen wurde.

6. Welche Datenschutzrechte habe ich?

Sie haben das **Recht auf Auskunft** nach Artikel 15 DSGVO, das **Recht auf Berichtigung** nach Artikel 16 DSGVO, das **Recht auf Löschung** nach Artikel 17 DSGVO, das **Recht auf Einschränkung** der Verarbeitung nach Artikel 18 DSGVO, das **Recht auf Datenübertragbarkeit** nach Artikel 20 DSGVO sowie das **Recht auf Widerspruch** nach Artikel 21 DSGVO. Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein **Beschwerderecht** bei einer zuständigen Datenschutzaufsichtsbehörde (Artikel 77 DSGVO i. V.m. § 19 BDSG).

Die für die Frankfurter Bankgesellschaft (Deutschland) AG zuständige Aufsichtsbehörde ist:

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
Gustav-Stresemann-Ring 1
65189 Wiesbaden
Referat Kreditinstitute
Telefon: +49-0611-1408-0
Fax: +49-0611-1408-900-901
E-Mail: poststelle@datenschutz.hessen.de

7. Besteht für mich eine Pflicht zur Bereitstellung von Daten?

Im Rahmen Ihrer Beschäftigung müssen Sie nur diejenigen personenbezogenen Daten bereitstellen, die für die Begründung, Änderung, Durchführung und Beendigung des Beschäftigungsverhältnisses und der Erfüllung der damit verbundenen vertraglichen Pflichten erforderlich sind oder zu deren Erhebung wir gesetzlich verpflichtet sind. Ohne diese Daten werden wir in der Regel nicht in der Lage sein, den Arbeitsvertrag mit Ihnen durchzuführen.

8. Inwieweit gibt es eine automatisierte Entscheidungsfindung (einschließlich Profiling) im Einzelfall?

Zur Begründung, Durchführung und Abwicklung des Beschäftigungsverhältnisses nutzen wir grundsätzlich keine automatisierte Entscheidungsfindung – einschließlich Profiling - gemäß Art. 22 DSGVO. Sollten wir diese Verfahren in Einzelfällen einsetzen, werden wir Sie hierüber und über die Ihnen zustehenden Rechte gesondert informieren, sofern dies gesetzlich vorgegeben ist.

D. Ihre Rechte

1. Einzelfallbezogenes Widerspruchsrecht

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstabe f der 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 DSGVO, das wir zur Bonitätsbewertung oder für Werbezwecke einsetzen. Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

2. Widerspruchsrecht gegen eine Verarbeitung von Daten für Werbezwecke

In Einzelfällen verarbeiten wir Ihre personenbezogenen Daten, um ihnen individuelle Angebot zu unterbreiten. Sie haben das Recht, jederzeit Widerspruch gegen die Verarbeitung Sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es damit in Verbindung steht.

Widersprechen Sie der Verarbeitung für Zwecke der Werbung, so werden wir Ihre personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten.

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

Frankfurter Bankgesellschaft (Deutschland) AG
Datenschutzbeauftragte/r
Junghofstraße 26
60311 Frankfurt am Main
Deutschland