

Informationen zum Datenschutz

Informationen zum Datenschutz

In diesem Dokument finden Sie Informationen zum Schutz Ihrer personenbezogenen Daten. Das sind z. B. Name, Geburtsdatum, Beruf oder Kontonummer. Den Schutz Ihrer Daten regelt die **Datenschutz-Grundverordnung (DSGVO)**.

Zusätzliche Informationen finden Sie im Internet unter <https://sparkasse.at/dsgvo>. Auf dieser Internetseite finden Sie auch Informationen zu gemeinsamen Verantwortlichkeiten. Das bedeutet, dass 2 oder mehr Verantwortliche gemeinsam festlegen, zu welchem Zweck und auf welche Art Daten verarbeitet werden.

1. Wer ist für die Verarbeitung meiner personenbezogenen Daten verantwortlich?

Erste Group Bank AG
Am Belvedere 1, 1100 Wien

Kontakt für Anfragen zum Datenschutz:

- Erste Group Bank AG, 0196 1905/AT Data Privacy Security Management, Am Belvedere 1, 1100 Wien
- E-Mail: DSGVO-Support@erstegroup.com
- Am einfachsten per Nachricht in George. Wenn Sie zwischen Themen auswählen können, klicken Sie auf „Datenschutz Grundverordnung/DSGVO“. Schreiben Sie sonst einfach „Datenschutz“ in den Betreff Ihrer Nachricht oder E-Mail

2. Wer ist der Datenschutzbeauftragte?

Gregor König
Erste Group Bank AG
Am Belvedere 1, 1100 Wien
E-Mail: datenschutz@erstegroup.com

3. Welche personenbezogenen Daten werden verarbeitet und wie werden sie erhoben?

Welche personenbezogenen Daten wir von Ihnen verarbeiten, hängt vom Umfang der Geschäftsbeziehung zwischen Ihnen und uns ab. Hier finden Sie eine Liste mit den möglichen Daten, die wir direkt bei den betroffenen Personen erheben. Es kann auch sein, dass wir Informationen aus den erhobenen Daten ableiten.

Bitte beachten Sie: Das bedeutet nicht zwangsläufig, dass wir diese Daten von Ihnen auch konkret verarbeiten:

Personen-Stammdaten:	Name, Adresse, Geburtsdatum, Nationalität, Familienstand etc.
Kontaktdaten:	E-Mail-Adresse, Telefonnummer etc.
Identifikationsdaten:	Benutzername, IP-Adresse, Bilder, Kundenkurz-Bezeichnung, Kunden-ID, Verfügernummer, Art und Nummer des Ausweises, Browser-Fingerprint, Identifikationsnummer für Internet-Cookies, Sozialversicherungs-Nummer, Personalnummer, Urkunden etc.
Persönliche Informationen:	Arbeitsverhältnis, Sprache, Kundenbetreuung im Kreditinstitut etc.
Personenbeziehungen:	Vertretung, Kundenbeziehung etc.
Marketing und Kundenbeziehungs-Management (CRM):	Financial-Health-Indikatoren, persönliche Interessen, Einladungen zu Veranstaltungen etc.
Verhaltensdaten:	Klick-Verlauf in George bzw. auf unseren Internetseiten, Daten über die Produktnutzung etc.

Konto-/Produktdaten:	Debitkarten, Kreditkarten, IBAN, Polizzen, Konditionen, Wertpapier-Depot, Versicherung etc.
Finanztransaktionen:	Wertpapier-Käufe, Umsätze von Zahlungskonten, Gehaltszahlungen etc.
Risikodaten:	Bonität, Risikoklasse, Risikokalkulationen/Rating, Kredite mit Schuldnerverzug etc.
Compliance und Recht:	Gerichtsverfahren, Meldungen an Behörden, Betrugsfälle, Warnhinweise etc.
Geschäftsdokumente:	Verträge, Abwicklung und Verwaltung von Wertpapier-Geschäften, Pfandurkunden etc.
IT-Daten:	Log-Dateien, Log-in-Daten, Änderungsdaten und -historie etc.
Audio- und Bilddaten:	Sprachaufzeichnungen, Videos, Bilder etc.
Strafrechtliche Verurteilungen und Straftaten:	Strafrechtliche Urteile, Strafanzeigen, Verwaltungs-Strafbescheide etc.

Wir erheben Ihre personenbezogenen Daten an verschiedenen Stellen und bei verschiedenen Anlässen, z. B. wenn Sie:

- Unsere Filialen besuchen oder Selbstbedienungs-Geräte nutzen
- Eines unserer Produkte eröffnen oder nutzen
- Unser Online-Angebot nutzen (insbesondere Webseiten, Internetbanking, Apps)
- Unsere sonstigen Serviceangebote und Kontaktmöglichkeiten nutzen, z. B. 24h Service, Gewinnspiele, Veranstaltungen

4. Für welchen Zweck werden meine personenbezogenen Daten verarbeitet? Welche rechtlichen Grundlagen gibt es?

Wir sind eine Bank nach dem Bankwesengesetz (BWG) und der EU-Kapitaladäquanz-Verordnung – siehe BWG § 1 (1) und EU-Kapitaladäquanz-Verordnung Artikel 4 (1) 1. Außerdem vermitteln wir andere Produkte und Dienstleistungen, z. B. Versicherungen und Bausparverträge. Für diese Tätigkeiten müssen wir Ihre personenbezogenen Daten verarbeiten.

Verarbeitung für die Vertragserfüllung und vorvertragliche Maßnahmen, die auf Ihre Anfrage erfolgen

Es hängt vom Vertrag ab, welche Leistungen wir für Sie erbringen dürfen. Das können z. B. Kreditvertrag, Kontovertrag, Leasingvertrag, Vermittlung einer Versicherung oder eine George Vereinbarung sein.

Wir müssen z. B. Ihre Daten verarbeiten, damit Sie sich beim Internetbanking George einloggen können und damit Sie George nutzen können, z. B. für Überweisungen. Den Umfang der Datenverarbeitung finden Sie in den Vertragsunterlagen und Geschäftsbedingungen.

Für unser Internetbanking George analysieren wir die gespeicherten Daten. Wir bereiten die Daten technisch auf, damit sie besser dargestellt werden können. Davon umfasst sind:

- Persönliche Informationen
- Kontostände, Buchungen und Umsatzdaten
- Die Kategorisierung von Kontoumsätzen
- Die Indizierung dieser Daten für eine schnellere Suche in George

Davon sind auch Daten betroffen, die Sie selbst in das Internetbanking George geladen haben.

Verarbeitung wegen rechtlicher Verpflichtungen

Wir müssen auch aus rechtlichen Verpflichtungen Ihre personenbezogenen Daten verarbeiten, z. B.

- Bankwesengesetz
- EU-Kapitaladäquanz-Verordnung
- Wertpapieraufsichtsgesetz
- Finanzmarkt-Geldwäschegesetz
- EU-Geldtransfer-Verordnung
- EU-Sanktionsverordnungen

Wir verarbeiten Ihre personenbezogenen Daten für folgende Aufgaben:

- Risikomanagement, vor allem für die Beurteilung von Kreditrisiko und Risiko von Verlusten durch interne Vorgänge oder Mitarbeiter:innen (operationelles Risiko)
- Umgang mit Beschwerden, Bearbeitung von Beschwerden und Analyse von Beschwerden
- Überwachung von Insiderhandel, Interessenkonflikten und Marktmanipulation
- Feststellen der Identität, Überwachung von Transaktionen, Verdachtsmeldungen, Einhaltung von Sanktionsvorschriften, Nachweise zur Mittelherkunft, Angaben zu Art und Zweck der Geschäftsbeziehung
- Einhaltung von Sanktionen
- Meldungen an das zentrale Kontenregister und Meldungen von Kapitalabflüssen
- Zahlungs-Dienstleistungen, z. B. zur Erkennung nicht-autorisierter oder betrügerischer Zahlungsvorgänge
- Buchhaltung, Controlling und Vorschriften zu Steuern und Abgaben
- Aufzeichnung von Telefongesprächen und elektronischer Kommunikation bei Wertpapier-Geschäften
- Auskünfte an Staatsanwaltschaft, Gerichte und Finanzstrafbehörden
- Offenlegung über die Identität von Aktionär:innen

Verarbeitung wegen berechtigter Interessen

In manchen Fällen dürfen wir oder Dritte Ihre Daten verarbeiten, weil es ein berechtigtes Interesse gibt. Es gibt folgende Gründe:

- Zur Anzeige von nützlichen Funktionen, Produkten, Features und Dienstleistungen in George
- Um nicht-rechtsverbindliche, behördliche Empfehlungen zu befolgen
- Für Maßnahmen zum Schutz von Mitarbeiter:innen und Kund:innen sowie zum Schutz des Eigentums der Bank
- Wenn wir unsere Rechte ausüben und verteidigen
- Wenn wir Daten mit Auskunfteien austauschen, um Risiken zu bewerten, z. B. Meldungen und Abfragen aus der Warnliste oder beim Kreditschutzverband von 1870
- Zur Verhinderung und Bekämpfung von Betrug, Geldwäsche und Terrorismusfinanzierung, z. B.:
 - Die Banken und Finanzinstitute haben eine Verdachtsdatenbank (VDB). In dieser Datenbank stehen Verdachtsfälle von Betrug, Betrugsversuch und ähnlichen Straftaten. Diese Daten werden verarbeitet. Es geht um Fälle, bei denen Betrug oder Betrugsversuche während einer Geschäftsbeziehung oder bei den Vorbereitungen dazu festgestellt worden sind. Die CRIF GmbH führt diese VDB als Auftragsverarbeiter. Wir können als Bank diese Datenbank nutzen, wenn wir eine neue Geschäftsbeziehung mit einer Person eingehen wollen. So können wir überprüfen, ob es von dieser Person schon Betrugsversuche gegeben hat
 - Erkennen von verdächtigen Verhaltensarten durch Datenmodelle
- Für die Dokumentation von vergangenen Schadensfällen. So können wir besser entscheiden, ob wir neue Kund:innen annehmen oder Kundenbeziehungen erweitern
- Zur Verbesserung der Datenqualität
- Zur Wahrung der IT-Sicherheit und des IT-Betriebs der Bank
- Aufzeichnungen und Niederschriften von Telefongesprächen zu folgenden Zwecken: Dokumentation rechtsgeschäftlich relevanter Erklärungen, Identifizierung von Verbesserungspotenzial zu Produkten und Dienstleistungen, Qualitätsmonitoring der Dienstleistungen sowie Identifizierung von Verbesserungspotenzial der Callcenter-Mitarbeiter:innen. Tonaufnahmen speichern wir nur und geben sie im Bedarfsfall an Dritte weiter, wenn das zu Beweis Zwecken notwendig ist. Auf dieser Internetseite finden Sie detaillierte Informationen zu den Verarbeitungen: <https://www.sparkasse.at/tiny/datenschutz-aufzeichnungen>
- Wenn wir aus verschiedenen Gründen Video-Überwachung einsetzen:
 - Um unser Hausrecht durchzusetzen
 - Um Angriffe zu verhindern
 - Um Beweise bei Straftaten zu sammeln
 - Um Kund:innen, Mitarbeiter: innen und unser Eigentum zu schützen
 - Um Rechtsansprüche durchzusetzen und zu verteidigen
 - Als Nachweis über Verfügungen und Einzahlungen, z. B. an Geldautomaten. Mit einer Verfügungsberechtigung bei einem Konto können Personen z. B. Überweisungen durchführen oder Daueraufträge einrichten. Wir dürfen Video-Überwachungen machen, damit wir feststellen können, welche Person etwas über Ihr Konto gemacht hat.

Wir können die Video-Aufzeichnungen auch für Sicherheitsschulungen von Mitarbeiter:innen verwenden. Wir verwenden die Video-Aufzeichnungen aber nur, wenn wir sie sorgfältig geprüft, bestimmte Situationen ausgewählt und weitere Sicherheitsmaßnahmen beachtet haben

- Wir verarbeiten Daten zur Geschäfts-, Vertriebs- und Konzernsteuerung, z. B.:
 - Um Kund:innen in Gruppen mit ähnlichen Merkmalen einzuteilen (Kundensegmentierung)
 - Für Überlegungen zu neuen Organisationsformen und Untersuchungen von Merkmalen von Kund:innen
 - um Werbung für Produkte zu vermeiden, die Kund:innen schon nutzen
 - Für die allgemeine Ausrichtung der Geschäftsstrategie und des ProduktportfoliosDazu gehört auch die Entwicklung von Datenmodellen für solche Maßnahmen.
- Sammlung von Daten zur Verbesserung von Arbeitsvorgängen und der Qualität unserer Dienstleistungen. Damit können wir sicherstellen, dass unsere Dienstleistungen, Services und Abläufe qualitativ hochwertig sind
- Laufende Berechnung Ihres Finanzierungspotenzials
- Wir dürfen Kund:innen auswählen, um ihre Zufriedenheit mit unseren Angeboten zu überprüfen
- Produktentwicklung, z. B. anhand von Datenmodellen
- Wir erstellen synthetische oder anonymisierte Daten, die ähnlich sind wie echte Daten. In wenigen Fällen kann es auch notwendig sein, dass wir für Tests echte Daten verwenden
- Wenn Sie uns ein Dokument mit einer elektronischen Signatur oder einem elektronischen Siegel schicken, schicken wir es an einen Validierungsdienst weiter. Ein Validierungsdienst ist ein Unternehmen, das überprüft, ob eine Signatur oder ein Siegel echt ist. Dieses Unternehmen kann z. B. der Signaturprüfdienst der Rundfunk und Telekom Regulierungs-GmbH sein
- Wenn wir ein Dokument mit Ihren Daten darin elektronisch unterschreiben, schicken wir es an einen Vertrauensdienste-Anbieter. Wir nutzen z. B. A-Trust
- Wir wollen unsere hohe Qualität in allen Beratungen und Kanälen sicherstellen. Wir wollen damit unseren Gründungsauftrag erfüllen: „Finanzielle Gesundheit für alle“. Dafür haben wir einen Beratungsablauf festgelegt. Der Ablauf richtet sich nach den Daten, die wir bekommen. Es geht dabei umfassend um die finanziellen Bedürfnisse unserer Kund:innen

Wir wollen Beratungen professionell vorbereiten und durchführen. Dafür verwenden wir folgende Daten:

- Stammdaten. Dazu gehören z. B. Name, Geburtsdatum oder Adresse
- Daten zu den Produkten, die Kund:innen benutzen
- Daten zu Transaktionen

Mit diesen Daten können wir feststellen, welche Beratung für Sie sinnvoll ist. Wir leiten Ihre aktuellen Finanzbedürfnisse aus folgenden Daten ab:

- Wie hoch sind die monatlichen Zahlungen, wie sieht z. B. Ihre Haushaltsrechnung aus?
- Wie viel Geld haben Sie gerade zur Verfügung, wie viel haben Sie gespart?
- Wie sieht der Vermögensaufbau aus?
- Gibt es eine Vorsorge?
- Wie sind die Risiken abgesichert?
- Gibt es eine Finanzierung?

Durch die Analyse dieser Daten können wir Sie noch besser beraten. Neben der Beratung zeigen wir Ihnen in George hilfreiche Tipps („Insights“) zu Ihrer finanziellen Gesundheit an.

Wir speichern die Informationen, damit unsere Beratungen langfristig sinnvoll sind. Wir löschen Ihre Daten aber spätestens nach 7 Jahren oder wenn unsere Geschäftsbeziehung endet.

Verarbeitung nach Einwilligung

Wir dürfen Ihre Daten auch verarbeiten, wenn es keinen Vertrag, keine rechtlichen Verpflichtungen und kein berechtigtes Interesse gibt: nämlich dann, wenn Sie uns Ihre Einwilligung geben. Es hängt immer vom Umfang der Einwilligung ab, welche Daten wir verarbeiten und wofür wir sie verwenden. Sie können uns z. B. erlauben, ein Foto von Ihnen zu machen, damit wir feststellen können, wer Sie sind.

Sie können Ihre Einwilligung jederzeit widerrufen. Aber der Widerruf gilt nicht für die Vergangenheit. Das heißt: Die Verarbeitung Ihrer Daten vor dem Widerruf bleibt rechtmäßig.

Verarbeitung für statistische Zwecke

Wir verarbeiten personenbezogene Daten auch für Statistiken. Das ist nach § 7 im Datenschutzgesetz möglich.

5. Verarbeitet die Bank auch Daten, die sie nicht von mir hat?

Die meisten personenbezogenen Daten, die wir verarbeiten, haben Sie uns selbst gegeben. Es ist aber möglich, dass wir Ihre Daten aus anderen Quellen bekommen.

Datenquelle	Kategorien der Daten	Zwecke und Rechtsgrundlagen
Öffentlich zugängliche amtliche Register, wie z. B. Firmenbuch, Grundbuch, Insolvenzdatei, Vereinsregister, Zentrales Melderegister, Gewerberegister	– Stammdaten und Kontaktdaten, vor allem Name, Geburtsdatum, Adresse – Persönliche Informationen, wie Funktionen, Tätigkeiten, vor allem Beruf, Organschaften (Informationen, in welchen Unternehmen eine Person eine Funktion hat, z. B. Vorstand oder Geschäftsführung), Beteiligungen, wirtschaftliche Tätigkeiten – Grundeigentum und damit verbundene Belastungen, wie z. B. ein Pfandrecht – Risikodaten, z. B. Daten zur Zahlungsfähigkeit, vor allem Insolvenzen, Konkurse	(A) Sorgfaltspflicht bei bankgeschäftlichen und -betrieblichen Risiken (wie z. B. Kreditrisikomanagement) nach dem Bankwesen-Gesetz und der EU-Kapitaladäquanz-Verordnung (B) Sorgfaltspflichten nach dem Finanzmarkt-Geldwäschegesetz und Sanktionsvorschriften (C) Berechtigtes Interesse an der Verhinderung und Bekämpfung von Betrug und ähnlichen Straftaten. Verhinderung von Geldwäscherei und Terrorismusfinanzierung (D) Berechtigtes Interesse an der Verbesserung der Datenqualität (E) Berechtigtes Interesse, einen geordneten Überblick über die eigene Konzernstruktur zu führen
Schuldnerverzeichnisse und Warnlisten, z. B. Kreditschutzverband von 1870 (KSV 1870), CRIF GmbH, Factiva Limited/Dow Jones	– Stammdaten, vor allem Name, Geburtsdatum und Adresse – Risikodaten, z. B. offene Forderungen, Schulden und Nichteinhaltung von Verträgen	Zusätzlich zu (A), (C) und (D): (F) Eigenes berechtigtes Interesse und berechtigtes Interesse anderer Banken und Finanzinstitute zum eigenen Schutz in ihrer Rolle als Gläubiger:innen (berechtigtes Interesse an möglichst wenig Risiko bei Geschäften)
Andere Institute aus dem Verbund von Erste Group, Erste Bank und Sparkassen	– Stammdaten und Kontaktdaten, vor allem Name, Geburtsdatum und Adresse – Risikodaten, z. B. Daten zur Zahlungsfähigkeit, vor allem offene Rechnungen und Schulden – Daten über Verdachtsfälle von Geldwäsche, strafrechtliche Verurteilungen und Straftaten sowie Daten zu Compliance und Recht	Zusätzlich zu (B) und (C): (G) Risikosteuerung und Konsolidierung im Verbund der Kreditinstitute nach dem Bankwesen-Gesetz und der EU-Kapitaladäquanz-Verordnung (H) Wenn Kund:innen einwilligen, darf die Bank die Daten für das Marketing verwenden
Verlage, die Adressen sammeln, und Unternehmen für Direktmarketing nach § 151 Gewerbeordnung	– Stammdaten und Kontaktdaten, vor allem Name, Geburtsdatum und Adresse – Persönliche Informationen, z. B. Daten, ob eine Person in einem Dateisystem für Kund:innen und Interessent:innen erfasst ist	Zusätzlich zu (D) und (G): (I) Die Bank will Werbung für Produkte vermeiden, die Kund:innen schon haben
Unsere Geschäftspartner bei der Vermittlung von Produkten, z. B. s Versicherung – WIENER STÄDTISCHE Versicherung AG Vienna Insurance Group oder s Bausparkasse	– Stammdaten und Kontaktdaten, vor allem Name, Geburtsdatum und Adresse – Daten zu Konten oder Produkten, die Sie benutzen, und Daten zu Transaktionen	Zusätzlich zu (G) und (H): (J) Erfüllung von Verträgen. Berechtigtes Interesse an Maßnahmen zur Steuerung der Geschäfte und des Vertriebs

Verdachtsdatenbank für Bank- und Finanzinstitute (CRIF GmbH)	– Stammdaten und Kontaktdaten, vor allem Name, Geburtsdatum und Adresse – Daten über Verdachtsfälle von Straftaten, wenn wir diese während einer Geschäftsbeziehung oder bei den Vorbereitungen dazu festgestellt haben. Vor allem Daten über den Hergang des Verdachtsfalls, zu welchem strafrechtlichen Bereich der Verdacht gehört und welche Art von Verdacht besteht	Zusätzlich zu (B) und (C): (K) Berechtigtes Interesse am Schutz vor einem möglichen Betrug oder Betrugsversuch sowie ähnlichen Straftaten. Diese Möglichkeit ist in § 4 Abs. 3 DSG geregelt. Berechtigtes Interesse am Schutz vor einer Rufschädigung der Bank
Vermittler:innen (Intermediäre) nach § 178 Z 1 Börsegesetz, z. B. Kreditinstitute oder Verwahrer:innen, die Wertpapiere verwalten oder Depotkonten führen	– Informationen über die Identität von Personen, die Aktien besitzen (Aktionär:innen), vor allem zur Feststellung, wer die betroffenen Personen sind	(L) Identität von Personen, die Aktien besitzen (Aktionär:innen). Feststellung, wer die betroffenen Personen sind, wenn sie 0,5 % oder mehr an Aktien oder Stimmrechten besitzen
Banken und Finanzinstitute im Auslandszahlungsverkehr, wenn die Erste Group Bank AG die Zahlung abwickelt. Die Erste Group Bank AG ist die Korrespondenzbank. Mehr Informationen finden Sie hier: https://www.erstegroup.com/de/financial-institutions/cash-management-fin-institutions	– IBAN und Kontonummer der Zahler:innen und der Empfänger:innen der Zahlungen – Währung der Konten, Währung der Zahlung, Betrag der Zahlung	Zusätzlich zu (B) und (C): (M) Tätigkeit als Korrespondenzbank bei Geschäften zwischen Banken (N) Berechtigtes Interesse an einer kostengünstigen und problemlosen Abwicklung der Zahlung

Für die hier genannten Datenarten und Datenverarbeitungen gelten auch die übrigen Punkte in diesem Informationsblatt. Ausgenommen ist Punkt 4 „Welche rechtlichen Grundlagen gibt es? Welche personenbezogenen Daten werden verarbeitet und wie werden sie erhoben?“.

6. Muss ich meine personenbezogenen Daten bereitstellen? Was passiert, wenn ich das nicht will?

Wir brauchen viele Ihrer personenbezogenen Daten für unsere Geschäftsbeziehung, z. B. damit wir Ihnen eine neue Debitkarte zuschicken können. Nach dem Gesetz dürfen wir keine Geschäftsbeziehung zu Ihnen haben, wenn wir nicht überprüfen können, wer Sie sind. Wenn wir nicht wissen, wie Ihre Zahlungsfähigkeit ist, können wir Ihnen keinen Kredit geben.

Wenn es wegen einer rechtlichen Vorschrift oder eines Vertrags notwendig ist, müssen wir Ihre Daten verarbeiten. Wenn Sie das nicht wollen, können wir bestimmte Services leider nicht anbieten.

In allen anderen Fällen verarbeiten wir Ihre Daten nur, wenn Sie uns Ihre Einwilligung geben. Diese Einwilligung ist selbstverständlich freiwillig. In diesen Fällen müssen Sie uns Ihre Daten nicht geben.

7. Gibt es Entscheidungen der Bank durch Datenverarbeitung inkl. Profiling ohne Eingriff einer Mitarbeiter:in?

Wenn wir Entscheidungen aufgrund von automatischer Datenverarbeitung treffen, werden wir Sie vorher darüber informieren.

Wenn wir einen Kredit vergeben, prüfen wir Ihre Zahlungsfähigkeit. Dazu verwenden wir das sogenannte Kredit-Scoring. Dabei untersuchen wir das Risiko, dass Sie den Kredit nicht zurückzahlen können. Dazu vergleichen wir Personen, die einen Kredit nehmen wollen, mit anderen Personengruppen.

Bei diesem Verfahren kommt ein bestimmter Wert heraus. Er heißt „Score-Wert“. Dieser Wert ermöglicht uns eine Vorhersage, mit welcher Wahrscheinlichkeit ein Kredit zurückgezahlt wird.

Um den Score-Wert zu berechnen, brauchen wir folgende Daten:

- Stammdaten, z. B. Familienstand, Anzahl der Kinder, Dauer der Beschäftigung oder Arbeitgeber:in
- Allgemeine finanzielle Verhältnisse, z. B. Einkommen, Vermögen, monatliche Ausgaben und Zahlungen, die eine Person leisten muss
- Zahlungsverhalten, z. B. Kreditrückzahlungen, Mahnungen und Daten von Kredit-Auskunfteien

Wenn das Risiko zu groß ist, lehnen wir einen Kredit ab. Es kann einen Eintrag in die Konsumentenkredit-Evidenz (KKE) des Kreditschutzverbands von 1870 (KSV 1870) geben. Außerdem kann es eine interne Warnung geben.

Wenn ein Kreditantrag abgelehnt wird, steht das 6 Monate lang in der KKE des KSV 1870 – wie im Bescheid der Datenschutzbehörde vorgesehen.

8. Wer bekommt meine personenbezogenen Daten?

- Kreditinstitute, Stellen und Personen im Verbund von Sparkassen, Erste Bank und Erste Group. Diese Stellen oder Personen bekommen Ihre personenbezogenen Daten, wenn sie diese für Folgendes brauchen:
 - Vertragliche, gesetzliche oder aufsichtsrechtliche Pflichten
 - Für das Risikomanagement innerhalb der Erste Group sowie für das Management von Kreditrisiken, wenn Kreditinstitute innerhalb der Erste Group idente Kund:innen haben
 - Sonstige berechnete Interessen.
- Auskunfteien, wie z. B. der Kreditschutzverband von 1870
- Öffentliche Stellen und Einrichtungen und Personen im hoheitlichen Auftrag, wenn wir rechtlich dazu verpflichtet sind oder unsere berechtigten Interessen wahren müssen

Das kann z. B. der Fall sein bei:

- Europäische Bankenaufsichtsbehörde
- Europäische Zentralbank
- Finanzmarktaufsicht
- Oesterreichische Nationalbank
- Finanzbehörden usw.
- Auftragsverarbeiter:innen und sonstige Dienstleister:innen, die wir beauftragt haben. Beispiele dafür sind IT, Backoffice, Rechts- und Steuerberatung, Wirtschaftstreuhand- und Inkassounternehmen. Wir dürfen Ihre Daten weitergeben, wenn das für den Auftrag notwendig ist
- Bankprüfer:innen und Jahresabschluss-Prüfer:innen, wenn es für die Prüfung notwendig ist
- Dritte, wenn es für das Einhalten eines Vertrags oder aufgrund von rechtlichen Vorschriften verpflichtend ist. Ein Beispiel dafür ist die Empfänger:in einer Überweisung und ihre Zahlungsdienstleister:in
- Validierungsdienste, die Ihre elektronische Signatur oder Ihr elektronisches Siegel prüfen müssen. So ein Dienst ist z. B. die Rundfunk und Telekom Regulierungs-GmbH
- Vertrauensdiensteanbieter, z. B. A-Trust. Diese schalten wir ein, wenn wir ein Dokument mit Ihren Daten elektronisch unterschreiben

Falls Sie eingewilligt haben, dürfen wir Ihre Daten auch an andere weitergeben.

Hier finden Sie eine Liste mit möglichen Empfänger:innen Ihrer Daten:

<https://sparkasse.at/dsgvo>

9. Übermitteln Sie meine Daten auch in Länder, die nicht in der EU sind?

Es gibt Fälle, in denen wir Ihre personenbezogenen Daten auch in Länder übermitteln können, die nicht in der EU sind:

- Wenn es erforderlich ist, damit wir Rechtsansprüche geltend machen, ausüben oder verteidigen können. Es kann auch eine Rechtspflicht geben. Das ist z. B. die Aufforderung einer Behörde, wenn es ein Rechtshilfeabkommen gibt
- Wir können Ihre Daten übermitteln, wenn das für einen Vertrag oder die Vorbereitungen für einen Vertrag notwendig ist. Das gilt z. B. für eine Überweisung in ein Land, das nicht in der EU ist
- Unsere Auftrags- und Sub-Auftragsverarbeiter:innen können in Drittländern ansässig sein. Wenn die Übermittlung nicht auf Grundlage eines Beschlusses der Europäischen Kommission zur Angemessenheit erfolgt, übermitteln wir die Daten auf Basis geeigneter oder angemessener Garantien. Auf Anfrage stellen wir Ihnen diese gern zur Verfügung
- Wir informieren Sie extra, wenn wir in anderen Fällen Daten in ein Land übermitteln, das nicht in der EU ist
- Hier finden Sie eine Liste mit möglichen Empfänger:innen Ihrer Daten, die in Nicht-EU-Ländern sind:
<https://sparkasse.at/dsgvo>

10. Wie lange heben Sie meine personenbezogenen Daten auf?

Wir bewahren Ihre personenbezogenen Daten so lange auf, wie es für einen bestimmten Zweck notwendig ist, z. B.:

- Für die Dauer unserer Geschäftsbeziehung
- Für die Dauer eines Gerichtsverfahrens, das gerade läuft
- Solange wir eine Forderung Ihnen gegenüber haben
- Wenn es ein Gesetz verlangt

Auch wenn Sie nicht mehr Kund:in bei uns sind, kann es notwendig sein, dass wir Ihre Daten aufbewahren.

Für die Aufbewahrung von Daten gibt es gesetzliche Bestimmungen. Die wichtigsten Bestimmungen sind:

- Unternehmens-Gesetzbuch § 212
Notwendige Aufbewahrung der Daten: 7 Jahre
- Bundesabgabenordnung § 132
Notwendige Aufbewahrung der Daten: 7 Jahre oder die Dauer des Abgabenverfahrens
- Wertpapieraufsichtsgesetz 2018 § 33
Notwendige Aufbewahrung der Daten: 5 Jahre (7 Jahre, wenn es die Finanzmarktaufsicht anordnet)
- Finanzmarkt-Geldwäschegesetz § 21
Notwendige Aufbewahrung der Daten: 10 Jahre ab Ende der Geschäftsbeziehung bzw. nach der gelegentlichen Transaktion

In Österreich gelten noch andere Vorschriften zur Aufbewahrung von Daten. Eine Übersicht finden Sie z. B. hier:

<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html>

Die Bank darf Ihre Daten auch aufbewahren, wenn es ein berechtigtes Interesse dafür gibt:

- Wir dürfen Finanzierungsanträge jedenfalls bis zu 18 Monate nach Erstellung aufbewahren. Es ist unser berechtigtes Interesse, dass wir den Kundenkontakt dokumentieren. So können wir Ihren Antrag schnell weiterbearbeiten, wenn Sie wieder zu uns kommen
- Wenn Sie den George Store nutzen und den Kauf nicht abschließen, speichern wir Ihre personenbezogenen Daten 60 Tage lang. In dieser Zeit können Sie den Wiederherstellungs-Link verwenden und den Kauf abschließen
- Wenn Sie den George Store nutzen, speichern wir Daten darüber für 60 Tage, z. B. Log-Daten, technische Protokolldaten, Datum und Zeitstempel. Das machen wir, damit wir mögliche Probleme erkennen können, die während des Kaufs auftreten. Wir nutzen diese Daten auch, damit wir Rechte durchsetzen und verteidigen können. Wir heben diese Daten außerdem auf, damit wir Wartungsarbeiten durchführen können
- SWIFT-Nachrichten werden 30 Jahre lang aufbewahrt. Das soll Betrug verhindern und bekämpfen sowie Geldwäsche und Terrorismusfinanzierung verhindern. SWIFT-Nachrichten sind eine sichere Art der Übermittlung, z. B. von Zahlungen
- Wir heben Daten über verkaufte Forderungen 30 Jahre ab dem Verkauf auf. Das berechtigte Interesse der Bank ist es, Einwendungen über den Verkauf zu vermeiden

- Wir können Ihre personenbezogenen Daten auch aufbewahren, wenn wir vergangene Schadensfälle dokumentieren wollen. Wir können die Daten auch verwenden, wenn wir entscheiden, ob wir eine neue Kundenbeziehung eingehen oder eine Kundenbeziehung erweitern wollen:

7 Jahre Aufbewahrung:

- Bei einem Schadensfall mit einer Schadenshöhe von höchstens 20.000 Euro
- Wenn die Bank aufgrund von besonderen Umständen kein Interesse an einer Geschäftsbeziehung hat

12 Jahre Aufbewahrung:

- Bei einem Schadensfall mit einer Schadenshöhe von mehr als 20.000 Euro
- Wenn während unserer Geschäftsbeziehung Insolvenz über Ihr Vermögen eröffnet wird

30 Jahre Aufbewahrung:

- In besonders schwerwiegenden Ausnahmefällen. Hier gibt es eine eingehende Prüfung im Einzelfall

Die Aufbewahrungsfrist beginnt:

- Wenn der Schadensfall abgeschlossen worden ist und es keine Schuld oder Forderungen mehr gibt
- Wenn ein Insolvenzverfahren beendet oder aufgehoben worden ist

Wir müssen die Daten über vergangene Schadensfälle außerdem für Berechnungen aufheben, z. B. für unser Modell zur Berechnung von Zahlungsausfällen. Aber nur wenige Personen können diese Daten einsehen. Kundenbetreuer:innen haben keinen Zugang mehr zu den Daten. Die Daten haben keinen Einfluss auf bestehende oder zukünftige Geschäftsbeziehungen.

11. Welche Rechte habe ich?

Die DSGVO gibt Ihnen einige Rechte für Ihre personenbezogenen Daten. Sie haben folgende Rechte:

- Sie können Auskunft erhalten (DSGVO, Art. 15)
- Sie können Ihre Daten berichtigen lassen (DSGVO, Art. 16)
- Sie können Ihre Daten löschen lassen (DSGVO, Art. 17)
- Sie können die Verarbeitung Ihrer Daten einschränken lassen (DSGVO, Art. 18)
- Sie können Ihre Daten übertragen lassen (DSGVO, Art. 20)
- Sie können Widerspruch einlegen (DSGVO, Art. 21)
- Sie haben das Recht, dass wir Entscheidungen nicht nur automatisiert treffen (DSGVO, Art. 22)

Genaue Informationen zum Recht auf Übertragung Ihrer Daten finden Sie hier:

<https://sparkasse.at/dsgvo>

Sie können Sie mit uns Kontakt aufnehmen, egal, welches Recht Sie ausüben wollen. Das können Sie auf eine der folgenden 5 Arten:

- Per Nachricht in George
Hier geht es am schnellsten. Wenn Sie zwischen Themen auswählen können, klicken Sie auf „Datenschutz Grundverordnung/ DSGVO“. Schreiben Sie sonst einfach „Datenschutz“ in den Betreff Ihrer Nachricht
- Über unser Formular auf der Internetseite <https://www.sparkasse.at/einmeldung-betroffenenrechte> zur Einmeldung von Betroffenenrechten („Wie und wo kann ich meine Rechte geltend machen?“)
- Per E-Mail, idealerweise mit einer qualifizierten elektronischen Signatur an DSGVO-Support@erstegroup.com
- Per Brief, bitte eigenhändig unterschrieben und mit Ausweiskopie an

Erste Group Bank AG
0196 1905/AT Data Privacy Security Management
Am Belvedere 1
1100 Wien

- Persönlich in einer Filiale der Bank

Bitte haben Sie Verständnis dafür, dass wir in Zweifelsfällen weitere Angaben zu Ihrer Person verlangen. Das ist auch zu Ihrem Schutz. Wir wollen sicherstellen, dass nur Berechtigte Ihre Daten sehen können.

Sie können auch Beschwerde einlegen, z. B.

- weil Sie nicht rechtzeitig eine Antwort auf einen Antrag erhalten,
- weil Sie der Ansicht sind, dass wir Ihrem Antrag nicht gesetzmäßig nachgekommen sind,
- weil Sie glauben, dass wir Ihr Recht auf Datenschutz verletzen.

Hier können Sie sich beschweren:

Österreichische Datenschutzbehörde

Barichgasse 40-42
1030 Wien
<https://www.dsb.gv.at>

Stand: Oktober 2025

Impressum:

Medieninhaberin, Herstellerin, Herausgeberin und Redaktion:
Erste Bank der österreichischen Sparkassen AG
Postanschrift: Am Belvedere 1, 1100 Wien