Erste Group Bank AG
Am Belvedere 1
1100 Wien
www.erstegroup.com

Informationen zum Datenschutz

Dieses Dokument enthält Informationen zum Schutz Ihrer personenbezogenen Daten, die in der **Datenschutz-Grundverordnung** (DSGVO) geregelt sind. Zusätzliche Informationen, auch zu gemeinsamen Verantwortlichkeiten, finden Sie auf der Seite Ihres Instituts unter: https://sparkasse.at/dsgvo

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

Erste Group Bank AG
Am Belvedere 1, 1100 Wien

Kontakt für datenschutzrelevante Anfragen:

Erste Group Bank AG
0196 1905/AT Data Privacy Security Management
Am Belvedere 1, 1100 Wien
DSGVO-Support@erstegroup.com

Am schnellsten erreichen Sie uns über eine s Kontakt-Nachricht in George: Wenn Sie zwischen Themen auswählen können, klicken Sie auf „Datenschutz Grundverordnung / DSGVO“. Sonst schreiben Sie einfach „Datenschutz“ in den Betreff Ihrer Nachricht.

2. Wer ist der Datenschutzbeauftragte?

Gregor König, Erste Group Bank AG, Am Belvedere 1, 1100 Wien, 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 oder aus den erhobenen Daten ableiten. Bitte beachten Sie: Das bedeutet nicht zwangsläufig, dass wir diese Daten von Ihnen auch konkret verarbeiten:

Personenstammdaten:	Name, Adresse, Geburtsdatum, Geschlecht, Nationalität, Familienstand, etc.
Kontaktdaten:	E-Mail-Adresse, Telefonnummer, etc.
Identifikationsdaten:	Benutzername, IP-Adresse, Bilder, Kundenkurzbezeichnung, Kunden-ID, Verfügernummer, Art und Nummer des Ausweises, Browser-Fingerprint, Identifikationsnummer für Internet-Cookies, Sozialversicherungsnummer, Personalnummer, Urkunden, etc.

Persönliche Informationen:	Arbeitsverhältnis, Ausbildung, Werdegang, Sprache, Kundenbetreuung im Kreditinstitut, etc.
Personenbeziehungen:	Vertretung, Kundenbeziehung, etc.
Marketing & 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 Zahlungsverkehrskonten, Gehaltszahlungen, etc.
Risikodaten:	Bonität, Risikoklasse, Risikokalkulationen/Rating, Kredite mit Schuldnerverzug, etc.
Compliance & Recht:	Gerichtsverfahren, Meldungen an Behörden, Betrugsfälle, Warnhinweise, etc.
Geschäftsdokumente:	Verträge, Dienstverträge, Abwicklung und Verwaltung von Wertpapiergeschäften, 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, 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 welche Zwecke und auf welcher Rechtsgrundlage werden meine personenbezogenen Daten verarbeitet?

Wir sind eine Bank nach § 1 (1) Bankwesengesetz und Artikel 4 (1) 1 EU-Kapitaladäquanz-Verordnung. Zusätzlich sind wir auch als Vermittlerin für andere Produkte und Dienstleistungen tätig, z. B. Versicherungen und Bausparverträge. Im Rahmen dieser Tätigkeiten verarbeiten wir Ihre personenbezogenen Daten:

Verarbeitung für die Vertragserfüllung und für vorvertragliche Maßnahmen, die auf Ihre Anfrage erfolgen
Es hängt vom Vertrag ab, welche Leistungen wir für Sie erbringen dürfen, z. B. Kreditvertrag, Kontovertrag, Leasingvertrag, Vermittlung einer Versicherung oder eine George-Vereinbarung. Den Umfang der Datenverarbeitung finden Sie in den Vertragsunterlagen und Geschäftsbedingungen.

Für unser Internetbanking George analysieren wir die hinterlegten Daten und bereiten sie für eine bessere Darstellung technisch auf. Diese Aufbereitung beinhaltet neben persönlichen Informationen, Kontoständen, Buchungen und Umsatzdaten auch die Kategorisierung von Kontoumsätzen und 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 aufgrund rechtlicher Verpflichtungen
Auch rechtliche Vorschriften erfordern, dass wir Ihre personenbezogenen Daten verarbeiten, z. B. Bankwesengesetz, EU-Kapitaladäquanz-Verordnung, Wertpapieraufsichtsgesetz, Finanzmarkt-Geldwäschegesetz und EU-Geldtransfer-Verordnung. Das betrifft:
- Risikomanagement, insbesondere Kreditrisiko und operationelles Risiko
- Beschwerdemanagement und Beschwerdebearbeitung, Analyse von Beschwerdefällen

- Monitoring von Insiderhandel, Interessenkonflikten und Marktmanipulation
- Identitätsfeststellung, Transaktionsüberwachung, Verdachtsmeldungen, Einhaltung von Sanktionsvorschriften
- Meldungen in das Kontoregister und Meldungen von Kapitalabflüssen
- Zahlungsdienstleistungen, z. B. zur Erkennung nicht autorisierter oder betrügerischer Zahlungsvorgänge
- Buchhaltung, Controlling und Erfüllung abgabenrechtlicher Vorschriften
- Aufzeichnen von Telefongesprächen und elektronischer Kommunikation bei Wertpapiergeschäften
- Auskünfte an Staatsanwaltschaft, Gerichte, Finanzstrafbehörden
- Offenlegung von Informationen über die Identität von Aktionär:innen

Verarbeitung aufgrund berechtigter Interessen
Ein berechtigtes Interesse zur Datenverarbeitung durch uns oder Dritte besteht in folgenden Fällen:

- Bewerbung neuer Produkte, Features und Dienstleistungen
- Um nicht-rechtsverbindliche, behördliche Empfehlungen zu befolgen
- Maßnahmen zum Schutz von Mitarbeiter:innen, Kund:innen sowie des Eigentums der Bank
- Ausüben oder Verteidigen von Rechten
- Datenaustausch für Bonitäts- und Ausfallsrisiken gegenüber Auskunfteien, z. B. Meldungen und Abfragen aus der Warnliste oder der Konsumentenkreditevidenz des Kreditschutzverband von 1870
- Betrugsprävention und -bekämpfung sowie Verhinderung von Geldwäscherei und Terrorismusfinanzierung, im Speziellen z. B.:
  - In der Verdachtsdatenbank (VDB) für Bank- und Finanzinstitute werden Verdachtsfälle von Betrug und Betrugsversuch nach §§ 146 ff StGB sowie ähnliche Straftaten erfasst und verarbeitet, die während der Geschäftsbeziehung oder bei ihrer Anbahnung festgestellt werden. Geführt wird diese Datenbank von der CRIF GmbH als Auftragsverarbeiter. Wenn Bank- und Finanzinstitute diese Datenbanklösung nutzen, können sie auch Daten empfangen, mit denen sie zu Beginn einer Geschäftsbeziehung mit Kund:innen überprüfen können, ob in der Vergangenheit Betrugsversuche unternommen wurden.
  - Entwicklung von Datenmodellen zum Erkennen verdächtiger Verhaltensmuster
- Dokumentation vergangener Schadensfälle als Entscheidungshilfe über das Eingehen neuer oder erweiterter Kundenbeziehungen
- Steigerung der Datenqualität
- Gewährleistung der IT-Sicherheit und des IT-Betriebs der Bank
- Aufzeichnungen von Telefongesprächen, z. B. bei Beschwerdefällen, für die Dokumentation rechtsgeschäftlich relevanter Erklärungen (z. B. Kartensperren) oder Schulungszwecke unserer Mitarbeiter:innen
- Videoüberwachungen, um unser Hausrecht durchzusetzen, zur Prävention von Angriffen, um bei Straftaten Beweise zu sammeln, zum Schutz von Kund:innen, Mitarbeiter:innen und Eigentum, zur Durchsetzung und Abwehr von Rechtsansprüchen oder zum Nachweis von Verfügungen und Einzahlungen, z. B. an Geldautomaten. Videoaufzeichnungen von derartigen Vorfällen können im Einzelfall nach sorgfältiger Prüfung auch für Sicherheitsschulungen unserer Mitarbeiter:innen eingesetzt werden.
- Maßnahmen zur Geschäfts-, Vertriebs- und Konzernsteuerung, wie z. B. Kundensegmentierung, Reorganisationen und damit einhergehende Kundenanalysen, Vermeiden von Werbung zu bereits genutzten Produkten, sowie die allgemeine Ausrichtung der Geschäftsstrategie und des Produktportfolios. Dazu zählt auch die Entwicklung von Datenmodellen für solche Maßnahmen.
- Maßnahmen zum Prozess- und Qualitätsmanagement: Wir erheben anlassbezogen Daten über unsere Prozesse und Services. Mit diesen Daten sichern wir die Qualität unserer Dienstleistungen, die Einhaltung unserer Service-Standards und die Effizienz unserer Prozesse.
- Laufende Berechnung Ihres Finanzierungspotenzials
- Auswahl zur Evaluierung der Zufriedenheit mit den angebotenen Serviceleistungen und Produkten
- Produktentwicklung, z. B. anhand von Datenmodellen
- Erstellen von synthetischen oder anonymisierten Daten zu Testzwecken (in eingeschränkten Fällen kann es auch erforderlich sein, Echtdaten zu Testzwecken heranzuziehen)
- Wenn Sie uns eine Datei mit einer elektronischen Signatur oder einem elektronischen Siegel

übermitteln, werden wir dieses Dokument für die Signatur-/Siegelprüfung an einen Validierungsdienst (z. B. Signaturprüfdienst der Rundfunk und Telekom Regulierungs-GmbH) übermitteln.
- Wenn wir ein Dokument elektronisch signieren, das Ihre Daten enthält, werden wir das Dokument an einen Vertrauensdienste-Anbieter (z. B. A-Trust) übermitteln.
- Wir wollen unsere hohen Qualitätsstandards über alle Beratungen hinweg sicherstellen, um unserem Gründungsauftrag gerecht zu werden: „Finanzielle Gesundheit für alle“. Dafür haben wir einen Beratungsablauf festgelegt, der auf Daten basiert und die Finanzbedürfnisse der Kund:innen gesamtheitlich betrachtet.
  Für die professionelle Vorbereitung und Durchführung von Beratungen analysieren wir diese Daten:
  - Stammdaten, z. B: Name, Geburtsdatum, Adresse
  - Daten zu genutzten Produkten, Transaktionen

  Daraus leiten wir einen aktuellen Status der Finanzbedürfnisse ab: monatliche Finanzen (Haushaltsrechnung), Liquidität und Reserve, Vermögensaufbau, Vorsorge, Risiken absichern und Finanzieren. Durch diese Datenanalyse können wir unsere Kund:innen noch treffsicherer in deren Interesse beraten. Damit wir Sie nachhaltig professionell beraten können, speichern wir die von Ihnen bereitgestellten Informationen. Spätestens nach 5 Jahren bzw. bei Auflösung der Geschäftsbeziehung werden die Angaben gelöscht.
- Die Erste Group Bank AG hat ein berechtigtes Interesse daran, einen geordneten Überblick über ihre Konzernstruktur zu führen. Dazu betreibt sie eine Datenbank, in der alle Konzernbeteiligungen abgebildet sind. An personenbezogenen Daten werden Name, Geburtsdatum und geschäftliche Korrespondenzadressen der jeweiligen Mandatsträger (z.B. Mitglieder Geschäftsführung, Vorstand, Aufsichtsrat, etc.) gespeichert. Diese Daten werden nach Ablauf von 20 Jahren nach Beendigung des letzten Mandats oder sonstiger interner Funktionen anonymisiert.

Verarbeitung aufgrund Einwilligung
Gibt es weder einen Vertrag noch rechtliche Verpflichtungen oder ein berechtigtes Interesse, kann die Datenverarbeitung dennoch rechtmäßig sein: nämlich dann, wenn Sie uns Ihre Einwilligung dazu erteilt haben. Umfang und Inhalt dieser Datenverarbeitung ergibt sich immer aus der jeweiligen Einwilligung – etwa wenn Sie uns erlauben, im Rahmen der Identitätsfeststellung ein Foto von Ihnen zu machen. Sie können eine Einwilligung jederzeit für die Zukunft widerrufen. Wenn Sie eine Einwilligung widerrufen, bleiben aber die Verarbeitungen bis zum Zeitpunkt des Widerrufs rechtmäßig. Das bedeutet also, ein Widerruf wirkt nicht für die Vergangenheit.

Verarbeitung für statistische Zwecke
Wir verarbeiten Ihre personenbezogenen Daten auch für statistische Zwecke nach § 7 Datenschutzgesetz.

5. Werden auch Daten verarbeitet, die nicht bei mir erhoben werden?

Die meisten personenbezogenen Daten, die wir über Sie verarbeiten, haben Sie uns selbst bekannt gegeben. Es ist aber möglich, dass wir Ihre Daten auch aus anderen Quellen erheben:

Datenquelle	Kategorien der Daten	Zwecke und Rechtsgrundlagen
Öffentlich zugängliche amtliche Register, wie z. B. Firmenbuch, Grundbuch, Insolvenzdatei, Vereinsregister, Zentrales Melderegister, Gewerberegister.	– Personenstammdaten und Kontaktdaten, insbesondere Name, Geburtsdatum, Adresse – Persönliche Informationen wie Funktionen, Tätigkeiten – insbesondere Beruf, Organschaften, Beteiligungen, wirtschaftliche Tätigkeiten; Grundeigentum und damit verbundene Belastungen) – Risikodaten (Bonitätsdaten, insbesondere Insolvenzen, Konkurse).	**(A)** Sorgfaltspflicht bei bankgeschäftlichen und -betrieblichen Risiken (z. B. Kreditrisikomanagement), Bankwesengesetz und EU-Kapitaladäquanz-Verordnung **(B)** Sorgfaltspflichten gemäß Finanzmarkt-Geldwäschegesetz und Sanktionsvorschriften **(C)** Berechtigtes Interesse an der Betrugsprävention und -bekämpfung (sowie ähnlichen Straftaten), Verhinderung von Geldwäscherei und Terrorismusfinanzierung

		(D) Berechtigtes Interesse an Verarbeitungen zur Steigerung der Datenqualität **(E)** Berechtigtes Interesse, einen geordneten Überblick über die eigene Konzernstruktur zu führen
Schuldnerverzeichnisse und Warnlisten, wie z. B. Kreditschutzverband von 1870 (KSV 1870), CRIF GmbH, Factiva Limited/Dow Jones	– Personenstammdaten und Kontaktdaten, insbesondere Name, Geburtsdatum, Adresse – Risikodaten, insbesondere Bonität, offene Forderungen und Schulden, vertragswidriges Verhalten	**Zusätzlich zu (A), (C) und (D):** **(F)** Eigenes berechtigtes Interesse und berechtigtes Interesse anderer Banken und Finanzinstitute am Gläubigerschutz und der Risikominimierung
Andere Institute aus dem Verbund von Erste Group, Erste Bank und Sparkassen	– Personenstammdaten und Kontaktdaten, insbesondere Name, Geburtsdatum, Adresse – Risikodaten, insbesondere Bonität, offene Forderungen und Schulden – Strafrechtliche Verurteilungen und Straftaten sowie Daten zu Compliance & Recht, wie Daten über Geldwäscheverdachtsfälle	**Zusätzlich zu (B) und (C)** **(G)** Risikosteuerung und Konsolidierung im Kreditinstitute-Verbund nach dem Bankwesengesetz und der EU-Kapitaladäquanz-Verordnung **(H)** Marketingzwecke, sofern eingewilligt wurde
Adressverlage und Direktmarketingunternehmen gemäß § 151 Gewerbeordnung	Personenstammdaten und Kontaktdaten, insbesondere Name, Geburtsdatum, Adresse und persönliche Informationen (Zugehörigkeit der Person zu einem Kunden- und Interessentendateisystem)	**Zusätzlich zu (D) und (G)** **(I)** Vermeiden von Werbung zu bereits genutzten Produkten
Unsere Kooperationspartner bei vermittelten Produkten (z. B. s Versicherung – WIENER STÄDTISCHE Versicherung AG Vienna Insurance Group; s Bausparkasse)	– Personenstammdaten und Kontaktdaten, insbesondere Name, Geburtsdatum, Adresse – Konto-/Produktdaten, Finanztransaktionen	**Zusätzlich zu (G) und (H)** **(J)** Vertragserfüllung; berechtigtes Interesse an Maßnahmen zur Geschäfts- und Vertriebssteuerung; Abrechnung etwaiger Provisionen
Verdachtsdatenbank für Bank- und Finanzinstitute (CRIF GmbH)	– Personenstammdaten und Kontaktdaten, insbesondere Name, Geburtsdatum, Adresse – Daten über den strafrechtlich relevanten Verdachtsfall während der Geschäftsbeziehung oder bei ihrer Anbahnung (insbesondere Sachverhalt, Verdachtskategorie und Verdachtsart)	**Zusätzlich zu (B) und (C)** **(K)** Berechtigtes Interesse am Schutz vor einem möglichen Betrug/Betrugsversuch sowie ähnlichen Straftaten (§ 4 Absatz 3 DSG) bzw. einem Reputationsschaden.
Intermediäre nach § 178 Z 1 Börsegesetz	Informationen über die Identität von Aktionärinnen nach § 178 Z 5 Börsegesetz –	**(K)** Identifizierung von Aktionär:innen, sofern diese 0,5 % oder mehr an Aktien oder Stimmrechten halten.
Banken und Finanzinstitute im Auslandszahlungsverkehr, wenn die Erste Group Bank AG als Korrespondenzbank die Zahlung abwickelt (https://www.erstegroup.com/de/financial-institutions/cash-management-fin-institutions)	– IBAN und Kontonummer der Zahler:in und Zahlungsempfänger:in – Kontowährung, Transaktionswährung, Betrag der Transaktion	**Zusätzlich zu (B) und (C)** **(L)** Tätigkeit als Korrespondenzbank im Zwischenbankengeschäft **(M)** Berechtigtes Interesse an einer kostengünstigen und effizienten Abwicklung der Transaktion

Für die soeben genannten Datenkategorien und Datenverarbeitungen gelten auch die übrigen Ausführungen dieses Informationsblattes, ausgenommen Punkt 4.

6. Bin ich verpflichtet, meine personenbezogenen Daten bereitzustellen? Was geschieht, wenn ich das nicht möchte?

Für unsere Geschäftsbeziehung sind wir auf viele Ihrer personenbezogenen Daten angewiesen, z.B. um Ihnen eine nachbestellte Debitkarte zuzusenden. Wenn wir Ihre Identität nicht prüfen können, verbietet uns das Gesetz die Geschäftsbeziehung. Kennen wir Ihre Bonität nicht, dürfen wir Ihnen keinen Kredit geben. Sie sehen: Dort, wo es aufgrund eines Vertrags oder einer rechtlichen Vorschrift erforderlich ist, müssen wir Ihre personenbezogenen Daten verarbeiten. Möchten Sie dies nicht, kann es sein, dass wir bestimmte Dienstleistungen leider nicht erbringen dürfen. In allen

anderen Fällen verarbeiten wir Ihre Daten nur mit Ihrer Einwilligung – und die ist selbstverständlich rein freiwillig. Sie sind nicht verpflichtet, in diesen Fällen Ihre Daten bereit zu stellen.

7. Gibt es eine Entscheidungsfindung, die auf automatisierter Verarbeitung beruht, inklusive Profiling?

Sofern bei einer spezifischen Verarbeitung eine automatisierte Entscheidungsfindung inklusive Profiling stattfindet, werden Sie dort vorab darüber informiert.

Bei der Kreditvergabe prüfen wir die Bonität mit dem sogenannten Kredit-Scoring. Dabei wird das Ausfallsrisiko von Kreditsuchenden mithilfe statistischer Vergleichsgruppen bewertet.
Der errechnete Score-Wert ermöglicht eine Prognose, mit welcher Wahrscheinlichkeit ein beantragter Kredit voraussichtlich zurückgezahlt wird. Zur Berechnung dieses Score-Wertes dienen folgende Daten:

- Ihre Stammdaten, z. B. Familienstand, Zahl der Kinder, Dauer der Beschäftigung, Arbeitgeber etc.
- Angaben zu den allgemeinen finanziellen Verhältnissen, z. B. Einkommen, Vermögen, monatliche Ausgaben, Verbindlichkeiten, Sicherheiten etc.
- Daten zum Zahlungsverhalten, z. B. Kreditrückzahlungen, Mahnungen, Daten von Kreditauskunfteien

Ist das Ausfallsrisiko zu hoch, wird der Kreditantrag abgelehnt und es kann einen Eintrag in die KKE des KSV 1870 sowie einen internen Warnhinweis geben. Wurde ein Kreditantrag abgelehnt, ist dies in der KSV 1870 KKE für 6 Monate ersichtlich, gemäß Bescheid der Datenschutzbehörde.

8. An wen werden meine personenbezogenen Daten weitergegeben?

Ihre personenbezogenen Daten können weitergegeben werden an:

- Kreditinstitute, Stellen und Personen innerhalb des Verbundes von Sparkassen, Erste Bank und Erste Group, die diese Daten für vertragliche, gesetzliche oder aufsichtsrechtliche Pflichten sowie für berechtigte Interessen benötigen. Das gilt besonders für das Risikomanagement innerhalb der Erste Group sowie für das Management von Kreditrisiken, wenn Kreditinstitute innerhalb der Erste Group idente Kund:innen haben.
- Auskunfteien, wie z. B. den Kreditschutzverband von 1870
- Öffentliche Stellen und Institutionen sowie Personen im hoheitlichen Auftrag, sofern wir rechtlich dazu verpflichtet sind oder um unsere berechtigten Interessen zu wahren, z. B. Europäische Bankenaufsichtsbehörde, Europäische Zentralbank, Finanzmarktaufsicht, Oesterreichische Nationalbank, Finanzbehörden etc.
- Von uns beauftragte Auftragsverarbeiter:innen und sonstige Dienstleister:innen (Verantwortliche), z. B. für IT, Backoffice, Rechts- und Steuerberatung, Wirtschaftstreuhand- und Inkassounternehmen, sofern diese die Daten für ihre Aufgabe benötigen
- Bank- und Jahresabschlussprüfer:innen, soweit dies für die Prüfungstätigkeit erforderlich ist
- Dritte, sofern es für die Vertragserfüllung oder rechtliche Vorschriften verpflichtend ist, z. B. die Empfänger:in einer Überweisung und deren Zahlungsdienstleister:in.
- Validierungsdienste wie z. B. die Rundfunk und Telekom Regulierungs-GmbH, sofern dies erforderlich ist, um eine von Ihnen übermittelte elektronische Signatur oder ein elektronisches Siegel zu prüfen
- Vertrauensdiensteanbieter:innen, z. B. A-Trust, wenn wir ein Dokument elektronisch signieren, das Ihre Daten enthält.

Die Weitergabe an Dritte kann auch dann erfolgen, wenn und solange Sie in die Weitergabe eingewilligt haben.

Eine Liste mit einer Übersicht möglicher Empfänger:innen finden Sie auf der Seite Ihres Instituts unter: https://sparkasse.at/dsgvo.

9. Werden meine personenbezogenen Daten in ein Drittland übermittelt?

Ihre personenbezogenen Daten können in den folgenden Fällen in ein Drittland übermittelt werden:
- Wenn dies erforderlich ist, um Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen bzw. auch wenn eine Rechtspflicht vorliegt, z. B. auf behördliche Aufforderung im Rahmen eines Rechtshilfeabkommens.
- Sofern es für Ihren Vertrag oder für vorvertragliche Maßnahmen erforderlich ist, z. B. wenn eine Überweisung in ein Drittland vorgenommen wird.
- Unsere Auftrags- und Sub-Auftragsverarbeiter:innen können in Drittländern ansässig sein. Sofern die Übermittlung nicht auf Grundlage eines Angemessenheitsbeschlusses der Europäischen Kommission erfolgt, übermitteln wir die Daten auf Basis geeigneter oder angemessener Garantien. Auf Anfrage stellen wir Ihnen diese gern zur Verfügung.
- In anderen Fällen, in denen an ein Drittland übermittelt wird, werden Sie gesondert informiert.

Eine Liste mit einer Übersicht möglicher Drittland-Empfänger:innen finden Sie auf der Seite Ihres Instituts unter: https://sparkasse.at/dsgvo.

10. Wie lange werden meine personenbezogenen Daten aufbewahrt?

Ihre personenbezogenen Daten werden so lange aufbewahrt, wie es für den jeweiligen Zweck erforderlich ist: Das kann etwa die Dauer der Kundenbeziehung, ein anhängiges Gerichtsverfahren oder der Bestand einer Forderung sein oder wenn es ein Gesetz vorschreibt. Die Aufbewahrung kann auch erforderlich sein, wenn Sie nicht mehr unsere Kund:in sind.

Die für ein Kreditinstitut wesentlichen gesetzlichen Bestimmungen sind z. B.:

- Unternehmensgesetzbuch § 212 (7 Jahre)
- Bundesabgabenordnung § 132 (7 Jahre oder für die Dauer eines Abgabenverfahrens);
- Wertpapieraufsichtsgesetz 2018 § 33 (5 oder 7 Jahre auf Anordnung der Finanzmarktaufsicht).
- Finanzmarkt-Geldwäschegesetz § 21 (10 Jahre ab Ende der Geschäftsbeziehung).

Eine Übersicht über weitere in Österreich geltende gesetzliche Aufbewahrungspflichten finden Sie z. B. hier:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html[1]

In folgenden Fällen hat die Bank ein berechtigtes Interesse, Ihre personenbezogenen Daten aufzubewahren:
- Finanzierungsanträge können jedenfalls bis zu 18 Monate nach Erstellung aufbewahrt werden. Dies dient unserem berechtigten Interesse, den Kundenkontakt zu dokumentieren und den Antrag rasch weiterbearbeiten zu können, wenn Sie wieder zu uns kommen.
- Wenn Sie den George Store nutzen und den Kauf nicht abschließen, werden Ihre personenbezogenen Daten 60 Tage lang gespeichert. In dieser Zeit können Sie den Wiederherstellungs-Link verwenden und den Kauf abschließen.
- Wenn Sie den George Store nutzen, werden Metadaten (z. B. Logdaten, technische Protokolldaten, Datum und Zeitstempel) im Zusammenhang mit dem abgeschlossenen Kauf 60 Tage lang aufbewahrt. Das machen wir, um potenzielle betriebliche Probleme zu erkennen, die sich aus dem Ablauf des Kaufs ergeben. Außerdem nutzen wir diese Daten, um mögliche Rechtsansprüche abzuwehren und um Wartungsarbeiten durchzuführen.
- SWIFT-Nachrichten werden zur Betrugsprävention und -bekämpfung sowie zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung 30 Jahre lang aufbewahrt.
- Daten über verkaufte Forderungen werden 30 Jahre ab Verkauf aufbewahrt. Dies dient dem berechtigten Interesse der Bank, mögliche Einwendungen aus dem Forderungsverkauf abzuwenden.
- Ihre personenbezogenen Daten können auch zur Dokumentation vergangener Schadensfälle aufbewahrt werden, als Entscheidungshilfe über das Eingehen neuer oder erweiterter

[1] Trotz sorgfältiger Prüfung kann keine Haftung für externe Inhalte übernommen werden.

Kundenbeziehungen. Konkret:
- 7 Jahre bei einem Schadensfall, wenn
  - die Schadenshöhe zum Fallabschluss maximal 20.000 Euro betragen hat oder
  - sonst aufgrund besonderer Umstände kein Interesse an einer Geschäftsbeziehung besteht
- 12 Jahre bei einem Schadensfall, wenn
  - die Schadenshöhe zum Fallabschluss mehr als 20.000 Euro betragen hat oder
  - während unserer aufrechten Geschäftsbeziehung über Ihr Vermögen die Insolvenz eröffnet wurde.
- 30 Jahre in besonders schwerwiegenden Ausnahmefällen nach eingehender Prüfung im Einzelfall.

Die Aufbewahrungsdauer beginnt, wenn der Schadensfall abgeschlossen wurde, das heißt sobald keine Schuld oder Forderung mehr besteht oder ein Insolvenzverfahren beendet oder aufgehoben wurde. Darüber hinaus müssen Daten über vergangene Schadensfälle zu regulatorischen Zwecken aufbewahrt werden, z. B. werden die Daten auch für unser Modell zur Berechnung von Ausfällen herangezogen. Auf diese Daten hat jedoch nur ein beschränkter Personenkreis Zugriff. Für Kundenbetreuer:innen sind sie nicht mehr ersichtlich. Die Daten haben auch keine Auswirkungen auf eine bestehende oder zukünftige Geschäftsbeziehung.

11. Welche Rechte habe ich?

Die DSGVO gewährt Ihnen einige Rechte zu Ihren personenbezogenen Daten. Sie haben das Recht auf: Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und auf Entscheidungen, die nicht ausschließlich auf einer automatisierten Verarbeitung beruhen – einschließlich Profiling. Ausführliche Informationen und wichtige Hinweise zum Recht auf Datenübertragbarkeit finden Sie auf der Seite Ihres Instituts unter: https://sparkasse.at/dsgvo.

Egal, welches Recht Sie geltend machen möchten, bitte übermitteln Sie Ihren Antrag (mit dem Hinweis über Ihr kontoführendes Institut) auf eine der fünf Arten an uns:

- Per s Kontakt-Nachricht in George
  Hier geht es am schnellsten! Wenn Sie zwischen Themen auswählen können, klicken Sie auf „Datenschutz Grundverordnung / DSGVO“. Sonst schreiben Sie einfach „Datenschutz“ in den Betreff Ihrer Nachricht.
- Über unser Webformular zur Einmeldung von Betroffenenrechten auf der Webseite unter „Datenschutz/Sicherheit“ - „Wie und wo kann ich meine Rechte geltend machen?“
- Per E-Mail, idealerweise mit qualifizierter elektronischer 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 Identität verlangen. Dies dient auch Ihrem Schutz, um nur Berechtigten den Zugriff zu Ihren Daten zu geben. Wenn Sie keine rechtzeitige Antwort auf einen Antrag erhalten oder der Ansicht sind, dass wir Ihrem Antrag nicht gesetzmäßig nachgekommen sind, oder Sie sich in Ihrem Recht auf Datenschutz verletzt sehen, können Sie auch Beschwerde bei der zuständigen Aufsichtsbehörde einlegen:

Österreichische Datenschutzbehörde
Barichgasse 40-42, 1030 Wien
https://www.dsb.gv.at

Stand: Mai 2025

Impressum: Medieninhaberin, Herstellerin, Herausgeberin und Redaktion: Erste Group Bank AG
Postanschrift: Am Belvedere 1, 1100 Wien