ERSTE Group

Data protection information

Data protection information

This document provides you with information on the protection of your personal data, such as your name, date of birth, occupation or account number. The protection of your data is governed by the **General Data Protection Regulation** (GDPR).

You can find more detailed information on the internet at https://sparkasse.at/dsgvo
On this website, you can also find information on shared responsibilities, i.e. two or more data controllers may jointly define the purpose and nature of the processing your data.

1. Who is the controller? Who is responsible for processing my personal data?

Erste Group Bank AG
Am Belvedere 1, 1100 Vienna

Contact for requests related to data protection:

- Erste Group Bank AG, 0196 1905/AT Data Privacy Security Management, Am Belvedere 1, 1100 Vienna
- Email: DSGVO-Support@erstegroup.com
- The quickest way to get in touch is by sending a message in your George app. Select “General Data Protection Regulation / GDPR” from the topics offered. Alternatively, you may indicate “Data protection” in the subject line of your message or email

2. Who is the Data Protection Officer?

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

3. What personal data is processed and how is it collected?

Which of your personal data is processed depends on the nature of the business relationship between us. Please find below the data that we may collect directly from data subjects. We may also generate information from the data collected.

Please note: We do not necessarily process all the data we collect from you.

Personal details:	Name, address, date of birth, nationality, marital status, etc.
Contact data:	Email address, telephone number, etc.
Identification data:	User name, IP address, images, customer short name, customer ID, user number, ID type and number, browser fingerprint, cookie ID, social security number, personnel number, documents, etc.
Personal information:	Employment, language, customer account manager at the credit institution, etc.
Relationships:	Authorised representative, customer relationship, etc.
Marketing and customer relationship management (CRM):	Financial health indicators, personal interests, event invitations, etc.
Behavioural data:	Click history in George or on our websites, data on product usage, etc.

Account/product data:	Debit cards, credit cards, IBAN, insurance policies, terms and conditions, securities account, insurance, etc.
Financial transactions:	Securities purchases, transactions in payment accounts, salary payments, etc.
Risk data:	Creditworthiness, risk class, risk calculations/rating, loan arrears, etc.
Compliance and legal data:	Legal proceedings, reports to authorities, fraud, warnings, etc.
Business documents:	Contracts and agreements, settlement and management of securities transactions, mortgage registration documents, etc.
IT data:	Log files, log-in data, change data and change history, etc.
Audio and image data:	Voice recordings, videos, images, etc.
Criminal convictions and punishable acts:	Criminal complaints, charges and judgments; administrative fines and penalties, etc.

We collect your personal data in various places and on various occasions, e.g. when you:

- visit one of our branches or use a self-service terminal
- open or use our products
- use our online services (in particular websites, internet banking, apps)
- use other services or contact channels offered by us, e.g. 24/7 service, prize competitions, events

4. What is the purpose of processing my personal data? What is the legal basis?

We are established as a bank in accordance with Section 1(1) of the Austrian Banking Act (BWG) and as a credit institution in accordance with Article 4(1)(1) of the EU Capital Requirements Regulation. We also act as an intermediary for other products and services, such as insurance policies and home savings plans. We need to process your personal data in order to provide these services.

Processing of data for performing a contract or taking steps at your request prior to entering into a contract

The services we provide to you may vary depending on the specific contract or agreement concerned (e.g. loan agreement, account agreement, leasing contract, insurance policy or a George online banking agreement).

We need to process your data, for example, to enable you to log in to your George account and to use the app to transfer funds. The details of such data processing is set forth in the contract or agreement and the terms and conditions.

We analyse and organise the stored data for use in our George internet banking services. This includes:

- processing personal information
- processing account balances, postings and transaction data
- categorising transactions
- indexing this data to enable faster searches in George

The activities described above also apply to data you upload to George internet banking yourself.

Processing of data for ensuring compliance with legal obligations

We may also need to process your personal data to meet legal requirements, such as the provisions of:

- the Banking Act (BWG)
- the EU Capital Requirements Regulation
- the Securities Supervision Act (WAG)
- the Financial Markets Anti-Money Laundering Act (FM-GwG)
- the EU Funds Transfer Regulation
- the EU sanctions regulations

We process your personal data when performing the following tasks:

- Risk management, especially for assessing credit risk and the risk of losses resulting from inadequate or failed internal processes or employee actions (operational risk)
- Handling, processing and analysing complaints
- Monitoring for insider dealing, conflicts of interest and market manipulation
- Identity verification, monitoring of transactions, suspicious activity reporting, compliance with sanction regulations, establishing the origins or sources of funds, information on the nature and purpose of the business relationship
- Compliance with sanctions
- Reports to the central accounts register and reporting of capital outflows
- Payment services, e.g. for detecting unauthorised or fraudulent payment transactions
- Accounting, controlling and compliance with laws and regulations on taxes and duties
- Recording of telephone conversations and electronic communications related to securities transactions
- Responding to inquiries and requests from public prosecutors, courts of law and financial crime authorities
- Disclosure of information on the identity of shareholders

Processing of data for purposes of legitimate interests

Processing of your personal data based by us or a third party may be based on a legitimate interest in the following cases:

- To show you useful functions, products, features and services in George
- To comply with non-binding recommendations issued by the authorities
- To implement measures to protect employees, customers and the bank's property
- To exercise or defend our rights
- To exchange data with credit reference agencies and credit bureaus for risk assessment purposes, e.g. data contained in the warning list of Austrian banks or kept by Kreditschutzverband von 1870 (KSV1870)
- To prevent and combat fraud, money laundering and terrorist financing, e.g.
  - Banks and financial institutions use a suspicious activity database (VDB). In this database, cases of suspected fraud, attempted fraud and similar criminal acts occurring in connection with, or during preparation of, business relations are recorded. CRIF GmbH is the processor of the data kept in this database. As a bank, we can access this database before entering into a new business relationship to verify if it contains any information on the person concerned
  - Identification of patterns of suspicious behaviour using data models
- To record past loss events. This data can help us decide whether to accept a new customer or extend an existing customer relationship
- To improve the quality of data
- To safeguard IT security and the bank's IT operations
- To make recordings and written records of telephone conversations for the following purposes: Documentation of statements and declarations with legal implications, identification of possible improvements to products and services, quality monitoring of services and identification of potential improvements for call centre employees. We store audio recordings and pass them on to third parties only if needed as evidence. You can find more detailed information on the data processing activities here: https://www.sparkasse.at/tiny/datenschutz-aufzeichnungen
- To use video surveillance, which we do only for the following reasons:
  - Ensuring that only authorised persons access our premises
  - Preventing attacks
  - Collecting evidence of criminal acts
  - Protecting our customers, employees and property
  - Enforcing and defending legal claims
  - Tracking user activity and payments, e.g. at cash machines
  - Persons who are authorised to operate an account can, for example, make bank transfers or set up standing orders. We use video surveillance to identify the person who used your account to make a payment or carry out a transaction.
    We may also use the video recordings for employee security training. However, we use the video material only after careful examination and selection of specific situations, always meeting applicable safety and security requirements

- To process data for business, sales and corporate governance purposes, e.g.
  - for grouping together customers with similar characteristics (customer segmentation)
  - when considering new structures and exploring customer characteristics
  - for avoiding advertising products that customers already use
  - for defining the overall business strategy and product portfolio

  This also includes the development of data models for this purpose.
- To collect data for optimising our work processes and the quality of our services. This helps us ensure the highest possible quality of our services and processes
- To provide data on your financing potential at any time
- To select customers for customer satisfaction surveys
- To promote the development of new products, including using data models
- To create synthetic or anonymised data that is similar to real data. In a small number of cases we may also need to use real data for testing purposes
- To verify electronic sign-offs. If you send us a document with an electronic signature or an electronic seal, we will forward it to a verification service. These are companies that check whether a signature or seal is genuine, such as the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR)
- To provide electronic sign-offs. When we e-sign a document containing your data, we send it to a qualified trust service provider, e.g. A-Trust
- To ensure high-quality advice and services across all channels. In accordance with our guiding principle, we strive to ensure financial health for all our customers
- To this end, we have defined a standard pathway for advisory services - based on the data we receive and aligned with our customers' needs

  We aim to provide our customers with professional advice tailored to their best interests. We use the following data to do this:
  - Personal details, including name, date of birth and address
  - Data on the products our customers use
  - Data on transactions

  We use this data to assess which advice is most suitable for you. We identify your financial needs using the following data:
  - What are your monthly incoming and outgoing payments?
  - How much money do you currently have available, what savings do you have?
  - What is your investment plan?
  - Are there any life insurance or other retirement plans?
  - How are the risks covered?
  - Is there any (debt) financing?

  By answering those questions and analysing the related data, we can provide even better advice. In addition, we will show you helpful tips ("Insights") on your financial health in George.

  We store this information to ensure financial advice remains consistent over time. However, we will delete your data after 7 years or when our business relationship ends.

Processing with consent

We may also process your data in the absence of a contract, legal requirement or legitimate interest provided that you give your consent. Which data we process and for what purpose depends on the scope of your consent. For example, you can permit us to take a photo of you for identification purposes.

You can revoke your consent at any time. However, this will apply only for future processing, meaning that any processing carried out before your withdrawal of consent remains lawful.

Processing for statistical purposes

We process personal data for statistical purposes in accordance with Section 7 of the Austrian Data Protection Act (DSG).

5. Does the bank process data other than the data collected from me?

Most of the personal data we process is data provided by you. However, we may also receive data about you from other sources.

Data source	Data categories	Purposes and legal basis
Public registers, e.g. companies register, land register, insolvency database, register of associations, central register of residents, business register	– Personal details and contact data, in particular name, date of birth, address – Personal information, such as functions, activities, in particular occupation, corporate offices (membership of corporate bodies, e.g. board of directors or management), shareholdings, economic activities – Property or land ownership and any related encumbrances, such as liens – Risk data, e.g. solvency data, in particular information on insolvency, bankruptcy	(A) Due diligence requirements for banking risks and operational risks (e.g. credit risk management) in accordance with the Austrian Banking Act and the EU Capital Requirements Regulation (B) Due diligence requirements under the Financial Markets Anti-Money Laundering Act and sanction regulations (C) Legitimate interest in preventing and combatting fraud and similar criminal offences; preventing money laundering and terrorist financing (D) Legitimate interest in improving the quality of data (E) Legitimate interest in maintaining an overview across Erste Group as a whole
Registers of debtors and warning lists, e.g. by KSV1870, CRIF GmbH, Factiva Limited/Dow Jones	– Personal details, in particular name, date of birth and address – Risk data, e.g. outstanding accounts receivable, debts and data on breach of contract	**In addition to (A), (C) and (D):** (F) Our legitimate interest or the legitimate interest of other banks and financial institutions in creditor protection and risk minimisation
Other affiliated companies or entities of Erste Group, Erste Bank und Sparkassen	– Personal details and contact data, in particular name, date of birth and address – Risk data, e.g. solvency data, in particular outstanding accounts and debts – Data on suspected cases of money laundering, criminal convictions and criminal activity as well as compliance data and legal data	**In addition to (B) and (C):** (G) Risk control and consolidation among credit institutions in accordance with the Banking Act and the EU Capital Requirements Regulation (H) Marketing purposes, provided that customers have given consent
Marketing data brokers and direct marketing companies in accordance with Section 151 of the Austrian Trade, Commerce and Industry Regulation Act (GewO)	– Personal details and contact data, in particular name, date of birth and address – Personal information, e.g. data on whether a person is recorded in a file system for (potential) customers	**In addition to (D) and (G):** (I) We want to avoid advertising of products that our customers already use
Our business partners for intermediary products, e.g. s Versicherung - WIENER STÄDTISCHE Versicherung AG Vienna Insurance Group or s Bausparkasse	– Personal details and contact data, in particular name, date of birth and address – Data on accounts or products you use and data on transactions	**In addition to (G) and (H):** (J) Contract performance; legitimate interest in controlling business and sales

Suspicious activity database for banks and financial institutions (CRIF GmbH)	– Personal details and contact data, in particular name, date of birth and address – Data on suspected criminal acts if discovered in connection with, or during preparation of, business relations In particular, data on the circumstances and type and nature of the suspected criminal act	**In addition to (B) and (C):** (K) Legitimate interest in protection against (attempted) fraud and similar criminal acts (Section 4(3) Data Protection Act); legitimate interest in protection against reputational damage for the bank
Intermediaries in accordance with Section 178(1) of the Austrian Stock Exchange Act (BörseG), e.g. credit institutions or custodians that manage securities or securities accounts	– Information on the identity of persons who own securities (shareholders), in particular for identification purposes	(L) Information on the identity of persons who own securities (shareholders); identification of shareholders if they hold 0.5% or more of the shares or voting rights
Banks and financial institutions involved in foreign payment transactions if Erste Group Bank AG processes the payment. Erste Group Bank AG acts as the correspondent bank You can find more detailed information here: https://www.erstegroup.com/en/financial-institutions/cash-management-fin-institutions	– IBAN and account number of the payers and the recipients – Currency of the accounts, currency of the payment, payment amount	**In addition to (B) and (C):** (M) Acting as the correspondent bank in interbank transactions (N) Legitimate interest in cost-effective and efficient payment processing

The information here also applies to all the other types of data and the data processing activities mentioned in this information notice (except for item 4 above "What is the purpose of processing my personal data? What is the legal basis? What personal data is processed and how is it collected?")

6. Is there an obligation to provide my personal data? What happens if I do not want to provide my personal data?

We need much of your personal data to do business with you, for example to send you a new debit card. Austrian law requires us to verify your identity. We need information on your solvency to grant a loan to you.

We must process your data if required by law or under a contract. If you do not want us to process such data, we may not be able to provide certain services to you.

In all other cases, we will only process your data if you give your consent. This consent is freely given and entirely voluntary. You are not obliged to provide your data in such cases.

7. Is there any automated decision-making, including profiling?

If we make decisions based on automated data processing, we will inform you in advance.

When we grant a loan to you, we will review your solvency using credit scoring. This means we assess the risk of whether you will be able to repay the loan. To do this, we compare persons who want to take out a loan with other groups of persons.

The resulting credit score gives us an idea of how likely you are to repay the loan.

For calculating your credit score we need the following data:

- Personal details, e.g. marital status, number of children, duration of employment or employer
- Data on general financial circumstances, e.g. income, assets, monthly expenditure and regular payments
- Data on payment behaviour, e.g. loan repayment, payment reminders and data from credit reference agencies and credit bureaus

If the risk is too high, we will refuse the loan. An entry may be made in the KSV1870 consumer credit register (KKE). In addition, an internal warning may be issued.

If a loan application is rejected, this will be shown in the KKE consumer credit register for 6 months (based on a decision of the Austrian Data Protection Authority).

8. Who will receive my personal data?

- Credit institutions, entities and persons in the network of affiliates of Sparkassen, Erste Bank and Erste Group. These entities or persons will receive your personal data if needed for the following purposes:
  - Contractual, statutory or regulatory obligations
  - Risk management within Erste Group; credit risk management where credit institutions within Erste Group have the same customers
  - Other legitimate interests
- Credit reference agencies and credit bureaus, such as KSV1870
- Public bodies and institutions as well as persons acting under government mandate as required by law or needed to protect our legitimate interests, e.g.:
  - European Banking Authority
  - European Central Bank
  - Austrian Financial Market Authority
  - Oesterreichische Nationalbank
  - Tax authorities and other public bodies
- Data processors and other service providers mandated by us (controllers), e.g. IT and back office services providers, law firms and tax consultants, chartered accountants and auditors as well as debt collectors. We may disclose your data where necessary for the mandate
- Bank auditors and auditors of annual financial statements where necessary for the audit
- Third parties if mandatory for compliance with the provisions of a contract or the law, e.g. the recipient of a bank transfer and their payment service provider
- Verification services that check your electronic signature or seal, such as the Austrian Regulatory Authority for Broadcasting and Telecommunications
- Qualified trust service providers, such as A-Trust. We use trust service providers to e-sign a document containing your data

If you have given your consent, we may also disclose your data to other third parties.

You can find a list of potential recipients of your data here:
https://sparkasse.at/dsgvo

9. Will you transmit my data to non-EU countries?

We may transmit your data to a non-EU country (third country), if

- this is necessary for us to assert, exercise or defend legal claims or if there is a legal obligation requiring us to do so, e.g. in the case of a mutual legal assistance treaty
- this is necessary for performing or drafting and preparing a contract, e.g. to transfer funds to a third country
- Our processors and sub-processors may be located in third countries. If the transfer is not based on an adequacy decision of the European Commission, we transmit the data on the basis of suitable or appropriate safeguards. We will provide you with information on such safeguards on request
- Should we transfer data to a non-EU country in other cases, we will inform you separately
- You can find a list of potential third-country recipients of your data here: https://sparkasse.at/dsgvo

10. How long do you keep my personal data?

We store your personal data for as long as it is needed for a specific purpose, e.g.

- for the duration of our business relationship
- for the duration of pending legal proceedings
- for as long as we have a claim against you
- as required by law

We may need to keep your data even after our business relationship with you has ended.

Data retention is governed by legal provisions, e.g. the Austrian

- Business Code (UGB) - Section 212
  Retention of data: 7 years
- Tax Code (BAO) - Section 132
  Retention of data: 7 years or as long as any tax proceedings are pending
- Securities Supervision Act 2018 (WAG) - Section 33
  Retention of data: 5 Years (7 years upon order of the Financial Market Authority)
- Financial Markets Anti-Money Laundering Act (FM-GwG) - Section 21
  Retention of data: 10 years from the end of the business relationship or, if a transaction is carried out outside of a business relationship (occasional transaction), 10 years after the transaction

In addition, there may be further provisions that govern the retention of data in Austria. You can find an overview here https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html

The bank may also keep your data if there is a legitimate interest in doing so, e.g.:

- Financing (loan or credit) applications may be retained for up to 18 months after receipt because it is in our legitimate interest to document customer contact. This will speed up processing of your application if you get back to us later
- If you use the “George Store” feature and do not complete the purchase, we will store your personal data for 60 days. During this time, you can use the recovery link and complete the purchase
- If you use the “George Store” feature for a purchase, we will store the related metadata (e.g. log data, technical log data, date and timestamp) for 60 days. This may help us identify and fix any errors during the purchase process. We also use this data to enforce and defend our rights. We also store this data to enable us to carry out maintenance work
- SWIFT messages are stored for 30 years for the purpose of preventing and combatting fraud and preventing money laundering and terrorist financing. SWIFT messages are a secure way of transmitting e.g. payment instructions
- We retain data on receivables sold for 30 years from the date of sale as this serves the bank’s legitimate interest to avoid objections to the sale

- We may also retain your personal data to record past loss events. Additionally, we may use the data when deciding whether to accept a new customer or extend an existing customer relationship. The following periods apply:

  Retention for 7 years:

  - In the event of a loss of up to EUR 20,000
  - If the bank has no interest in a business relationship due to special circumstances

  Retention for 12 years:

  - In the event of a loss of more than EUR 20,000
  - If insolvency proceedings are initiated against your assets during our business relationship

  Retention for 30 years:

  - In exceptionally serious cases, the facts of which are subject to thorough scrutiny

The retention period begins

- when the loss event has been closed and any debts or claims have been settled
- when insolvency proceedings have been terminated or cancelled

In addition, we need to keep data on past loss events for analysis purposes, e.g. for modelling payment defaults. However, only a small group of persons can access this data. Customer account managers cannot access this data. This data is irrelevant for existing or future business relationships.

11. What are my rights as a data subject?

The GDPR gives you the following rights regarding personal data:

- Access to your personal data (Article 15)
- Rectification of your personal data (Article 16)
- Erasure of your personal data (Article 17)
- Restriction of processing of your personal data (Article 18)
- Portability of your personal data (Article 20)
- Objection to processing of your personal data (Article 21)
- Objection to automated individual decision-making (Article 22)

You can find more detailed information on the right to portability of your data here:
https://sparkasse.at/dsgvo

No matter which right you wish to exercise, do not hesitate to contact us. There are five ways to contact us:

- Send a message in your George app, this is the quickest way. Select “General Data Protection Regulation / GDPR” from the topics offered. You can also simply write “Data protection” in the subject line of your message
- Use the form on our website https://www.sparkasse.at/einmeldung-betroffenenrechte to exercise your rights as a data subject (“How and where can I exercise my rights?”)
- Send an email (ideally with electronic signature) to
  DSGVO-Support@erstegroup.com
- Post a letter signed by you (and attach a copy of your ID) to

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

- Come and see us in one of our branches

We may in some cases request further personal details to establish your identity. We do this to ensure that only authorised persons can access your data.

You may file a complaint, e.g.

- if you have not received a response to an application or request in due time
- if you think that we have not complied with your request as required by law
- if you believe that your right to privacy has been violated

Send your complaint to:

Österreichische Datenschutzbehörde (Austrian Data Protection Authority)

Barichgasse 40-42
1030 Vienna
https://www.dsb.gv.at

Version dated October 2025

Publishing information:
Media owner, producer, publisher and editor:
Erste Bank der oesterreichischen Sparkassen AG
Postal address: Am Belvedere 1, 1100 Vienna