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

Information on Data Protection and Data Processing

This document contains information on the protection of your personal data as regulated by the **General Data Protection Regulation** (GDPR). Additional information, including on joint controllerships, is available on the webpage of your Bank at: https://sparkasse.at/dsgvo

1. Who is the data controller?

Erste Group Bank AG
Am Belvedere 1, 1100 Vienna

Contact for data protection-related inquiries:

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

The fastest way to do this is via an s Contact message in George: if two topics are displayed for you to choose from, click on "General Data Protection Regulation (GDPR)". Otherwise, simply type "Data protection" in the subject line of your message.

2. Who is the Data Protection Officer?

Gregor König, Erste Group Bank AG, Am Belvedere 1, 1100 Vienna, DPO@erstegroup.com

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

Which of your personal data we process depends on the scope of the business relationship between you and us.
Here you will find a list of the possible data that we collect directly from the data subjects or derive from the data collected. Please note: This does not necessarily mean that we actually process this data from you:

Personal master data:	Name, address, date of birth, gender, nationality, marital status, etc.
Contact data:	E-Mail-address, telephone number, etc.
Identification data:	Username, IP address, images, customer short name, customer ID, user number, type and number of ID, browser-fingerprint, identification number for Internet cookies, social security number, personnel number, documents, etc.

Personal information:	Employment relationship, training, career, language, customer service at the bank, etc.
Personal relations:	Representation, customer relations, etc.
Marketing & CRM:	Financial health indicators, personal interests, invitations to events, etc.
Behaviour data:	Click history in George or on our websites, data on product usage, etc.
Account-/product data:	Debit cards, credit cards, IBAN, policies, conditions, securities custody account, insurance, etc.
Financial transactions:	Securities purchases, turnover from payment transaction accounts, salary payments, etc.
Risk data:	Creditworthiness, risk class, risk calculations/rating, loans with debtor default, etc.
Compliance & legal:	Legal proceedings, reports to authorities, cases of fraud, warnings, etc.
Business documents:	Contracts, service contracts, settlement and administration of securities transactions, mortgage certificates, etc.
IT-data:	Log-data, Log-in-data, Change data and history, etc.
Audio- and image data:	Voice recordings, videos, images, etc.
Criminal convictions and offences:	Criminal judgements, criminal charges, administrative penalty notices, etc.

We collect your personal data in various places and on various occasions when you:

- visit our branches or use self-service devices
- open or use one of our products
- use our online services (websites, internet banking, apps)
- use our other services and contact options (e.g. 24-hour service, competitions, events)

4. For what purposes and on what legal bases will my personal data be processed?

We are a bank organized according to Article 1 (1) of the Austrian Banking Act and Article 4 (1) 1 of the EU Capital Adequacy Regulation. In addition, we also act as mediator for other products and services, e.g. insurance and building society contracts. In the course of these activities, we process your personal data:

Processing for the performance of a contract or of pre-contractual measures taken upon your request
The services we are called upon to provide for you will depend on the contract in question, e.g. loan agreement, account contract, leasing contract, insurance brokerage or an agreement on George. We will need to process your data so that you can, for instance, log in to George, manage your account online and carry out transactions. The scope of such data processing will be set forth in the contract documents and the General Terms and Conditions.

We analyse the stored data for our Internet banking system George and prepare it technically for better presentation. In addition to personal information, account balances, bookings and turnover data, this processing also includes the categorisation of account transactions and the indexing of this data for faster searching in George. This also affects data that you have uploaded to George Internet banking yourself.

Processing to satisfy a legal obligation
We will need to process your data also on account of legal obligations, e.g. the Austrian Banking Act, the EU Capital Adequacy Regulation, the Securities Supervision Act, the Financial Markets Money Laundering Act and the EU Funds Transfer Regulation. This relates to:
- Risk management, especially credit risk and operational risk
- Complaint management and complaint handling, analysis of complaint cases

- Monitoring of insider trading, conflicts of interest and market manipulation
- Identity determination, transaction monitoring, reporting of suspicious activities, compliance with sanction regulations
- Reports to the account register and reporting of capital outflows
- Payment services, e.g. for the detection of unauthorised or fraudulent payment transactions
- Accounting, controlling and compliance with tax&fee regulations
- Recording of telephone conversations and electronic communication in the course of securities transactions
- Information to public prosecutors, law courts, tax penalty authorities
- Disclosure of information on the identity of shareholders

Processing due to legitimate interests
A legitimate interest for data processing by us or third parties exists in the following cases:
- Promotion of new products, features and services
- To comply with non-legally binding official recommendations
- Measures to protect employees, customers and the Bank's property
- Exercising or defending rights
- Data exchange for creditworthiness and default risks inquiries with an information bureau, for instance reports and queries regarding the warning list or the consumer credit record of the Kreditschutzverband von 1870 *(Credit Protection Association of 1870)*
- Preventing and combatting fraud as well as preventing money laundering and terrorist funding, including but not limited to:
  - Suspected cases of fraud and attempted fraud and similar criminal offences pursuant to Sections 146 et seq. of the Austrian Criminal Code (StGB) that are detected during the business relationship or during its initiation will be recorded and processed in the Suspicious Transaction Data Base (STDB) for banking and financial institutions. This data base is kept by CRIF GmbH as processor. Banking and financial institutions using this data base solution can also receive data with which they can check, at the beginning of a business relationship with a customer, whether fraud attempts have been made in the past.
  - Development of data models to detect suspicious behaviour patterns
- Documentation of past damage cases as a decision-making aid for entering into new or extended customer relationships.
- Improving data quality
- Ensuring the security of IT and of the Bank's IT operations
- Recording of telephone conversations, e.g. for complaint cases, documentation of legally relevant declarations (e.g. card blocking) or for training of our employees
- Video surveillance for enforcing our house rules, for the prevention of attacks, for collection of evidence in the case of criminal offences, protection of customers, employees and property, enforcement of and defence against legal claims or as evidence for dispositions and deposits, e.g. at cashpoints. Video recordings of such incidents can also be used for security training of our employees in individual cases after careful examination.
- Measures for business, sales and group management, such as customer segmentation, reorganisation and associated customer analyses, avoidance of advertising for products already in use as well as the general direction of the business strategy and product portfolio. This also includes the development of data models for such measures.
- Measures for process and quality management: We collect data on our processes and services on an event-driven basis. We use these data to ensure the quality of our services, compliance with our service standards and the efficiency of our processes.
- Ongoing calculation of your financing potential
- Selection to evaluate satisfaction with the services and products we offer
- Product development using, inter alia, data models
- Creation of synthetic or anonymised data for testing purposes (in limited cases it may also be necessary to use real data for testing purposes).
- If you send us a file containing a digital signature or a digital seal, we will transmit this document to a validation service (e.g. signature verification service of “Rundfunk und Telekom Regulierungs-GmbH” – the radio and telecommunications regulatory company) for signature/seal verification.
- If we provide a document that contains your data with our digital signature, we will transmit the document to a trust service provider (e.g. A-Trust).

- In order to increase the quality across all advisory interactions and therefore keeping up to our purpose of bringing financial health to all clients, we defined a data driven process analysing customer needs holistically.
  To ensure a professional preparation and interaction we analyse following data:
  - Master data, such as name, date of birth, address
  - Data of products and transactions

  Based on this information we derive our clients' actual financial status for the relevant financial needs: Monthly Cashflow (budget plan), Liquidity and Reserve, Building Wealth, Pre-caution, Protecting risks and Managing Debt. These objective criteria allow us to provide consistent service in the interest of our clients. For the sake of professional future advisory interactions, we save provided information. Data will be deleted if its either older than 5 years or if the business relationship is dissolved.
- Erste Group Bank AG has a legitimate interest in maintaining an organised overview of its group structure. For this purpose, it operates a database in which all Group holdings are mapped. The personal data stored includes the name, date of birth and business correspondence addresses of the respective office holders (e.g. members of the management, management board, supervisory board, etc.). This data is anonymised 20 years after the end of the last mandate or other internal function.

Processing on the basis of consent
If there is neither a contract nor a legal obligation or a legitimate interest, processing the data may still be lawful if you have given us your consent to do so. The scope and content of this data processing will invariably depend on the consent given in a certain case - for example, if you allow us to take your photo in the context of establishing your identity. You can withdraw your consent at any time for the future. The withdrawal of consent shall, however, not affect the lawfulness of processing before the withdrawal of consent. This means that withdrawal of consent shall not be effective for the past.

Processing for statistical purposes
We also process your personal data for statistical purposes in accordance with Article 7 of the Austrian Data Protection Act.

5. Will data other than those collected from me be processed?

Most of your personal data that we process will have been provided by you. However, your data may also originate from other sources:

Data source	Data categories	Purposes and legal bases
Publicly accessible, official registers such as companies registers, land registers, insolvency files, registers of associations, the central census bureau register, the trade register	– Personal master data, in particular name, date of birth, address – Personal information like functions, activities - in particular profession, board functions, shareholdings, economic activities, real estate ownership and associated encumbrances – Risk data (Creditworthiness data, in particular insolvencies, bankruptcies).	**(A)** Due diligence obligation in case of banking business and operational risks (e.g. credit risk management), Austrian Banking Act and EU Capital Adequacy Regulation. **(B)** Due diligence obligations under the Financial Market Money Laundering Act and sanctions regulations **(C)** Legitimate interest in preventing and combatting fraud (and similar criminal acts), prevention of money laundering and of terrorist funding **(D)** Legitimate interest in processing operations to improve data quality **(E)** Legitimate interest in maintaining an organised overview of its own group structure

Debtor directories and warning lists, e.g. Kreditschutzverband von 1870 (KSV 1870), CRIF GmbH, Factiva Limited/Dow Jones	– Personal master data, in particular name, date of birth, address – Risk data, in particular, creditworthiness data like receivables and debts due, behaviour contrary to contract	**In addition to (A), (C) and (D):** **(F)** Own legitimate interest and other banks' and financial institutions' legitimate interest in creditor protection and risk minimisation
Other institutes from the network of Erste Group, Erste Bank und Sparkassen	– Personal master data, in particular name, date of birth, address – Risk data, in particular, creditworthiness data like receivables and debts due – Criminal convictions and offences as well as compliance and legal data, such as data on suspected cases of money laundering	**In addition to (B) and (C)** **(G)** Risk control and consolidation in the network of credit institutions according to the Austrian Banking Act and the EU Capital Adequacy Regulation **(H)** Marketing purposes, if consent was granted
Address publishers and direct marketing companies pursuant to Article 151 of the Austrian Trade, Commerce and Industry Regulation Act	Personal master data, in particular name, date of birth, address, and personal information (affiliation of the person to a customer and potential customer file system)	**In addition to (D) and (G)** **(I)** Avoidance of advertising for products already in use
Our cooperation partners for brokered products (e.g. "s" Versicherung – WIENER STÄDTISCHE Versicherung AG Vienna Insurance Group; "s" Bausparkasse)	– Personal master data, in particular name, date of birth, address – Account/product data, financial transactions	**In addition to (G) and (H)** **(J)** Contract performance; legitimate interest in business and sales control measures
Suspicious activity data base for banking and financial institutions (CRIF GmbH)	– Personal master data, in particular name, date of birth, address – Data on the suspected case relevant under criminal law during the business relationship or at the time of its initiation (in particular, the facts, category of suspicion and type of suspicion)	**In addition to (B) and (C)** **(K)** Legitimate interest in the protection against possible fraud/attempted fraud as well as similar criminal offences (Article 4(3) of the Data Protection Act) or reputational damage
Mediators according to Article 178 subpara 1 Austrian Stock Exchange Act	Information on the identity of shareholders pursuant to Article 178 subpara. 5 Stock Exchange Act	**(L)** Identification of shareholders holding 0.5% or more of shares or voting rights.
Banks and financial institutions in foreign payment transactions, if Erste Group Bank AG settles the payment as correspondent bank (https://www.erstegroup.com/en/financial-institutions/cash-management-fin-institutions)	– IBAN and account number of the payer and payee – Account currency, transaction currency, amount of the transaction	**In addition to (B) and (C)** **(M)** Acting as a correspondent bank in interbank business **(N)** Legitimate interest in a cost-effective and efficient settlement of the transaction

For the categories of data and data processing mentioned above, the other explanations in this information sheet shall also apply (with the exception of item 4.)

6. Am I obliged to provide my personal data? What will happen if I do not want to do so?

For our business relationship, we require many of your personal data, e.g. for re-order of a debit card that is to be sent to you. If we cannot verify your identity, the law will prohibit us from doing business with you. If we do not know your creditworthiness, we will not be allowed to grant you a loan. So you see we must process your personal data wherever it is required by contract or by law. If you do not want us to do so, we may unfortunately not be allowed to provide certain services. In all other cases, we will process your data only with your consent – and any such consent must be given by you on a purely voluntary basis. You are in no way obliged to provide your data in these cases.

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

If automated decision-making, including profiling, takes place in the course of a specific processing operation, you will be informed of this in advance.

When granting loans, we check your creditworthiness on the basis of the so-called credit scoring. In the process, the default risk of credit applicants is assessed with the help of statistical benchmark groups.
The calculated score enables us to forecast the probability with which a loan applied for is likely to be redeemed. The following data are used to calculate this score:

- Your master data, e.g. marital status, number of children, length of employment, employer, etc.
- Information on your general financial circumstances, e.g. income, assets, monthly expenses, liabilities, collaterals, etc.
- Data on payment behaviour, e.g. loan repayments, reminders, data from credit information bureaus

If the risk of default is too high, the credit application will be rejected and there may be an entry in the KSV 1870 KKE and an internal warning. If a credit application is rejected, this will be shown in the KSV 1870 KKE for 6 months (according to the Notification of the data protection authority).

8. To whom will my personal data be disclosed?

Your personal data may be disclosed to:

- Credit institutions, bodies and persons within the network of Sparkasse savings banks, Erste Bank and Erste Group who require the data for contractual, legal or regulatory duties as well as for legitimate interests. This applies in particular to risk management within Erste Group and to the management of credit risks when credit institutions within Erste Group have identical customers.
- Information bureaus like Kreditschutzverband von 1870 *(Credit Protection Association of 1870*)
- Public bodies and institutions as well as persons with a sovereign mandate, to the extent that we are legally required to do so or in order to protect our legitimate interests, e.g. the European Bank Supervisors, the European Central Bank, Financial Market Authority, the Austrian National Bank, tax authorities, etc.
- Processors and other service providers (controllers) commissioned by us, e.g. for IT, back office, legal and tax advice, chartered accountants and collection companies, to the extent they require the data for their tasks.
- Bank auditors and auditors of annual financial statements, insofar as this is necessary for the auditing activity
- Third parties, if this is mandatory for the fulfilment of the contract or legal provisions, e.g. the recipients of a bank transfer and their payment service provider.
- Validation services, e.g. Rundfunk und Telekom Regulierungs-GmbH *(the radio and telecommunications regulation company*), to the extent this is necessary to verify a digital signature or digital seal transmitted by you.
- Trust service providers, e.g. A-Trust, if we provide a document containing your data with our digital signature.

Disclosure to third parties may also take place if you have consented to the disclosure and for the period of your valid consent.
A list containing an overview of potential recipients can be found on your bank's webpage at: https://sparkasse.at/dsgvo.

9. Will my data be transferred to a third country?

Your personal data may be transferred to a third country in the following cases:

- this is necessary in order to assert, exercise or defend legal claims or there is a legal obligation, e.g. at the request of the authorities under a mutual legal assistance agreement.
- This is necessary for your contract or for pre-contractual measures, for instance, if funds are to be transferred to a third country
- Our processors and sub-processors may be located in third countries. Unless the transfer is based on an adequacy decision of the European Commission, we will transfer the data on the basis of appropriate or suitable safeguards. We will be happy to provide you with these on request.
- You will receive a special notification in other cases of data being transferred to a third country.

A list containing an overview of potential recipients in third countries can be found on your Bank's webpage at: https://sparkasse.at/dsgvo.

10. How long will my personal data be stored?

Your personal data will be stored for as long as is necessary for the respective purpose: this may be the duration of the customer relationship, pending legal proceedings or the existence of a claim, or if required by law. Retention may also be necessary if you have ceased to be our customer.

The essential legal provisions applicable to credit institutions include:

- the Austrian Companies Code, Article 212 (7 years)
- the Federal Tax Code, Article 132 (7 years or for the duration of tax proceedings);
- the Securities Supervision Act 2018, Article 33 (5 or 7 years by order of the Financial Market Authority).
- Financial Market Money Laundering Act, Article 21 (10 years from the end of the business relationship).

An overview of other statutory retention obligations applicable in Austria can be found here, for example:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html[1]

The Bank has a legitimate interest in retaining your personal data in the following cases:
- Applications for financing can be kept for up to 18 months after they have been made. This serves our legitimate interest in documenting a customer contact and our ability to process the application quickly when you come back to us.
- If you use George Store and do not complete the purchase, your personal data will be stored for 60 days. During this time, you can use the recovery link and complete the purchase
- When you use the George Store, metadata (e.g., log data, technical log data, date and timestamp) related to the completed purchase is stored for 60 days. We do this to identify potential operational issues arising from the purchase process. We also use this data to defend against potential legal claims and to perform maintenance.
- SWIFT messages are kept for 30 years for the purpose of preventing and combatting fraud and for the prevention of money laundering and terrorist funding.
- Data on receivables sold are kept for 30 years from the date of sale. This serves the Bank's legitimate interest of averting possible objections arising from the sale of receivables.
- Your personal data may also be retained to document past damage cases, as an aid to decision-making about entering into new or extended customer relationships. Specifically:
  - 7 years in a damage case, if
    - the amount of damage at the time the case was closed did not exceed 20,000 euros, or
    - there is otherwise no interest in a business relationship due to special circumstances
  - 12 years in a damage case if
    - the amount of the loss at the time the case was closed was more than 20,000 euros, or
    - insolvency proceedings have been instituted against your assets during our business relationship.

[1] Even though we carefully check external links, we cannot be held liable for their content and security.

- 30 years in particularly serious, exceptional cases after detailed examination in each individual case.

The retention period starts when the damage case has been closed, i.e. as soon as a debt/claim no longer exists or insolvency proceedings have been terminated or cancelled. In addition, data on past damage cases must be stored for regulatory purposes, e.g. the data are also used for our model to calculate defaults. However, only a limited group of people will have access to these data. They are no longer visible to account managers. The data will also not affect existing or future business relationships.

11. What are my rights?

The GDPR grants you certain rights regarding your personal data. You have the right to access, rectification, erasure, restriction, data portability, objection and to decisions not based solely on automated processing, including profiling. For detailed information and important guidance on the right to data portability please visit the webpage of your Bank at: https://sparkasse.at/dsgvo.

No matter which right you wish to assert, please submit your request (with reference to your account-holding bank) in one of the five ways:

- by s Contact message in George:
  This is the fastest way! If two topics are displayed for you to choose from, please click on "General Data Protection Regulation" (GDPR). Otherwise, simply type "Data protection" in the subject line of your message
- via our web form for exercising data subject rights on the webpage under “Privacy / How and where can I assert my rights?”
- by e-mail, ideally with a qualified digital signature, to GDPR-Support@erstegroup.com
- by letter, signed in your own hand and with a copy of an identity piece, to:
  Erste Group Bank AG
  0196 1905/AT Data Privacy Security Management
  Am Belvedere 1, 1100 Vienna
- personally in one of the Bank's branches

Please understand that in case of doubt we may request further information about your identity. This also serves for your own protection, to prevent unauthorised persons from accessing your data. If you do not receive a timely response to a request or if you believe that we have not complied with your request in accordance with the law, or if you feel that your right to data protection has been violated, you will be entitled to lodge a complaint with the competent supervisory authority:

Austrian Data Protection Authority
Barichgasse 40-42, 1030 Vienna
https://www.dsb.gv.at

Version dated May 2025

Credits and legal notice: Owned, produced, published and edited: Erste Group Bank AG
Postal address: Am Belvedere 1, 1100 Vienna