Customer Information
Data Protection
12/2025

Bank Winter
SEIT 1892

1. General

Personal data and data applications are covered by the General Data Protection Regulation (DSGVO) and the Data Protection Amendment Act 2018 (DSG).

We hereby inform you about the processing of your personal data and the data protection claims and rights to which you are entitled. The content and scope of the particular data processing are largely based on the products and services that you have requested or that have been agreed upon with you.

1.1. Who is responsible for data processing and who can you contact?

The entity in charge of the data processing	The Data Protection Officer
Bank Winter & Co. AG, FN 124457 a, Singerstraße 10, 1010 Wien Tel.: 01/515 04-0 Fax.: 01/515 04-200 contact@bankwinter.com	**Bank Winter & Co. AG,** **Attn.: Data Protection Officer** FN 124457 a, Singerstraße 10, 1010 Wien Tel.: 01/515 04-218 Fax.: 01/515 04-200 dataprotection@bankwinter.com

2. Which data are processed and where does this data originate from?

We process the personal data we receive from you as part of the business relationship[1]. We also process data that we have legitimately received from credit agencies, debtor registers[2] or from publicly available sources[3].

Personal data includes your personal details (name address, contact details, date and place of birth, nationality etc.), credentials (such as identity card data) and authentication data (such as specimen signature). In addition, this may include order data (such as payment orders), data from the fulfillment of our contractual obligations (such as turnover data in payment transactions), information about your financial status (such as tax data, creditworthiness data, scoring or rating data), advertising and sales data, documentation data (such as consulting records), register data, image and sound data (such as video or telephone recordings), processing results generated by the bank itself, data for compliance with legal and regulatory requirements as well as other comparable data.

[1] E.g. through the account opening documentation.
[2] E.g. KSV1870 Holding AG.
[3] E.g. commercial register, register of associations, land register, media.

Your data security is our highest concern. In the context of your data processing, Bank Winter observes strict data security measures (technical and organizational measures) and protects all personally identifiable data, above all against loss, theft or unauthorized access by third parties. By means of modern encryption and access restrictions, we offer the best protection against unauthorized access to transmitted or stored information.

3. For which purposes and on what legal basis is the data processed?

Bank Winter processes your personal data in accordance with the provisions of the General Data Protection Regulation (DSGVO) and the Data Protection Amendment Act 2018 (DSG),

- For the fulfillment of (pre) contractual obligations[4]

  The processing of personal data[5] is carried out for the provision and arrangement of banking business and financial services, in particular for the execution of our contracts with you and the execution of your orders and all activities required for the operation and management of a credit and financial services institution.

  The purposes of data processing are based primarily on the specific product[6] and may include, inter alia, needs analyses, consulting, asset management and asset support, and the execution of transactions.

  The specific details for the purpose of data processing can be found in the contract documents and terms and conditions.

- For the fulfillment of legal obligations[7]

  The processing of personal data may be necessary for the purpose of fulfilling various legal obligations, in particular from the Banking Act (BWG), Financial Market Money Laundering Act (FM-GwG), Securities Supervision Act (WAG), Stock Exchange Act (BörseG), as well as regulatory requirements (e.g. of the European Central Bank, the European Banking Authority, the Austrian Financial Market Authority) to which Bank Winter is subject as an Austrian credit institution.

  Examples of legal obligations to which Bank Winter is subject (not exhaustive):

  - Identification purposes, transactions monitoring, reporting to the financial intelligence units in suspicious cases, compliance with legal sanctions
  - Monitoring of insider trading, conflict of interests and market manipulation, relaying this information to the FMA in accordance with the Securities Supervision and Stock Exchange Acts
  - Providing information to financial crime authorities in the context of financial criminal proceedings due to willful financial offence

[4] Art 6 clause 1b DSGVO.
[5] Art 4 no.1 DSGVO.
[6] E.g. Bank account, deposit, credit, securities, savings, procurements, safe deposit box rent, etc.
[7] Art 6 clause 1c DSGVO.

- Reports in the register of accounts and reports of capital outflows to federal tax authorities
- Reporting of tax-related data in accordance with Common Reporting Standard (CRS)
- Management and reporting of complaints
- Identification and reporting of fraudulent payment transactions
- Reporting of telephone calls and electronic communication in connection with investment services
- Provision of information to financial authorities, courts and public prosecutors
- Disclosure of information concerning the identity of shareholders

- For the protection of legitimate interests[8]

  If necessary, within the framework of balancing of interests in favor of Bank Winter or a third party, data may be processed beyond the actual fulfillment of the contract, in order to safeguard legitimate interests of Bank Winter or a third party. In the following cases, data is processed to safeguard legitimate interests:

  - Consultation of and data exchange with credit agencies (e.g. Austrian Credit Protection Association 1870) for the identification of credit risks and default risks;
  - Review and optimization of procedures;
  - Video surveillance for collecting proof in case of criminal offences or evidence of transactions and deposits (e.g. at ATMs); these serve especially to protect customers and employees;
  - Measures for business management and further development of services and products;
  - Measures for protecting employees and customers and the property of Bank Winter;
  - Measures for fraud prevention and combatting fraud (Fraud Transaction Monitoring);
  - In the framework of prosecution.

- Within the scope of your consent[9]

  If you have granted us consent to process your personal data, processing will only take place in accordance with the purposes set out in the declaration of consent and to the extent agreed therein. Any consent given may be revoked at any time with

[8] Art.6 clause 1f DSGVO.
[9] Art 6 clause 1a DSGVO.

future effect. The legality of previous data processing based on your consent is not affected by the revocation of your consent.

If Bank Winter intends to process your personal data for a purpose other than that for which the data was collected, Bank Winter will provide you with information for that purpose and any other relevant information prior to such processing.

4. Who receives my data?

With regard to forwarding data to other third parties, we must point out that as an Austrian credit institution, Bank Winter is obligated to comply with banking secrecy in accordance with § 38 Banking Act (BWG) and therefore to maintain confidentiality regarding all the customer related information and facts, with which we have been entrusted or made accessible to us due to the business relationship. Therefore, we can share your personal data only if you have explicitly released us from banking confidentiality in advance and in writing or if we have a legal or regulatory obligation or authorization to do so.

Your personal data may be forwarded to:

- Offices/departments/employees within Bank Winter that need the information for fulfilling (pre) contractual, legal and regulatory duties
- Companies commissioned by Bank Winter as long as they need it for fulfilling the respective services and obligations[10]. All the data processing companies are contractually obligated to keep your data confidential and to process it only in the context of service provision
- Public authorities and institutions such as the European Banking Authority, European Central Bank, Austrian Financial Market Authority, Tax Authorities, US Tax Authorities (in the framework of FATCA) if there is a legal or regulatory obligation
- Other credit and financial institutions or similar institutions to which we send data in order to maintain the business relationship with you (e.g. correspondent banks, stock exchanges, custodian banks, credit service agencies)
- Bank and Financial Auditors, provided the information is necessary for their auditing activities
- Other third parties, provided the information is necessary for the fulfillment of a contract or the fulfillment of legal regulations

A transfer to countries outside of the EU or the EEA (so-called third countries) only takes place if required to execute your orders (e.g. payment and securities orders), required by law (e.g. tax reporting obligations), you have given us consent, other suitable guarantees exist, an adequacy decision by the European Commission for the particular third country exists or, within the scope of order data processing, support from IT service providers. If

[10] In particular Accenture TiGital GmbH (IT service provider) and PSA Payment Services Austria Ltd.

services providers in third countries are used, they are obliged to comply with the written instructions and standard contractual clauses of the data protection level in Europe.

5. How long will my data be stored?

To the extent necessary, we process your personal data for the duration of the entire business relationship (from the initiation, performance until the termination of a contract) and furthermore, we process it in accordance with the legal safe-keeping and documentation obligations. These can result from, inter alia:

- the Austrian Commercial Code (§ 212 UGB, 7 years)
- the Federal Fiscal Code (§ 132 BAO, 7 years or for the duration of a tax procedure)
- the Financial Market Money Laundering Act (§21 FM-GwG, 10 years from the termination of the business relationship), or
- the Securities Supervision Act 2018 (§ 33 WAG 2018, 5 years or up to 7 years by order of the Financial Market Authority).

In addition, the statutory limitation periods which result for example from the General Civil Code (ABGB) and in some cases can last up to 30 years (the general limitation period is 3 years), must be taken into consideration for the safekeeping period.

6. Which protection rights do I have?

At any time, you have the right to obtain (1) information (whether and which of your personal data is processed), (2) to correct (correction or completion of incorrect personal data), (3) to delete or restrict processing (if processing is no longer necessary for the fulfillment of the obligation, if the data has been unlawfully processed or it is necessary due to a legal obligation), (4) the right to objection against processing (if there are particular reasons for doing so) and (5) the right to data portability according to the prerequisites of the Data Protection Law.

To exercise these rights and any complaints, please contact our data protection officer under the contact details mentioned in point 1.1

Data protection complaints can also be sent to the competent supervisory authority at the address below;

Österreichische Datenschutzbehörde
Austrian Data Protection Authority
Barichgasse 40-42
1030 Wien
Tel.: 01/ 521 52 0
dsb@dsb.gv.at

7. Am I obligated to provide data?

In the context of the business relationship, you must provide personal data which is necessary to establish and maintain the business relationship, as well as the information which we are legally required to collect. If you do not provide this information to us, in principle we must reject the conclusion of the contract and/or the performance of the order and/or will no longer be able to fulfill an existing contract and be obliged to terminate it.

8. Is there automated decision making including profiling?[11]

Bank Winter does not use automated decision-making under Art. 22 DSGVO. This means that no decision about you, the establishment or conduct of the business relationship (e.g. loans) is made purely in an automated way without any further control or decision by company employees. Should exclusively automated decision-making occur in individual cases, you will be informed about it separately and specifically.

A credit assessment (credit scoring) and/or customer rating is carried out for loans and overdrafts. The default risk of credit seekers is assessed with the help of statistical comparison groups. The calculated score should make it possible to predict how likely it is that the credit that has been applied for will be repaid. To calculate this score, your master data (e.g. marital status, number of children, duration of employment, employer, etc.), information of your overall financial situation (e.g. income, assets, monthly expenses, total liabilities, collaterals, etc.) and your payment history (e.g. proper loan repayments, warnings, information from credit service agencies) are used. If the default risk is too high, the credit application is rejected, if applicable, an entry is made in the consumer loan register maintained by KSV 1870 and an internal warning notice is received. If a credit application has been rejected, it is visible for 6 months in the consumer loan register maintained by KSV 1870 in accordance with the decision of data protection authorities.

A risk analysis is carried out for the determination of the money laundering risk. The customer's money laundering risk is calculated with the help of stored risk factors (e.g. geographical risk, product risk). The calculated value should enable a classification into different risk classes. Your master data (e.g. name, nationality, place of residence, held / desired products) are used to calculate this risk value. If the money laundering risk is too high, the business relationship with the customer may be rejected. There is no automated transfer to third parties.

9. Use of data via the website (contact form) and online banking

Personal data is only collected on our website or the online banking homepage and processed for the purpose of processing an inquiry if you have actively communicated this via the contact form provided. Indirect personal information, except for the IP address, will not be stored or processed. No cookies are used.

[11] Art. 22 DSGVO.