



General data protection information according to Art. 13 and 14 GDPR

With the following information, we would like to give you an overview of the processing of your personal data by us and your rights under data protection law. Which data is processed in detail and how it is used depends largely on the services used.

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

The responsible body is:

Oberbank AG

Untere Donaulände 28, A-4020 Linz
Phone: +43 (0732) 7802-0
E-mail: office@oberbank.at

You can contact our data protection officer at:

Oberbank AG - Data Protection Officer

Untere Donaulände 28, A-4020 Linz
Phone: +43 (0732) 7802-0
E-mail: datenschutz@oberbank.at

2. What data do we process and what sources do we use?

We process the personal data that we receive from you or from a third party commissioned by you as part of our business relationship.

In addition, we process - to the extent necessary for the provision of our services - personal data that we

- from other companies and service providers (processors pursuant to Art. 28 GDPR) in the Oberbank Group,
- from cooperation partners (e.g. Generali Versicherungs AG, Bausparkasse Wüstenrot AG, central (credit) brokers such as Deutsche Vermögensberatungs AG, EFS Euro Finanz Service Vermittlungs AG, Finanzpuls AG, INFINA Credit Broker GmbH, Intercare Finanz & Service GmbH, OVB Allfinanzvermittlungs GmbH, REALfinanz Baufinanzierungsberatung MPSZ GmbH & Co KG and Swiss Life Select Österreich GmbH),
- from address publishers and direct marketing companies pursuant to Section 151 of the German Commercial Code, from operators of information systems relevant to creditworthiness (e.g. CRIF GmbH, Kreditschutzverband von 1870 Holding AG, Creditreform Wirtschaftsauskunftei Kubicki KG, SCHUFA Holding AG),
- of court commissioners in the settlement of estates,
- of guardianship and criminal courts,
- from the Money Laundering Reporting Office (A-FIU) at the Federal Criminal Police Office and from the Banking Association (bank warnings and warnings about falsified legitimation data),
- or from publicly accessible sources (e.g. company register, land register, trade register, central register of associations, central register of residents, central credit register of the Austrian National Bank, edict file, insolvency file, media, internet)

have permissibly received.

Relevant personal data includes your personal details (name, address, contact details, date and place of birth, nationality, marital status, number of children, professional details), identification data (e.g. ID card data) and authentication data (e.g. specimen signature, U-Pad signature).



In addition, this may also include order and clearing data (e.g. payment orders), data from the fulfillment of our contractual obligations (e.g. sales data in payment transactions), creditworthiness data including data on payment behavior (e.g. warning lists of banks and small loan evidence of the credit protection association of 1870 [debtor directories] and the credit agency CRIF GmbH, scoring or rating data), insolvency data, financial identification data (e.g. credit or debit card data) or anti-money laundering and compliance data, advertising and sales data, documentation data (e.g. consultation protocol), register data, image and sound data (e.g. video or telephone recordings), data on electronic business transactions (e.g. apps, cookies, IP address) and other data comparable to the categories mentioned.

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

We process personal data in accordance with the provisions of the European Data Protection General Data Protection Regulation (GDPR) and the Data Protection Act.

- **For the fulfillment of contractual obligations (Art. 6 para. 1 lit. b GDPR)**

The processing of personal data (within the meaning of Art. 4 No. 2 GDPR) is carried out for the provision of banking transactions and financial services in the context of the performance of our contracts with you or for the implementation of pre-contractual measures that are carried out at your request. The purposes of data processing depend primarily on the specific product (e.g. account, loan, securities, deposits, building society savings, foreign exchange business, brokerage) and may include needs analyses, advice, asset management and support as well as the execution of transactions. Further details on the data processing purposes can be found in the relevant contractual documents and terms and conditions.

- **For the fulfillment of legal obligations (Art. 6 para. 1 lit. c GDPR)**

The processing of personal data may be necessary due to various legal obligations (e.g. Banking Act, Financial Markets Money Laundering Act, Securities Supervision or Stock Exchange Act, PSD2) or due to regulatory requirements (e.g. European Central Bank, European Banking Authority, Oesterreichische Nationalbank, Financial Market Authority) to which we are subject as a bank. The purposes of data processing include creditworthiness checks (credit assessment, credit scoring), identity checks, verification of beneficial ownership and payment behavior (Know Your Customer process), fraud and money laundering prevention (e.g. reports to the Money Laundering Reporting Office in certain suspected cases), the fulfillment of tax control and reporting obligations (e.g. due to the Common Reporting Standard Act, Foreign Account Tax Compliance), monitoring of insider trading, conflicts of interest and market manipulation, recording of telephone calls and electronic communication in the securities business as well as the assessment and management of risks within the Bank and the Oberbank Group and for the purpose of fulfilling legally prescribed sustainability analyses (ESG risk scoring based on the EU taxonomy, as well as the calculation of the green asset ratio and the eligibility ratio). In addition, data is processed for the purposes of accounting, controlling and compliance with tax regulations. We are also subject to the obligation to disclose information about the identity of shareholders. In certain cases, as a credit institution, we are required by law to provide information to authorities (e.g. provision of information to the FMA under the Securities Supervision and Stock Exchange Act, to financial criminal authorities in the context of financial criminal proceedings, to federal tax authorities under the Account Register and Account Inspection Act, to the public prosecutor's office under the Code of Criminal Procedure, etc.).



- **On the basis of your consent (Art. 6 para. 1 lit. a GDPR)**

If you have given us your consent to process your personal data for certain purposes (e.g. for certain advertising measures such as the Oberbank newsletter), the lawfulness of this processing is given on the basis of your consent. The scope and content of this data processing is always determined by the respective consent. You can withdraw your consent at any time with effect for the future. The withdrawal of consent does not affect the lawfulness of the data processed until the withdrawal.

- **As part of the legitimate interests (Art. 6 para. 1 lit. f GDPR)**

If necessary, we will process your data beyond the actual fulfillment of the contract to protect the legitimate interests of Oberbank AG or third parties. Examples of this are

- Consultation of and data exchange with credit agencies and debtor directories (e.g. Austrian Credit Protection Association of 1870, CRIF GmbH, Creditreform Wirtschaftsauskunftei Kubbicki KG, SCHUFA Holding AG) to determine creditworthiness and default risks;
- Testing and optimization of procedures for needs analysis and direct customer contact;
- Advertising or market and opinion research;
- Measures for business management and further development of services and products;
- Process and quality management measures (to ensure the quality of our services);
- compliance with our service standards and the efficiency of our processes);
- Assertion of legal claims and defense in legal disputes;
- Ensuring the bank's IT security and IT operations;
- Prevention and investigation of criminal offenses;
- Measures to protect customers and employees as well as the bank's property (e.g. video surveillance to safeguard domiciliary rights, to collect evidence in the event of criminal offenses or to provide evidence of transactions and deposits. Publicly accessible bank premises and ATMs operated by the controller are monitored);
- Measures for building and system security (e.g. access controls);
- Risk management measures within the Oberbank Group;
- ESG stress test and the calculation of CO2 emissions according to PCAF;

Right to object pursuant to Art. 21 GDPR

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on point (f) of Art. 6 (1) GDPR (data processing on the basis of a balancing of interests). This also applies to profiling based on this provision within the meaning of Art. 4 No. 4 GDPR. If you object, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing serves the establishment, exercise or defense of legal claims.

4. Who receives your data?

Within Oberbank AG, access to your data is granted to those departments and employees who need it to fulfill contractual, legal and regulatory obligations or on the basis of legitimate interests. In addition, service providers commissioned by us (processors pursuant to Art. 28 GDPR) will receive your data if they are required to fulfill the respective service. These are companies in the categories of credit services, IT services, logistics, printing services, telecommunications, debt collection, advice and consulting, and marketing. All processors and sales partners are contractually obliged to maintain banking secrecy and confidentiality regarding all facts of which they become aware and must treat your data confidentially. Within the group of companies, your data may be



forwarded to 3 Banken IT GmbH, Oberbank Service GmbH, 3 Banken Versicherungsmakler GmbH, Oberbank Leasing GmbH and their leasing subsidiaries (e.g. 3 Banken Kfz-Leasing GmbH, Oberbank Kfz-Leasing GmbH, Oberbank Immobilien-Leasing GmbH, Oberbank Operating Leasing GmbH and Oberbank Immobilien-Service GmbH) as well as to our EU branches for administrative reasons, for risk management due to legal or official obligations or because the processing of customer data is necessary. With regard to the transfer of data to other third parties, we inform you that, as an Austrian credit institution, we are obliged to maintain banking secrecy in accordance with § 38 of the Austrian Banking Act and are therefore obliged to maintain confidentiality regarding all customer-related information and facts that come to our knowledge in connection with our business relationship. We may therefore only pass on your personal data if you have expressly released us from banking secrecy in writing in advance or if statutory, contractual or regulatory provisions oblige and authorize us to provide information. Under these conditions, your data may be passed on to public bodies and institutions (e.g. financial market supervisory authorities, European Central Bank, financial authorities) or to other credit and financial services institutions as well as our bank and auditors or comparable institutions that we need to carry out the business relationship (depending on the contract, e.g. correspondent banks, custodian banks, stock exchanges, credit agencies) if there is a legal or official obligation to do so data from the bank's video surveillance may be transmitted to competent authorities or the court and other bodies for the purpose of law enforcement in individual cases. In addition, your personal data may be passed on to validation services such as Rundfunk und Telekom Regulierungs-GmbH in order to verify an electronic signature or electronic seal that you have transmitted. Your data may also be passed on to trust service providers (e.g. A-Trust) if we electronically sign a document that contains your data.

5. Is data transferred to a third country or to an international organization?

Data is transferred to entities in countries outside the European Union (so-called third countries) if this is necessary for the execution of your orders (e.g. payment and securities orders), is required by law, you have given us your express consent or one of the exceptions set out in Art. 44 et seq. of the GDPR is fulfilled. We will inform you separately about the details, if required by law.

6. How long will your data be stored?

We process and store your personal data for as long as is necessary to fulfill our contractual and legal obligations. It should be noted that our business relationship is a continuing obligation that is intended to last for several years. If your personal data is no longer required for the fulfillment of contractual obligations, it will be deleted regularly, unless its temporary further processing is necessary to fulfill retention periods under commercial and tax law, which result from the Austrian Commercial Code (UGB), the Federal Fiscal Code (BAO), the Banking Act (BWG), the Financial Markets Money Laundering Act (FM-GwG) and the Securities Supervision Act (WAG), among others. The retention and documentation periods specified there are five to ten years from the end of the business relationship. Retention may therefore also be necessary if you are no longer our client. In addition, the statutory limitation periods for the purpose of preserving evidence for the exercise, defense or assertion of legal claims, which, for example, according to the General Civil Code (ABGB), are usually three years, but in certain cases can also be up to 30 years, are decisive for the storage period. The bank may also have a legitimate interest in retaining your personal data. For example, data from the bank's video surveillance is deleted after 90 days at the latest if it is no longer required for the purposes pursued with the video surveillance.



7. Do you have an obligation to provide data?

As part of our business relationship, you must provide the personal data that is necessary for the establishment and execution of a business relationship and the fulfillment of the associated contractual obligations or that we are legally obliged to collect. Without this data, we will generally have to refuse to conclude the contract or execute the order or will no longer be able to perform an existing contract and may have to terminate it. In particular, we are obliged under the Financial Markets Money Laundering Act (FM-GwG) to identify you before establishing the business relationship, for example by means of your passport, and to collect your name, place of birth, date of birth, nationality and residential address. To enable us to comply with this legal obligation, you must provide us with the necessary information and documents and notify us immediately of any changes during the course of the business relationship. If you do not provide us with the necessary information and documents, we may not enter into the business relationship requested by you. However, you are not obliged to give your consent to the processing of data that is not relevant to the fulfillment of the contract or that is not required by law or regulatory requirements.

8. To what extent is there automated decision-making in individual cases?

In principle, we do not use fully automated decision-making in accordance with Art. 22 GDPR to establish and conduct the business relationship. In connection with products to be concluded online, there may be an automated rejection of the online conclusion if your details do not meet the requirements defined for the product. In these cases, please contact a customer advisor. If we use these procedures in other individual cases, we will inform you of this separately if this is required by law.

9. Does profiling take place?

We sometimes process your data automatically with the aim of evaluating certain personal aspects (profiling). We use profiling in the following cases, for example:

- Due to legal and regulatory requirements, we are obliged to combat money laundering and terrorist financing. This also involves data analysis (e.g. in payment transactions). These measures also serve to protect you.
- We use evaluation tools to provide you with targeted information and advice on products. These enable needs-based communication and advertising, including market and opinion research.
- We use scoring to assess your creditworthiness. This involves calculating the probability that a customer will meet their payment obligations in accordance with the contract. The calculation may include, for example, income, expenditure, existing liabilities, occupation, employer, length of employment, experience from the previous business relationship, contractual repayment of previous loans and information from credit reference agencies. The scoring is based on a mathematically and statistically recognized and proven procedure. The calculated score values help us to make decisions when concluding product contracts and are included in ongoing risk management.

10. Data security

We strive to ensure the highest possible level of protection and security in digital data traffic (e.g. e-mail traffic, Oberbank customer portal, Oberbank apps, etc.) and to take all necessary technical and organizational measures to ensure the security of data processing. This is primarily to protect your electronic messages, including data and information, that we receive or already have. The



aim is to be able to guarantee up-to-date, careful handling of digital data traffic based on a high level of technical protection. To this end, we also use software to detect malware that may be contained in file attachments to emails, for example. Incoming digital messages are therefore checked for malware. This serves to prevent unauthorized access to your data and information and that of the institute. These measures are also intended to ensure improved protection against malware such as computer viruses, spam and Trojans.

11. What data protection rights do you have?

Every data subject has the right of access (Art. 15 GDPR), rectification (Art. 16 GDPR), erasure (Art. 17 GDPR), restriction of processing (Art. 18 GDPR), data portability (Art. 20 GDPR), the right to object to data processing if it is based on legitimate interest, within the scope of the statutory provisions (Art. 21 GDPR) and the right not to be subject to a decision based solely on automated processing, including profiling (Art. 22 GDPR). If you address a data subject right to us, we will request proof of identity from you in cases of doubt. In this way, we can ensure that your data is not passed on to unauthorized third parties and therefore serves to protect you. You can withdraw your consent to the processing of personal data at any time. This also applies to declarations of consent that you gave us before the General Data Protection Regulation came into force. Please note that the revocation only takes effect for the future. Processing that took place before your revocation is not affected. If you believe that the processing of your personal data does not comply with data protection regulations, please contact us so that we can clarify your concerns. In addition, you have the right to submit your concerns in connection with the processing of your personal data to a supervisory authority in the EU. In Austria, the supervisory authority is the:

Austrian Data Protection Authority

Barichgasse 40-42, 1030 Vienna

Phone: +43 (01) 52152-0

E-mail: dsb@dsb.gv.at

12. Information on data protection

Current information on data protection at Oberbank AG can be accessed at any time at www.oberbank.at/datenschutz.