



Data protection information - Oberbank Customer Portal and Oberbank Apps

The following information is intended to provide you with an overview of how we process your personal data when you use the Oberbank Customer Portal or oBusiness and the Oberbank apps (Banking App, oBusiness App and Security App), as well as your rights under data protection law. General information on data protection at Oberbank can be found [here](#).

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

The responsible body is:

Oberbank AG
Untere Donaulände 28, A-4020 Linz
Telephone: +43 (0732) 7802-0
Email: office@oberbank.at

You can contact our Data Protection Officer at:

Oberbank AG – Data Protection Officer
Untere Donaulände 28, A-4020 Linz
Telephone: +43 (0732) 7802-0
Email: 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 when you set up or use the Oberbank Customer Portal, oBusiness, the Oberbank apps or the services, and that is relevant. Relevant personal data includes, for example, your personal master data (gender, title, name, date of birth, address details, contact details, account details and other information), transaction data (account movements and transactions), authentication data, identification data, device information (IP address, operating system and browser type), etc.

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 General Data Protection Regulation (GDPR) and the Data Protection Act.

3.1. To fulfil contractual obligations (Art. 6(1)(b) GDPR)

Your personal data is processed for the purpose of performing our contracts with you and executing your orders, as well as for carrying out pre-contractual measures. You can find the specific details regarding the purpose of the data processing listed here in the relevant contractual documents and terms and conditions (e.g. Internet banking agreement for the Oberbank Customer Portal and Oberbank App).

3.1.1. Oberbank Customer Portal

If you have an Oberbank Customer Portal (Internet banking), we process your data in connection with the services you have requested (e.g. eBanking, electronic mailbox, eShop, etc.).

3.1.2. Oberbank Banking App

If you have an Oberbank Customer Portal (Internet banking) and download the Banking App to your smartphone running the iOS or Android operating system, we process your data within the scope of the services you have requested (e.g. Financial Manager).

3.1.3. Security App

If you have access to the Oberbank customer portal (online banking) or the Banking App, you can download and use the Security App. In doing so, we process your data for the purposes of customer authentication (e.g.



for changing personal details, adjusting limits, or concluding contracts in the eShop). When activated, the Oberbank Security App requires information from your phone's status to connect with the Oberbank Internet Banking user.

3.1.4. oBusiness

If you are a business customer with an oBusiness account, we process your data in connection with the services you have requested (e.g. payments).

3.1.5. oBusiness App

If you are a business customer with oBusiness access and download the Business App onto your smartphone or tablet running the iOS or Android operating system, we process your data in connection with the services you have requested (e.g. signing/authorising orders previously entered in oBusiness).

3.2. To comply with legal requirements (Art. 6(1)(c) GDPR)

The processing of personal data may be necessary due to various legal or regulatory requirements to which we, as a bank, are subject (e.g. under the Banking Act or the Financial Market Money Laundering Act, the Securities Supervision Act or the Stock Exchange Act). Please refer to our [general data protection information](#) for further details. Pursuant to Section 87(1) of the Payment Services Act (ZaDiG), certain services available in the customer portal or the banking app (e.g. (two-factor) authentication when accessing the payment account, authorisation of transactions, authorisation when viewing older account transactions) require strong customer authentication, which is carried out via the Security App.

3.3. On the basis of your consent (Art. 6(1)(a) GDPR)

Where you have given us your consent to process your personal data for specific purposes, the lawfulness of this processing is based on your consent. The scope and content of this data processing are always determined by the relevant consent. Your consent is voluntary and may be withdrawn at any time with effect for the future.

3.4. On the basis of a balancing of interests (Art. 6(1)(f) GDPR)

Where necessary, we will process your data (e.g. IP address, date and time of access, user ID) beyond the actual performance of the contract to safeguard the legitimate interests of Oberbank AG or third parties. Examples of this include:

- Measures for the further development of services and products
- Measures for process and quality management
- Ensuring IT security / system security and fault analysis
- Prevention of fraudulent or abusive behaviour
- Enquiry/complaint management, including in relation to the submission of reviews

Right to object under Article 21 of the GDPR

You have the right to object at any time, on grounds relating to your particular situation, to the processing of personal data concerning you which is carried out on the basis of Article 6(1)(f) GDPR (data processing based on a balancing of interests). 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 to establish, exercise or defend legal claims.

4. Who receives your data?

Within Oberbank AG, those departments and employees who require your data to fulfil contractual, legal and regulatory obligations, or on the basis of legitimate interests, will have access to it. In addition, service providers commissioned by us (processors under Article 28 of the GDPR) will receive your data, provided that this is



necessary for the performance of the respective service. These include, for example, companies in the categories of IT services, telecommunications and marketing, as well as data storage in secure data centres.

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

Data is transferred to entities in countries outside the European Union (so-called third countries) insofar as this is necessary to execute 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 Articles 44 et seq. of the GDPR applies. We will inform you separately of the details, where 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 fulfil our contractual and legal obligations. Once your personal data is no longer required, it is regularly deleted, unless its continued processing for a limited period is necessary to comply with commercial and tax law retention periods. The prescribed retention and documentation periods are five to ten years from the end of the business relationship. Retention may therefore also be necessary even if you are no longer our customer. Furthermore, the statutory limitation periods for the purpose of preserving evidence for the exercise, defence or assertion of legal claims are decisive for the storage period; these are generally three years under the General Civil Code (ABGB), but may in certain cases extend up to 30 years.

7. Are you obliged to provide data?

Within the framework of our business relationship, you must provide the personal data necessary for the establishment and conduct of a business relationship and the fulfilment of the associated contractual obligations, or which 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. Should you fail to provide us with the necessary information and documents, we will not be able to enter into the business relationship you have requested. However, you are not obliged to give your consent to the processing of data that is not relevant to the performance of the contract or is not required by law or regulatory authorities.

8. To what extent is automated decision-making or profiling used in individual cases?

No automated decision-making, including profiling, takes place within the Oberbank customer portal, oBusiness or the Oberbank banking apps in accordance with Article 22 of the GDPR. Should we use these procedures in other individual cases, we will inform you of this separately.

In connection with products to be taken out online, the credit assessment or our lending guidelines may result in an automated rejection of the online application if your details do not meet the requirements defined for the product. You have the right to request that Oberbank carry out a manual review of the automated decision by Oberbank staff, to present your own point of view, and to challenge the automated decision.

If profiling is to be carried out for other purposes, we require your separate and explicit consent (which may be withdrawn at any time). Your personal data will not be used for other purposes without your prior explicit consent.

9. Data security

We strive to ensure the highest possible level of protection and security in digital data traffic and to take all necessary technical and organisational measures to guarantee the security of data processing. This is primarily to protect the electronic messages, including data and information, that we receive and those already in our possession. The aim is to ensure that digital data traffic is handled in a modern, careful manner and in accordance with a high standard of technical protection.



10. What data protection rights do you have?

Every data subject has the right to 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 (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 exercise a data subject right with us, we may ask you to provide proof of identity in cases of doubt. This enables us to ensure that your data is not disclosed to unauthorised third parties and therefore serves to protect you. You may withdraw your consent to the processing of personal data at any time. This also applies to declarations of consent that you provided to us prior to the General Data Protection Regulation coming into force. Please note that the withdrawal only takes effect for the future. Processing carried out prior to your withdrawal 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 address your concerns. Furthermore, you have the right to raise your concerns regarding the processing of your personal data with a supervisory authority in the EU. In Austria, the supervisory authority is:

Austrian Data Protection Authority

Barichgasse 40–42, 1030 Vienna

Telephone: +43 (01) 52152-0

Email: dsb@dsb.gv.at

11. Information on data protection

Up-to-date information on data protection at Oberbank AG is available at any time at www.oberbank.at/datenschutz.