BENKER UAB

DATA PRIVACY POLICY

Version 3.1

Release date: 10.10.2024

Like most website operators, Benker (GDPR Data Recipient and Controller) collects data about visitors to our Website at benker.io (Website) and our mobile application. This helps us understand how useful the Website and the application are and how to improve them. We also process personal data (i.e.: to send newsletters and analyse interest in our services). Our data collection practices are governed by this Data Privacy Policy (Policy), which tells you what data we collect, how we use that data and who has access to that data.

You will also find important information about your privacy rights, so please read the Policy carefully.

We respect your privacy, protect and process your Personal data in accordance with the rules of Regulation (EU) 2016/679 of the European Parliament and of Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)), Law on Legal Protection of Personal Data of Republic of Lithuania and other applicable regulatory enactments.

This Policy may at any time be amended if the scope of processing or our processing practices change. You are required to acquaint yourself with the Policy every time it is updated.

Data Controller:

BENKER UAB, company code 305084126, address Lvivo g. 25-702, LT-09320 Vilnius, Lithuania. (Benker, we or us) is the controller of your personal data. The Controller operates as electronic money institution (E-Money institution) under Electronic Money Institution (EMI) licence Nr. 91. issued and regulated by the Bank of Lithuania. You can contact us by email at *hello@benker.io.*

1. INFORMATION WE COLLECT AND HOW WE USE IT

In this Policy, “personal data” is defined as any information relating to an identified or identifiable natural person.

1.1. Newsletters

When you register at our Website to receive our newsletter, we collect your name, country of residence, and e-mail address. We process this data for the purposes of sending you correspondence with information about Benker, our services, related news and other information that we consider may be of interest to you. We also use the collected data to analyse interest in our services based on demographical and geographical attributes.

Legal basis to collect and process this personal data is your consent.

1.2. Inquiries and answers

When you contact us with an enquiry via the contacts available at our Website we will process your contact details and content of your message to respond to your enquiry.

Legal basis to collect and process this personal data is our legitimate interest to respond to enquiries about us and our services.

1.3. Cookies

When you browse our Website, we collect and process certain personal data via use of cookies.

Please read our Cookie Policy for additional information here:
http://data.benker.io/cookiepolicy.pdf

1.4. Enhanced Due Diligence

In cases specified in BENKER's AML policy's “Application of enhanced due diligence” section, BENKER shall perform enhanced due diligence on Customer, where additional information is obtained by BENKER, such as, but not limited to the following:

- information about the Customer and the Beneficiary;
- information about the proposed nature of the business relationship;
- information about the sources of funds and the sources of wealth of the Customer and the Beneficiary;
- information about the causes of any planned or executed monetary operations or transactions.

1.5. Mobile application and Web client

Information while signing up:

- personal details: your name, birth details (date, place, name, mother name);
- contact details: your home address, email address and phone number;
- identification document: type of document, issue date, document number and issuing country;
- photograph.

Information from mobile application usage:

- details about payments to and from your BENKER account.

Information about the mobile device:

- technical information: device type, device name, IP address, device ID and operating system, so we can analyse how our app works and fix any problems.

2. WHO MAY SEE YOUR DATA

We put our best efforts to keep your data safe and always require the highest level of security and confidentiality from our employees, partners and group companies, which are subjects which we may share your data with.

We may share your personal data with our trusted services providers when they provide services to us or to you on behalf of us and under our instructions. This may include, for example, providers of IT solutions and cloud services. We will control and shall remain responsible for the use of your personal data at all times.

Your personal data may be disclosed to public authorities if we are required to disclose personal data by law or to comply with a lawful request of authorities.

If we are ever involved in a corporate transaction, for example if our shares are bought by third parties, we may transfer your personal data to investors or potential investors, as well as other recipients involved in the relevant transaction.

3. HOW LONG WE KEEP YOUR DATA

Your personal data collected when you register to receive newsletter will be processed until you withdraw your consent (unsubscribe).

Personal data related to your inquiries will be stored for up to 2 years.

In order to properly provide financial services, your personal data is stored for a longer period of time in accordance with the requirements of applicable legal acts as well as if personal data needs to be stored to protect our legitimate interests or those of any third parties, e.g. in the event of a legal dispute. The term of storage of Your personal data may be additionally extended for up to 2 years upon a reasoned instruction of a competent authority.

Our most common time limits for the storage of Your personal data are listed below:

- personal data necessary for the provision of Our services to You/Your represented legal entity and fulfilment of our commitments and obligations arising out of our GTC for the Provision of services we will keep all for all the period of business relationships with You and for the below indicated periods from their termination;
- copies of client identity verification documents, beneficial ownership identification data, direct video transmission (live video broadcast records), other information obtained during verification of client identity will be retained for at least 8 years from the date of business relationship termination (according to the applicable legislation, storage time may be extended for further period on reasonable order from competent authority, however not exceeding 2 years);
- business communication with a client (including correspondence and recordings of phone conversations) will be retained for at least 5 years since the termination of business relationship, if is related to the fulfilment of money laundering and terrorist financing prevention requirements. (according to the applicable legislation, storage time may be extended for further period on reasonable order from competent authority, however not exceeding 2 years). However, if there is a justified need to retain a specific recording for a longer period, this may be reviewed by the director in conjunction with the ***Data Protection Officer*** (***DPO***);

- documents and data confirming/justifying validity of monetary operations and transactions, other legally valid and relevant information/documentation will be retained for at least 8 years since the execution of monetary operation or conclusion of the transaction (according to the applicable legislation, storage time may be extended for further period on reasonable order from competent authority, however not exceeding 2 years);
- for data to prove the fulfilment of our obligations we will keep the general limitation period for the requirement, in accordance with the regulatory enactments for limitation periods of claims, for example, depending on the specific circumstances of the situation, may be applied a limitation period of 10 years established in the Civil Code of the Republic of Lithuania, also taking into account the time limits for submitting claims, set out in the Code of Civil Procedure of the Republic of Lithuania;
- video surveillance records, other than those listed above, will be retained 30 days from the date from recording thereof (video surveillance records, in case certain data is issued to investigation bodies/officers and used for investigation of an offensive action according to the procedure of the applicable law, may be stored for longer period, specified by the relevant regulatory enactments).

Personal data related to application usage may be stored. We continuously process the data from the conclusion of the contract to the termination of the contract.

We store the data during the contract and 1 year after the termination thereof. More can be found in BENKER's GTC.

See Cookie Policy to find out how long cookies are stored on your device.

4. WHERE WE KEEP YOUR DATA

We only store personal data on our own servers, which we have built in ***AMAZON AWS***.

Our organization is committed to ensuring the proper protection of personal data, therefore we only store data on servers operated in EEA countries.

5. THIRD PARTY SERVICE PROVIDERS AS DATA PROCESSORS

To ensure the highest level of financial service and to meet regulatory requirements, the following listed activities are provided to our clients by providing services provided by market participants who can guarantee adequate security for the high quality of the financial service, so that appropriate security measures are also in place for the processing of personal data.

We work with the following service providers:

TPL - Our BIN Sponsor

IDENFY - Our KYC service provider

TRIBE - Our Open Banking Service provider

THALES - Our CARD Producer

SEON - Our transaction monitoring and fraud detection provider

AMAZON - Our cloud computing service provider

MONGODB - Our database service provider

BRANCH - Our deep linking service provider

F**IREBASE** - Our crash analytics service provider

IBAN.COM - Our IBAN validation and calculation service provider

JIRA - Our software development tool service provider

Our contracted partners receive the customer data only to the extent and for the time necessary for the tasks, based on which the activity, service or product included in the contract is provided to our customers. The personal data of our customers will not be transferred for any other purpose, and we expect this from our contracted partners as well.

6. YOUR RIGHTS

By contacting us at *hello@benker.io* you may exercise your rights as the data subject, including the following:

- the right to request access to your personal data. You may access, correct, update, change or remove your personal data at any time. However, please note that certain information is strictly necessary in order to fulfil the purposes defined in this Policy and may also be required by law. Thus, you may not remove such personal data;
- the right to request rectification of your personal data;
- the right to request erasure of your personal data. If personal data is erased under your request, we will only retain such copies of the information as are necessary for us to protect our or third parties' legitimate interests, comply with governmental orders, resolve disputes, troubleshoot problems, or enforce any agreement you have entered into with us;
- the right to withdraw consent regarding processing of personal data;
- the right to data portability.

In some cases, you may have a right to request restriction of processing of your personal data or to object to processing of your personal data. If you think there is a problem with the way we are handling your personal data, you have a right to file in a complaint with the Lithuanian State Data Protection Inspectorate **(https://vdai.lrv.lt/en/).**

Data Protection Officer:

email address: dpo@benker.io

phone number: +36 70 6287426

Vilnius, 10.10.2024