Privacy Policy

Effective date: 25/11/2020
Last updated: 10/11/2021

This Privacy policy is addressed to private individuals (natural persons) who visit our website and/or use our services and explains the information on the processing of their personal data (hereinafter will be addressed as you/your).

This Privacy policy describes how we collect, use, process, and disclose your information, including personal information, relating to your access to and use of Finci UAB (Finci) services. Please read it carefully as this policy is legally binding on you when you use Finci services. If you do not agree with this Privacy policy, you should immediately refrain from using our website and/or application and/or services.

We may collect and process your individually identifiable information, namely information that identifies a person or can, with reasonable efforts, identify a person (hereinafter – "**Personal data**") in order to provide proper services for you.

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 the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter – "**GDPR**"), Law on Legal Protection of Personal Data of the Republic of Lithuania and other applicable regulatory enactments.

We reserve the right to update, change or replace any part of this Privacy policy by posting updates and/or amendments and/or alterations to our website, updating the "Last Updated" date at the top of this Privacy policy. It is your responsibility to check this page periodically for changes. If you continue to use and/or access the website following the posting of any changes, this automatically constitutes acceptance of those changes. In the event you disagree with any amendment and/or alteration and/or update you shall immediately terminate the use of our website and/or services.

1. DETAILS OF THE CONTROLLER

The Controller and owner of the website **www.finci.com** is Finci UAB, registration number: 304934066, registered office: Mėnulio str. 11-101, LT-04326 Vilnius, Republic of Lithuania. The Controller operates as electronic money institution (E-Money institution) under Electronic Money Institution (EMI) license Nr. 60, issued and regulated by the Bank of Lithuania.
You can contact us by phone: **+370 691 106 93** or by writing to the following e-mail address: **info@finci.com**.

2. CONTACT DETAILS FOR COMMUNICATION ON PERSONAL DATA PROTECTION ISSUES

If you have any questions relating to this Privacy policy or processing of your Personal data, you may contact us by using the communication channels listed in the previous paragraph (paragraph 1) or by contacting our personal data protection officer by writing to the following e-mail address: **dpo@finci.com**.

3. THE PURPOSES AND LEGAL JUSTIFICATION OF PERSONAL DATA PROCESSING

We collect and process your Personal data only for legitimate purposes in accordance with the rules of data protection and processing established by GDPR and other applicable rules.
As a regulated EMI, we are obliged to comply with the legal obligations provided by the following legal regulations (but not limited): the Law on Payments of the Republic of Lithuania, the Law on Electronic Money and Electronic Money Institutions of the Republic of Lithuania, Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (hereinafter – "Regulation (EU) 2015/847") and the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania Money Laundering and Terrorist Financing Prevention legislation (hereinafter – "**Applicable legislation**").

We shall also comply with local and international anti-money laundering (hereinafter – "**AML**") and counter-terrorist financing ("**CTF**") obligations, as well as to implement know your customer (hereinafter – "**KYC**") requirements. We will only process your Personal data for lawful purposes defined in this Privacy Policy (please see further points 3.1 to 3.6).

While processing your Personal data we will comply with GDPR and other Personal data protection applicable laws and regulatory enactments, as well as with data processing principles, which means that your Personal data will be:

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- Relevant to the purposes we have informed you about and limited only to those purposes;
- Accurate and kept up to date;
- Maintained only for as long as necessary for the purposes we have informed you about;
- Kept securely and protected against unauthorized or unlawful processing and against loss or destruction using appropriate technical and organizational measures.

3.1. The commencement and provision of services - electronic money issuance, redemption, payment services, currency conversion, cards issuing and payment processing services - and for the fulfilment of obligations under the services agreement:

As part of this, we will process the following Personal data: name, surname, personal identification number, tax identification number, address, date of birth, data from an identity document/residence permit and a copy of the identity document/residence permit , photo, direct video transmission (live video broadcast records) recording, citizenship, email address, phone number, payment account number, bank statements, pay slips, employment agreements, contracts, invoices, employment history, IP address, current activity, current public function, information about main business partners (and their Personal data), source of funds and wealth, data from a power of attorney, information on transactions and other data required by the Applicable legislation.

Below you can find the details and additional information why, for what sub-purposes and/or what data for certain sub-purpose (where explained) we will process.

We will process your Personal data to:

- identify you as a prospective client and/or client's – legal entity's director/legal representative/management board/supervisory board member/ authorized person or employee, and implement relevant "Know your customer" procedures;
- to understand your financial circumstances;
- identify ultimate beneficial owner or controlling person of the account;
- collect information regarding client's main business partner;

- verify your mobile number and e-mail address;
- conclude an agreement (General Terms and Conditions for the Provision of services) for services with you/your represented legal entity;
- open an account to you/your represented legal entity and provide you with our services;
- if you are already a Finci client, we use your personal data to meet our obligations relating to any transactions you make (for example, making payments into and out of your Finci account, making payments with your Finci payment card);
- to communicate with you, if you contact us or we contact you (including correspondence and records of phone calls).

Within the client onboarding process, in addition to Personal data processing for the purposes of client identification and contact details verification, in compliance with the requirements of AML and KYC, we will use document authenticity verification services provided by external vendor, including validation of KYC documentation, business documentation required for legal entity onboarding, verification of beneficial ownership and information checking in national registers of Member States as required by the Applicable legislation. We will use vendor's overnight screening services for potential sanctions and politically exposed person (PEP) matches, negative information in adverse media.

If you are indicated as the beneficial owner or a controlling person of a legal client, we shall process the following your Personal data: name, surname, date of birth, residency/nationality, identification document's/residence permit's data, nature and description of the beneficial ownership, source of funds and wealth (where required) and other data required by the Applicable legislation.

If you are indicated as the client's main business partner we may process the following your Personal data: name, surname, date of birth, citizenship, invoices, data revealing business relationship between you and the client and other Personal data according to the Applicable legislation.

- process your/legal entity's payment orders and execute payment transactions;
- process electronic money issuance and remittance;
- process currency exchange transactions;

As part of transaction processing we will process your identification data and your payment account data, payment transaction data, payment recipients Personal data (name, surname, account number and the recipient bank details), IP address, other data required by the Applicable legislation;

- handle necessary procedures according to anti-money laundering and terrorist financing regulations;
- make relevant risk assessments;
- monitor transactions;
- ensure proper risk and organizational management;
- keep contact and necessary communication with you;
- process client's requests and complaints, where relevant.

In order to communicate with you and process the requests and complaints received from you in accordance with the General Terms and Conditions for the Provision of services, where relevant, we may process the following your Personal data: name, surname, position/representation rights, e-mail address, telephone number and other Personal data that is indicated in your requests/complaints.

In order to fulfil our Contractual obligations, ensure the best quality of services and resolve disputes, we have a right to collect evidence about business communication with the clients (correspondence, recordings of conversations).

If your employer uses Finci Business and nominates you as a Finci cardholder and/or account user, your employer will provide us with information about you. This will also include your identification taken by Finci.

If your employer nominates you as a Finci cardholder, we will also get information about any transactions you make with your Finci Business payment card.

The main legal grounds of Personal data processing for the above mentioned purposes are:

1) your consent to the personal data processing (Article 6 (a) of GDPR) and (Article 9 (2) (a) of GDPR, in case in your identification process we get any of special categories of your Personal data, e.g., identification via "liveness check" - direct video transmission (live video broadcast records);

2) conclusion and performance of the contract with data subjects (Article 6 (b) of GDPR);

3) fulfilment of legal obligations under Applicable legislation (Article 6 (c) of GDPR);

4) legitimate interests of the controller (Article 6 (f) of GDPR), such as identifying you as a client and/or client's representative/beneficial owner/controlling person, ensuring contact with you and best quality of service.

3.2. AML/CTF and transaction monitoring

As part of this, we would need to comply with AML/CTF legal framework, establish your/your represented legal entity's client risk classification, monitor transactions, carry out risk score and AML/CTF risk exposure assessment.

For the implementation of our legitimate interest within the AML/CTF framework we may verify information relating to you against credible publicly available information sources; ensure monitoring of your transaction and provide information to the supervisory authorities and investigative authorities in the cases provided by legal enactments, ensure the maintenance of relevant registers, e.g., risk register, beneficial owners' register.

As a regulated entity, we are obliged to conduct retrospective monitoring of clients' activities. In order to fulfil these obligations, additional information request for Personal data may be sent to verify information required by Applicable legislation. While monitoring payment transactions, we may also require to provide us the documents confirming economic substance/legitimacy of the transaction, that might also contain Personal data.

The legal ground of Personal data processing for this purpose is:

1) fulfilment of legal obligations under Applicable legislation (Article 6 (c) of GDPR);

2) legitimate interests of the controller (Article 6 (f) of GDPR), such as identifying you as a client and/or client's beneficiary, ensuring contact with you.

3.3. Providing marketing activities and/or informing you on our services

As part of this we may send you commercial communications to e-mail according to your consent or our legal relationships (agreement) with you. If you subscribe for our newsletters or you are our existing client/client's representative/contact person, we may send you information and offers/special offers regarding our products and services that might interest you. We may also

provide you with information about other goods and services we offer that are similar to those you have already used or asked for. We may also provide you with (push) notifications of our new products and offers via our applications if you are using them, if you have subscribed to them.

If you are not willing to receive our commercial communications, you can inform us and refuse the further receipt of commercial communications any time, we also providing you free of charge and easy-to-implement opportunity to unsubscribe in our commercial communication sent to you by e-mail. If you don't want to further receive push notifications via our applications, you can manage user preferences by switching off this option.

For this purpose, we might need at least the following personal data: your name, surname, data of legal entity you represent, e-mail address, location, services and products you have used or asked for or looked for in our applications and other user experience data.

The legal grounds of Personal data processing for this purpose are:

1) your consent to the Personal data processing (Article 6 (a) of GDPR);

2) conclusion and performance of the contract with data subject (Article 6 (b) of GDPR);

3) legitimate interests of the controller (Article 6 (f) of GDPR), such as informing you about our services, sending you information on our special offers/products etc.

3.4. Prevention of security threats to property interests and other essential legitimate interests of the Controller or of third parties

As part of this, we should carry out video surveillance of our territory, buildings and other property, make telephone records, use personal data processors to provide a variety of functions, if necessary, to disclose information to supervisory authorities, judicial bodies, agencies, courts and other public authorities or officials, to exercise the rights conferred by law to ensure other legitimate interests of the Controller or third parties.

For this purpose, we might need to process at least the following Personal data: client's/visitor's appearance (image), name, surname (if possible), object address, location and time, and other data as necessary.

The legal ground for the processing of Personal data for this purpose is:

1) legitimate interests of the Controller (Article 6 (f) of GDPR).

3.5. Ensuring proper supply of our services

As part of this, we would need to carry out the maintenance and development of our websites, technical systems and IT infrastructure, technical and organizational solutions that can also use your Personal data (for example, by watching cookies), with a view to ensure providing of proper services to you. Regarding our use of cookies, please read also our Cookies policy.

The legal ground for the processing of Personal data for this purpose is:

2) legitimate interests of the Controller (Article 6 (f) of GDPR).

We shall take appropriate measures to process your personal data in accordance with the Applicable legislation and to ensure that your Personal data is not accessed by third parties who do not have the appropriate legal basis for the processing of your Personal data.

4. THE SOURCES OF OBTAINING YOUR PERSONAL DATA

We can get your personal data in one of the following ways:

- from you, visiting our website, applications and/or subscribing to our services;
- from you, providing your Personal data for identification and KYC purposes via our website and/or applications;
- from you, in the process of entering into a mutual agreement with us;
- from you, if you submit any requests, complaints, e-mails, or call us;
- from you, when you are using our products/services;
- from our clients, if they make payments to you or indicate you as a payment recipient, business partner, relative and other;
- from legal entities, where you are related to such legal entities in any manner, e.g., employee, representative, contact person, authorized person, cardholder, beneficial owner, contractor, shareholder, participant and other relations to such legal entities;
- from other legal entities or natural persons in the process of fulfilling contractual or legal requirements and documents provided to us, e.g., contracts, property valuation reports and other documents;
- from other financial institutions, e.g., banks, payment institutions etc.;
- from our partners, e.g., identification vendors;
- from third-party registers as required by Applicable legislation or according to our legitimate interests;
- from State institutions and registers, e.g., the Bank of Lithuania, the Ministry of Finance, the State Enterprise Centre of Registers, law enforcement institutions, other registers and public authorities;
- from bailiffs in accordance with the requirements of debt property information and suspension of assets if relevant court decision was made;
- where applicable, from video surveillance records.

5. WHY DO YOU HAVE TO GIVE US YOUR PERSONAL DATA?

Above all, we are collecting your information to fulfil the commitments under the General Terms and Conditions for the Provision of services entered with you, to fulfil the legal obligations that are binding on us, and to pursue our legitimate interests. In these cases, it is necessary for us to obtain certain information for the purposes involved, so that failure to provide such information may endanger the commencement of or provision of services to you. If the data are not required, but their submission could help to improve our services provided to you, we will indicate that the provision of data is voluntary.

6. THE RECEIPIENTS/POSSIBLE RECEIPIENTS OF YOUR PERSONAL DATA

Your Personal data could be accessed as needed by and shared with:

- our employees or directly authorized persons who are required to process this Personal data to perform their duties;
- Personal data processors;
- Third parties, carefully assessing whether such Persona data transfer has an appropriate legal basis.

Your Personal data could be accessed as needed by and shared with:

Your Personal data will be transmitted to third parties that we use to provide our services; these parties have been rigorously assessed and offer a guarantee of compliance with the legislation on the processing of Personal data. These parties have been designated as data processors and carry out their activities according to the written agreement, the instructions given by us and under our control.

We may work with the following categories of Personal data processors:

- outsourcing accountants, auditors, financial management and legal advisers;
- Internet/computer software services providers, companies specializing in IT and marketing services;
- IT infrastructure services providers;
- Helpdesk services providers;
- Companies that carry out KYC/AML database checks and fraud database checks;
- Customer support services providers;
- Global financial messaging infrastructure services providers (eg., SWIFT, Ripple);
- Global payment systems (e.g. Visa, MasterCard);
- Video surveillance/security services provider/s;
- Other persons connected with the provision of our services.

Personal data processors may change from time to time, so we may also make relevant changes to this Privacy policy.

Third parties:

We may also be required to share your Personal data with various financial institutions, payment services providers and/or law enforcement bodies and officials, supervisory authorities/regulatory bodies and financial crime investigation service to comply with Applicable legislation, prevent fraud or enforce an agreement we have with you;

We may also share your personal data to comply with applicable laws and regulations, to respond to a legal requests of law enforcement bodies and officials, supervisory authorities/regulatory bodies, or to other third parties if it is provided by applicable law, and/or if it is relevant for the protection of our and our employees legitimate interests, property or safety, or legitimate interests of third parties or data subject.

7. TERMS OF PERSONAL DATA RETENTION/STORAGE

Your Personal data is stored for as long as their storage is required for appropriate purposes for the processing of Personal data, as well as in accordance with the Applicable legislation.

Data may be stored in an electronic form and/or in paper format, provided always that your Personal data will be stored securely and protected against unauthorized or unlawful processing and against loss or destruction, using appropriate technical and organizational measures.

When assessing the length of the storage of Personal data, we take into account existing regulatory requirements, aspects of contractual performance, your instructions (e.g. in the case of consent), and our legitimate interests. If your Personal data is no longer needed for the purposes specified, we will delete them or destroy them.

Below, we indicate the most common time limits for the storage of your Personal data:

- Personal data necessary for the provision of our services to you/your represented legal entity and

fulfillment of our commitments and obligations arising out of General Terms and Conditions 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 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 fulfillment of money laundering and terrorist financing prevention requirements. (according to 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 CEO in conjunction with the Data Protection Officer;
- 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 execution of monetary operation or conclusion of the transaction (according to Applicable legislation, storage time may be extended for further period on reasonable order from competent authority, however not exceeding 2 years);
- 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, taking into account also the time limits set out in the Civil Procedure Law for submitting claims;
- Video surveillance records will be retained 30 (thirty) days from the date when it is recorded (video surveillance record, in case certain data is issued to investigation bodies/officers and used for investigation of an offensive action according to the procedure of applicable law, may be stored for longer period, specified by the relevant regulatory enactments).

8. YOUR PERSONAL DATA TRANSFER TO COUNTRIES OUTSIDE THE EUROPEAN UNION (EU) OR THE EUROPEAN ECONOMIC AREA (EEA)

Usually, we do not transfer your Personal data to countries outside the European Union or the European Economic Area. However, if we need to transfer your Personal data to third countries in the meaning of GDPR for the purposes related to provision of our services or protection of our legitimate interests, we will do that in strict compliance with GDPR rules.

For instance, your Personal Data may be provided to third countries in the meaning of GDPR in those cases, when your payment transfer is carried out to a third country, or a partner (correspondent) from a third country is engaged in the payment execution.

All Personal data sharing events are controlled under strict data sharing agreements with relevant parties in order to maintain correspondent banking relationships and provide smooth services under agreement.

We may also send your information to third countries in the meaning of GDPR to keep to global legal and regulatory requirements and to provide ongoing support services.

9. PROFILING AND AUTOMATED DECISION-MAKING

Profiling carried out by us involves processing of Personal data by automated means for the purposes of legislation relating to risk management and continuous and periodic monitoring of transactions in order to prevent fraud, money-laundering and terrorist financing events. However, we do not make automatic decisions based on profiling.

For the purpose of direct marketing and statistical analysis, profiling may be carried out by using Google, Facebook and other analytics tools.

The main legal grounds of Personal data processing for these purposes are:

1) conclusion and performance of the contract with data subject (Article 6 (b) of GDPR);
2) fulfilment of legal obligations (Article 6 (c) of GDPR), e.g., Applicable legislation.
3) legitimate interests of the controller (Article 6 (f) of GDPR), such as managing risks related with the Client and its transactions, AML/CTF purposes.

10. YOUR RIGHTS AS DATA SUBJECT

Restoring your personal data:

If there are changes to Personal data that you have provided to us, please contact us at e-mail **info@finci.com** and provide us with the relevant data so that we can achieve the relevant Personal data processing purposes.

Your right to access and correct your Personal data:

In accordance with the provisions of the GDPR, you have the right to require us to have access to your Personal data at our disposal, to request their rectification, erasure, processing limitation, to object to the processing of your Personal data, as well as the right to data portability in the cases and procedures set out in the GDPR.

We respect your right to access and control your Personal data, so if we receive your request, we will respond to it within the time limits laid down in the regulatory framework (usually not later than one month if there is no specific request that takes longer to prepare the answer), and if it is possible, we will correct or delete your Personal data accordingly, or undertake the necessary measures to enable your Personal data portability as possible.

You may obtain information about your Personal data or exercise other rights as a data subject in one of the following ways:

- by submitting an appropriate application in person and identifying yourself at our office at the address: Mėnulio str. 11-101, LT-04326 Vilnius, Republic of Lithuania, each working day from 10-16;
- by submitting an appropriate application to us by post to the following address: Mėnulio str. 11-101, LT-04326 Vilnius, Republic of Lithuania;
- by submitting an appropriate application to us by e-mail: info@finci.com ; it is recommended that you sign it with a qualified electronic signature when submitting a relevant application, sending it via e-mail.

Upon receipt of your submission, we will evaluate the content and the possibility of identifying you, and, depending on the situation, we reserve the possibility of asking you to further identify yourself in order to ensure the security and disclosure of your Personal data to the person concerned.

Withdrawal of consent

If the processing of your Personal data is based on your consent, you have the right to withdraw it at any time and we will no longer process your Personal data processed on the basis of your consent. However, please be informed that the withdrawal of consent cannot affect the processing of Personal data which is necessary for the fulfilment of the requirements of regulatory enactments or which is

based on a contract, our legitimate interests or other legal bases for the lawful processing of Personal data provided for in regulatory enactments.

11. RIGHTS COMPLAINTS REGARDING YOUR PERSONAL DATA PROCESSING

If you have any questions or concerns regarding our processing of your Personal data, we encourage you to contact us first.

If you still want to submit the complaint, you can do it in following ways:

a. by filling in Finci's complaint form and sending it via online banking message; or
b. via e-mail **talk@finci.com** sending filled in and signed with a qualified electronic signature Finci's complaint form.

A complaint form can be found on the Finci's website in the section "Legal documents". When submitting a complaint, you must properly fill in relevant fields provided in the complaint form. If at least one of the appropriate fields are not filled in or not fully filled in, Finci shall have the right to request to supplement the complaint and/or submit relevant annexes to it.

The complaint and its annexes (if any) must be either in the Lithuanian or English language. If the complaint and/or its annexes are in other languages, Finci has the right to request the complaint and/or documents to be translated into the Lithuanian or English language. The translation into Lithuanian or English must be certified by the translation office and/or the translator's signature, which must be certified by a notary public.

If, however, you believe that we have not been able to resolve the issue with each other and you believe that we are nevertheless in violation of your right to the protection of Personal data, you have the right to lodge a complaint with the Lithuanian State Data Protection Inspectorate (**https://vdai.lrv.lt/en/**).