Effective date: 25/11/2020
Last updated: 28/07/2025

This Privacy policy (hereinafter – Privacy policy) is addressed to private individuals (natural persons) who visit our websites (hereinafter – Web) and/or applications (hereinafter – App) operated by us, visit our social networking sites such as Instagram, Facebook, LinkedIn, YouTube (hereinafter - Social media accounts), use our services, contact us by email, phone, or other electronic communication channels.

This Privacy policy describes how we collect, use, process, and disclose your personal information. Please read it carefully, as this Privacy policy is legally binding on you when you use the above-mentioned services. If you do not agree with this Privacy policy, you should immediately refrain from using our Web, App, Social media accounts and/or services.

We respect your privacy and process your personal data (hereinafter – **Personal data**) in accordance with 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**), the Law on the Legal Protection of Personal Data of the Republic of Lithuania and other applicable legal acts.

We reserve the right to update, change, or replace any part of this Privacy policy by posting revisions on our website and updating the "Last updated" date at the top of this Privacy policy. It is your responsibility to review this page periodically for any changes. Your continued use of the Web, App and/or services after the posting of any changes constitutes your acceptance of those changes. If you do not agree with any updates, changes, or amendments, you must immediately stop using our Web, App and/or services.

FINCI's Web, App or services are not directed to individuals under the age of 18, and we do not knowingly request or collect any information about individuals under the age of 18. If you are under the age of 18, please do not provide any personal information. If it is suspected that an individual submitting personal information is under the age of 18, FINCI will require the individual to close their account and will take steps to delete their information as soon as possible.

The Web, App or Social media accounts may contain links to, for example, websites of our partners. This Privacy policy does not apply to such external websites. We encourage you to review the privacy policies of any third-party sites or platforms before disclosing any personal information or proceeding further.

1. DETAILS OF THE DATA CONTROLLER

The controller and owner of the websites: **www.finci.com**, Internet bank **ib.finci.com**, Open banking developer.finci.com, Access control server for 3-D secure authentication (3DS) acs.finci.com is FINCI UAB, registration number: 304934066, registered office: Mėnulio str. 11-101, LT-04326 Vilnius, Republic of Lithuania. The controller operates as an electronic money institution (EMI) under Electronic Money Institution (EMI) license No. 60, issued and regulated by the Bank of Lithuania.

You can contact us by phone: **+370 691 10693** or by writing to the following e-mail address: **info@finci.com**.

2. CONTACT DETAILS FOR COMMUNICATION ON PERSONAL DATA PROTECTION

If you have any questions related 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 Data Protection Officer by writing to the following e-mail address: **dpo@finci.com**.

3. THE PURPOSES AND LEGAL BASIS 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 laws.

As a regulated EMI, we are obliged to comply with the legal obligations provided by the following legal regulations (but not limited to): 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 the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania (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 implement know your customer (hereinafter – **KYC**) requirements.

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 specific purposes that we have clearly explained to you and not used in any way that is incompatible with 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 including, but not limited, 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 used for biometric identity verification)
• citizenship
• email address
• phone number
• records of phone calls
• 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
• your status as a politically exposed person
• services usage information
• other data required by the Applicable legislation.

FINCI mobile App data
When you use the FINCI mobile application, we may collect additional information required for App functionality, analytics, fraud prevention, security, compliance and account management:

- crash logs, diagnostics, and other App performance data
- photos and videos
- files and docs
- mobile phone
- other device information and features (such as notifications, if you enable them)

Below you can find the details and additional information for what specific purposes and/or what data for certain 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;
- 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 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 and biometric identity 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 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 detail), 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 in 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.

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

If your employer uses FINCI Business and nominates you as FINCI cardholder and/or account user, your employer will provide us with information about you. This will also include your identification and information about any transactions you make with FINCI Business payment card.

The legal basis of Personal data processing for the above-mentioned purposes are:

1. Your consent to the personal data processing (Article 6 (1) (a) of GDPR) and (Article 9 (2) (a) of GDPR, in case in your identification process we collect any of special categories of your Personal data, e.g., biometric data via "liveness check" - direct video transmission (live video broadcast records);
2. The conclusion and performance of the contract (Article 6 (1) (b) of GDPR);
3. Compliance with legal obligations under Applicable legislation (Article 6 (1) (c) of GDPR);
4. Legitimate interests of the controller (Article 6 (1) (f) of GDPR), such as identifying you as a client and/or client representative/beneficial owner/controlling person, maintaining contact, and ensuring high-quality service.

3.2. AML/CTF and transaction monitoring

We will process the Personal data for this purpose as indicated in Paragraph 3.1.

As part of this, we must comply with the AML/CTF legal framework, establish your and/or your represented legal entity's client risk classification, monitor transactions, and carry out risk scoring and AML/CTF risk exposure assessments.

To fulfil our legal obligations under the AML/CTF framework, we may verify information relating to you against credible, publicly available sources; monitor your transactions; provide information to supervisory and investigative authorities, where required by applicable law; maintain relevant registers (e.g., risk register, beneficial owners' register).

As a regulated EMI, we are also obliged to conduct retrospective monitoring of clients' activities. To fulfil these obligations, we may send additional information requests for personal data to verify details required under the Applicable Legislation.

While monitoring payment transactions, we may request documents confirming the economic substance or legitimacy of a transaction. These documents may also contain personal data.

The legal basis personal data processing for this purpose is as follows:

1. Fulfilment of legal obligations under the Applicable Legislation (Article 6 (1)(c) of the GDPR);
2. Legitimate interests of the controller (Article 6 (1)(f) of the GDPR), such as identifying you as a client and/or a client's beneficiary and ensuring effective communication.

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

As part of this, we may send you commercial communications by e-mail, based on your consent or our legitimate interest. If you subscribe to our newsletters or you are our existing client, client's representative, or contact person, we may send you information and 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 requested.

We may also provide you with (push) notifications of our new products and offers via our App, if you are using it and have subscribed to receiving such notifications.

If you do not wish to receive our commercial communications, you can inform us and refuse further communications at any time. We also provide you, free of charge, with an easy-to-use option to unsubscribe via a link included in every commercial e-mail we send.

If you do not want to receive push notifications via our App, you can manage your user preferences by switching off this option.

For this purpose, we might need at least the following Personal data:

- your name,
- surname,
- data of the legal entity you represent,
- e-mail address,
- location,
- services and products you have used, requested, or searched for in our App, and

- other user experience data.

The legal bases for personal data processing for this purpose are:

1. Your consent to the processing of personal data (Article 6(1)(a) of the GDPR);
2. Legitimate interests of the controller (Article 6(1)(f) of the GDPR), such as informing you about our services, and sending you information about our special offers or products.

3.4. Prevention of threats to FINCI's or third parties' legitimate interests

As part of this, we carry out video surveillance of our territory, buildings, and other properties, record phone conversations and protect our rights in case of disputes or claims.

If necessary, we may disclose information to supervisory authorities, judicial bodies, law enforcement agencies, courts, or other public officials, as well as to insurers, in order to exercise rights conferred by law or to protect other legitimate interests of FINCI or third parties.

Video surveillance is continuous and operates 24 hours a day, 7 days a week.

For this purpose, we might need to process at least the following Personal data:

- the client's or visitor's image and other data captured by video surveillance
- name and surname (if available)
- address of the object
- location and time
- phone number
- email address
- other information related to criminal activity
- administrative or other violations
- legal and/or insurance matters, content of the complaint
- claim, or proceeding, and
- any information related to a dispute or claim

The legal bases for the processing of personal data for this purpose are:

1. Your consent to the processing of personal data (Article 6(1)(a) of the GDPR);
2. Legitimate interests of the controller (Article 6(1)(f) of the GDPR), such as ensuring the security of our assets, information, employees, and third parties; preventing, detecting, and controlling illegal acts and incidents; and ensuring effective protection of our rights.

3.5. Conclusion of agreements for service delivery, payment processing, and FINCI operations

FINCI processes Personal data for the purposes of concluding, executing, and monitoring the execution of contracts for internal use, processing payments under concluded contracts, and handling complaints and claims related to the conclusion, execution, and/or termination of contracts.

In addition, FINCI processes personal data to ensure the accurate fulfillment of tax obligations: issuing and/or receiving invoices, calculating taxes and payments, declaring information to supervisory tax authorities, managing payments, maintaining accounting records, and managing debt.

For this purpose, we might need to process at least the following Personal data:

- name
- surname
- email address
- phone number
- position
- workplace
- represented person (when acting on behalf of a company or another individual)
- relationship with the represented person
- individual activity data
- payment data, and other
- collaboration-related data.

The legal bases for the processing of personal data for this purpose are:

1. The processing is necessary for the conclusion and performance of a contract (Article 6(1)(b) of the GDPR);
2. The processing is necessary for compliance with a legal obligation imposed on the controller to ensure proper financial accounting (Article 6(1)(c) of the GDPR), in accordance with laws on payments, taxation, financial accounting and reporting, and other applicable legislation;
3. The legitimate interests of the controller or a third party to effectively manage financial operations and debts (Article 6(1)(f) of the GDPR).

3.6. Web and/or App administration, development, security, and fraud prevention

As part of this, we may carry out the maintenance and development of our Web and/or App, technical systems, and IT infrastructure, as well as implement technical and organizational solutions that may involve the use of your Personal data (for example, by placing cookies), in order to ensure the proper provision of services to you.

Regarding our use of cookies, please also refer to our Cookies Policy.

For this purpose, we might need to process at least the following Personal data:

- IP address
- device information, and
- data collected via cookies

All personal data processed by us, including via App, is encrypted in transit using industry-standard protocols. In addition, we apply security measures such as encryption at rest, secure authentication, continuous monitoring, and strict access controls to safeguard your data.

The legal bases for the processing of personal data for this purpose are:

1. Your consent (Article 6(1)(a) of the GDPR);
2. Legitimate interests of the controller (Article 6(1)(f) of the GDPR), such as ensuring the smooth functioning, development, and security of the Web and/or App.

3.7. Managing Social media accounts

We use external social media platforms such as Facebook, Instagram, LinkedIn, and YouTube to share updates on trends, services, events, and to promote our brand. When you interact with our channels or share personal information, we may receive and use the data you voluntarily provide, such as comments on our posts. These platforms are operated by providers like Meta, who may collect additional personal data about you. For details on how they process your data, please refer to their respective privacy policies.

For this purpose, we might need to process at least the following Personal data:

- username
- comments and shares on posts
- information about clicks on “like” and “follow”
- information about reactions to entries
- photos
- details of messages and our replies (e.g., time of receipt, content, attachments)
- rating information, and
- any other information you voluntarily provide.

The legal basis for the processing of personal data for this purpose is our legitimate interest in promoting our brand, products, and services (Article 6(1)(f) of the GDPR).

3.8. Recruitment

In connection with recruitment, we will collect, use, and store the following categories of Personal data about you:

- The data you have provided to us in your curriculum vitae (CV) and the Personal data contained in your covering letter (if applicable). This data may include: name, title, address, telephone number, personal email address, date of birth, employment history, qualifications, social media accounts, profession, professional memberships, educational achievements, diplomas, certificates, transcripts, languages, computer skills, and national service completion.
- The data received from the feedback provided by referees (upon your consent).
- The data received from publicly accessible professional sources, such as LinkedIn, where we collect the data included on your profile.
- The data you provide during interviews.

Please note that for recruitment purposes, we do not require you to send us copies of your identification documents, diplomas, and/or other professional qualification certificates. However, we may ask you to present or provide these documents during the employment process.

Normally, we do not process sensitive Personal data, or special categories of personal data, for recruitment purposes. However, there may be occasions when such data becomes known to us during the recruitment process. If so, we will process your sensitive personal data only if we are permitted by law to do so. For instance:

- We may use data about your disability status to assess whether reasonable accommodation is needed during the recruitment process, for example, for interviews or testing.
- We may use data about your nationality or ethnicity to determine whether a work permit or visa is required for the role.

Your personal data is processed solely for the purposes of the recruitment process.

The legal bases for the processing of personal data are as follows:

1. Your consent (Article 6(1)(a) of the GDPR), for example, when submitting a CV voluntarily or allowing us to retain your CV for future vacancies;

2. The conclusion or performance of a contract (Article 6(1)(b) of the GDPR), when processing data of candidates with whom a decision to conclude an employment or other contract has been made;
3. Compliance with a legal obligation (Article 6(1)(c) of the GDPR), in individual cases where regulatory requirements apply to specific positions; or processing of special categories of data (Article 9(2)(b) of the GDPR), when such data is necessary for employment-related obligations and permitted by law;
4. Legitimate interests of the controller (Article 6(1)(f) of the GDPR), for example, contacting candidates, documenting the recruitment process in the event of disputes or legal claims, and limiting the scope of data collection to what is necessary.

4. THE SOURCES OF OBTAINING YOUR PERSONAL DATA

We can receive your Personal data from one of the following sources:

- from you, when you visit our Web, App, Social media accounts and/or subscribing our services;
- from you, when you provide your personal data for identification and KYC purposes via our Web and/or App;
- 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 and other documents;
- from other financial institutions, e.g., banks, payment institutions;
- 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 WE NEED 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 mentioned above in this Privacy policy. 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 is 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 RECIPIENTS OF YOUR PERSONAL DATA

Your Personal data could be accessed as needed by and shared with our directly authorized persons/companies who are required to process this Personal data to perform their duties, such as:

- outsourcing accountants, auditors, financial management and legal advisers, insurance;
- global financial messaging infrastructures that are subject to oversight by relevant authorities (eg., SWIFT);
- global payment systems (e.g. Visa, MasterCard);

Personal data processors (see the categories of Personal data processors below):

Your Personal data will be transferred 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:

- Software services providers, companies providing IT services and
- Providers of marketing services;
- IT infrastructure services providers;
- Helpdesk services providers;
- Companies that carry out KYC/AML checks and fraud database checks;
- Customer support services providers;
- Video surveillance/security services providers;
- 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, carefully assessing whether such Persona data transfer has an appropriate legal basis:

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. RETENTION OF PERSONAL DATA

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 consider 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 cooperation 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 90 (ninety) days from the date when they are 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);
- For Social media accounts, data is stored according to their respective settings;
- We will retain your Personal data for recruitment for a period of 1 (one) year upon your explicit consent. We retain your Personal data for that period so that we can show, in the event of a legal claim, that we have not discriminated against employment candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. We further retain such Personal data in case a similar role becomes vacant for which you will be a fitting candidate.

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**:

- a data processing agreement that describes such transfer and includes Standard Contractual Clauses for international transfers; or
- an adequacy decision adopted by the European Commission, which means that the European Commission has recognized the country in which the third party is established and/or carries on business as providing an adequate level of protection of personal data; or
- a specific authorization by the data protection supervisory authority to carry out such transfer; or
- your consent to the transfer of your Personal Data outside the EU / EEA.

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.

To enable us to publish content on Social media accounts, we disclose data to the following operators of social networking platforms:

- Meta Platforms Ireland Limited (Ireland) and Meta Platforms, Inc., (USA), (data is transferred in accordance with an adequacy decision issued by the European Commission; active participant of EU-U.S. Data Privacy Framework and Swiss-U.S. Data Privacy Framework);
- LinkedIn Ireland Unlimited Company (Ireland) and LinkedIn Corporation (USA) (data is transferred in accordance with an adequacy decision issued by the European Commission; active participant of EU-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework and Swiss-U.S. Data Privacy Framework);
- YouTube Inc. (USA) (data transferred in accordance with the EU Standard Contractual Clauses approved by the European Commission).

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 to prevent fraud, money-laundering and terrorist financing events. However, we do not make automatic decisions based on profiling.

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

The main legal basis 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

If you wish to withdraw your consent for the processing of Personal data or to exercise any of your rights set out below, you may contact us by email **dpo@finci.com**.

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, restrict processing, to object to the processing of your Personal data, to object to the application to you of a fully automated decision, including profiling, where such a decision may have legal consequences or a similar significant effect on you, as well as the right to data portability in the cases and procedures set out in the GDPR.

Deleting or uninstalling the FINCI App does not delete your FINCI account. You may delete your FINCI account by contacting us at **dpo@finci.com** . However, we may retain certain information for up to 8 years, or longer if required by anti-money laundering, counter-terrorism financing, or other applicable financial regulations. Such retained data will be securely stored and used only for compliance purposes.

We respect your rights, 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).

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 based on 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.

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: **dpo@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 to ensure the security and disclosure of your Personal data to the person concerned.

11. 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 our Data protection officer first.

If you still want to submit the complaint, you can do it in the 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 the relevant fields provided in the complaint form. If at least one of the appropriate fields is 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.

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/**), Sapiegos st. 17, Vilnius, Lithuania, phone. (8 5) 271 2804, 279 1445, fax. (8 5) 261 9494, e-mail **ada@ada.lt**.