

PRIVACY POLICY

This Privacy Policy (the “Policy”) sets out the principal terms governing the processing of personal data of visitors to the website of UAB Finance EU, the operator of the Florrid crowdfunding platform (legal entity code 306726092, registered office at Debesijos g. 8-38, LT-10314 Vilnius, Lithuania) (the “Company” or “we”), its clients (investors and project owners), their representatives and beneficial owners (“you”).

The controller of your personal data is UAB Finance EU, legal entity code 306726092, with its registered office at Debesijos g. 8-38, LT-10314 Vilnius, Lithuania.

This Policy has been prepared in accordance with:

- a. the General Data Protection Regulation (the “GDPR”);
- b. the Law of the Republic of Lithuania on Legal Protection of Personal Data;
- c. the Law of the Republic of Lithuania on Electronic Communications; and
- d. other legislation applicable to the Company, its crowdfunding activities and the provision of such services, as well as instructions and recommendations issued by supervisory authorities.

If you have any questions concerning the protection of your personal data or the provisions of this Policy, please contact the Company by email at info@florrid.com.

When processing your personal data, the Company complies with the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation and accuracy. The Company also implements security measures and procedures designed to protect your personal data against unauthorised access, disclosure, loss, alteration, destruction or other unlawful processing.

1. DEFINITIONS

- 1.1. Capitalised terms used in this Policy shall have the meanings set out below, unless the context requires otherwise:
 - 1.1.1. Personal Data means any information that may be used to identify a natural person directly or indirectly, as well as any information relating to an identified natural person;
 - 1.1.2. Data Subject means a natural person who is a visitor to the Company’s website at <https://florrid.com> (the “Website”), a client of the Company, a person submitting an enquiry to the Company, or another person connected with the Company’s activities and/or services;
 - 1.1.3. Processing means any operation performed on Personal Data, including, without limitation, collection, recording, organisation, storage, alteration, consultation and use.
- 1.2. Other terms used in this Policy shall have the meanings assigned to them in the GDPR, other applicable legislation and the Company’s internal rules.

2. PURPOSES AND LEGAL BASES OF PERSONAL DATA PROCESSING RETENTION PERIODS AND CATEGORIES OF PERSONAL DATA PROCESSED

- 2.1. The Company processes your Personal Data for the purposes and to the extent set out below:

Purpose of processing	Legal basis for processing	Retention period	Scope of processing
1. Remote identity verification	Your consent	Identity verification data are retained for 8 years after the end of the business relationship. The period may be extended by no more than 2 additional years. Biometric data (facial image and video) are used solely for a one-time identity check. No facial template is created or stored; after verification, these data are deleted and only the verification result (match/non-match) is retained for the above 8-year period. If services are refused, data are retained for 2 years from the date of the refusal decision.	Full name, personal identification number, date of birth, nationality, identity document details and copies, photograph, biometric data such as a facial image (selfie) and video, permanent residence permit details, telephone number, email address, residential address, registered address or correspondence address.
2. Ongoing monitoring of business relationships	Legal obligation	8 years after the end of the business relationship. The period may be extended by no more than 2 additional years.	Data required to apply measures for the prevention of money laundering and terrorist financing and to ensure compliance with international sanctions, including the purpose of the client relationship, politically exposed person status, source of wealth, counterparties and business activities, participation in companies and other legal entities, managers, controlling persons or representatives, beneficial owners, representatives' contact details, IP address, login location and other relevant information.
3. Creditworthiness assessment	Legal obligation; GDPR Article 6(1)(b) - performance of a contract	10 years from the date of the Project Owner's most recent financing transaction. If services are refused, data are retained for 2 years from the date of the refusal decision.	Data required to comply with the Crowdfunding Regulation and perform the contract: (a) data available in JAR, JADIS, JANGIS, TAAR, the Mortgage Register, Creditinfo, public sources and NTR; (b) data supplied by the client, including contact details, approved financial statements for the previous three years, projected cash flows, business plan, forecast financial statements, information on security (property valuation, cost estimate, permits, designs, evidence of payments, etc.) and, where necessary, supporting cash-flow information, account statements, State Social Insurance Fund Board statements and certificates concerning convictions and criminal offences.

Purpose of processing	Legal basis for processing	Retention period	Scope of processing
4. Reliability assessment	GDPR Article 6(1)(c) - legal obligation	Information, data and documents collected or assessed during the Project Owner's reliability assessment are retained for 10 years from the date of the most recent financing transaction. If services are refused, data are retained for 2 years from the date of the refusal decision.	Data concerning convictions and criminal offences; performance of financial obligations; civil claims, administrative or criminal proceedings, investments, risks undertaken and loans that may materially affect financial reliability; records concerning the Project Owner in conviction registers and other reliable databases lawfully available to the Company. The processing relies on the automated creditworthiness calculation form approved by the Bank of Lithuania.
5. Assessment of investment experience and knowledge	GDPR Article 6(1)(c) - legal obligation	10 years after the end of the business relationship or agreement with the investor. If services are refused, data are retained for 2 years from the date of the refusal decision.	Full name, age, education, income, savings, liabilities, investment experience, investment objectives and other related information.
6. Administration of crowdfunding transactions	GDPR Article 6(1)(b) - performance of a contract; GDPR Article 6(1)(c) - legal obligation	10 years after the agreement or loan agreement ends.	Full name and registered residence; for a legal entity, the manager's or authorised person's full name, personal identification number, email address and telephone number; telephone number, email address, loan agreement number, dates of conclusion and termination, dates when debt recovery was referred and withdrawn, investment details, purpose and amount of the loan, repayment schedule, information on security and other related information.
7. Prevention of money laundering and terrorist financing	GDPR Article 6(1)(c) - legal obligation; public interest	Copies of client identity documents, beneficial owner identification data, other data obtained during client identification, and account and/or contractual documents are retained for 8 years after the end of transactions or the business relationship. The period may be extended by no more than 2 additional years.	Full name, personal identification number, date of birth, registered and residential addresses, nationality, email address, telephone number, shareholders' or beneficial owners' shareholdings, investment object and expected amount, income, principal source and true owner of funds, account and/or contractual documents, business correspondence, documents and data evidencing monetary operations or transactions, IP address, checks in public and reliable registers, other KYC data, politically exposed person status and other relevant information.

Purpose of processing	Legal basis for processing	Retention period	Scope of processing
8. Compliance with international sanctions requirements	GDPR Article 6(1)(c) - legal obligation; public interest	8 years after the end of the business relationship. The period may be extended by no more than 2 additional years.	Full name, personal identification number, date of birth, registered and residential addresses, nationality, email address, telephone number, shareholders' or beneficial owners' shareholdings, investment object and expected amount, income, principal source and true owner of funds, account and/or contractual documents, business correspondence, documents and data relating to transactions, IP address, checks in public and reliable registers, other KYC data, politically exposed person status, inclusion on sanctions lists and other relevant information.
9. Conclusion and performance of agreements	GDPR Article 6(1)(b) - steps taken before entering into a contract and performance of a contract	10 years after the agreement ends.	Full name, telephone number, email address, identification and identity verification data and other data necessary to provide the Company's services and conclude or perform the agreement. In certain cases, we may process the Personal Data of your lawful heirs, including copies of identity and inheritance documents, bank account number and other inheritance-related information.
10. Improvement of service quality, including examination of complaints and/or claims	Legitimate interests; GDPR Article 6(1)(c) - legal obligation	2 years from the date on which the enquiry, complaint or claim is submitted.	Full name, telephone number, email address, residential, registered or correspondence address, information about actions performed on the Website and related technical information, IP address used to connect, operating system version and device parameters, login information including session time and duration, search terms entered on the Website, letters, emails, chat messages and other communications and their content.
11. Prevention, restriction and investigation of abuse, fraud, unlawful use or disruption of services, and establishment, exercise or defence of legal claims	GDPR Article 6(1)(c) - legal obligation; GDPR Article 6(1)(f) - legitimate interests	10 years from the event giving or potentially giving rise to a claim. If suspected unlawful activity is investigated, the data are retained for the duration of the investigation and any related dispute.	Full name, telephone number, email address, residential, registered or correspondence address, letters, emails and other communications and their content, identity data, information on property, transactions, loans, liabilities, deposits made through the Platform or Website, the account from which a deposit was made and other relevant information.
12. Responding to your enquiries	Your consent; performance of a contract	Data contained in enquiries submitted to the Company by telephone, email or other electronic or physical means, and data relating to the persons making them, are retained for 2 years from the date of the enquiry.	Full name, telephone number, email address, residential, registered or correspondence address, letters, emails, chat messages and other communications and their content.

Purpose of processing	Legal basis for processing	Retention period	Scope of processing
13. Processing of statistical data	GDPR Article 6(1)(c) - legal obligation	Indefinitely in anonymised form.	Information about the Project Owner and funds raised; aggregated information about investors and invested amounts, broken down by investors' tax residence and distinguishing sophisticated and non-sophisticated investors; and other statistical information required by law. These data are processed so that no individual Data Subject can be identified, meaning that the Personal Data are anonymised.
14. Debt recovery and administration	Performance of a contract	10 years from the date of final and proper settlement or repayment of the debt.	Full name, personal identification number, date of birth, residential, registered or correspondence address, telephone number, email address, amount owed, duration of delay, payment date, data required to assess solvency, security for performance and other information relating to the debt.
15. Provision of information to investors	GDPR Article 6(1)(c) - legal obligation	10 years from the date of the Project Owner's most recent financing transaction.	Information about the Project Owner(s) and crowdfunding project, management and contact details, and all natural and legal persons responsible for information in the key investment information sheet. For natural persons, this includes the full name and position of members of the Project Owner's administrative, management or supervisory bodies, property valuation reports and other relevant information.

3. PROCESSING OF PERSONAL DATA FOR DIRECT MARKETING PURPOSES

- 3.1. We may send direct marketing communications by electronic means, including emails, newsletters and text messages:
 - 3.1.1. to legal entities without prior consent, provided that each communication offers a clear, free-of-charge and easily exercisable option to object to any further use of electronic communications services, including email, for direct marketing purposes; and
 - 3.1.2. to natural persons only where (i) we have obtained the recipient's prior consent, or (ii) the recipient is an existing client, we obtained their electronic contact details in connection with providing services, and the marketing concerns our own similar services, provided that a clear, free-of-charge and easily exercisable option to object to such use of contact details is offered both when the details are collected and in every subsequent communication.
- 3.2. Where direct marketing communications are sent on the basis of consent, you have the right to withdraw your consent at any time, without affecting the lawfulness of processing carried out before its withdrawal.
- 3.3. We provide a clear, free-of-charge and easily exercisable option to withdraw your consent at any time. You may opt out of our direct marketing communications at any time by notifying us at info@florrid.com or by using the unsubscribe link included in the communication. Every direct

marketing communication sent by us will clearly identify the sender and provide a valid contact address through which the recipient may request that such communications cease.

- 3.4. Please note that emails, including informational notices relating to the performance of our contractual obligations, telephone calls or other communications connected with the performance of concluded agreements do not constitute direct marketing.

4. HOW DO WE OBTAIN YOUR PERSONAL DATA

- 4.1. We process Personal Data that:

- 4.1.1. you provide to us directly;
- 4.1.2. our clients provide to us where, for example, you are their family member or a representative, employee, contractor, founder, shareholder, member or owner of a client that is a legal entity, or the owner of property offered as collateral;
- 4.1.3. we receive in documents submitted by clients, such as applications and questionnaires, written explanations, payment documents, property valuation documents, sale and purchase agreements and other agreements, insurance documents, court decisions and refinancing consents;
- 4.1.4. we obtain from external sources, including:
 - 4.1.4.1. other financial institutions;
 - 4.1.4.2. supervisory and other public authorities or institutions, such as the Bank of Lithuania;
 - 4.1.4.3. the State Enterprise Centre of Registers, including the Population Register, the Information System of Members of Legal Entities (JADIS), the Subsystem of Beneficial Owners of Legal Entities (JANGIS), the Register of Legal Entities and other registers;
 - 4.1.4.4. entities administering joint debtor databases, such as Creditinfo and Okredo;
 - 4.1.4.5. law enforcement authorities;
 - 4.1.4.6. natural or legal persons, including notaries, bailiffs and lawyers, when they provide data in compliance with contractual or statutory requirements;
- 4.1.5. we obtain by monitoring the use of our systems and services.

- 4.2. The Company may also verify publicly available information about you in order to check the information and transactions you have provided.

- 4.3. When providing Personal Data to us, you are responsible for ensuring that the data are accurate, complete and up to date. If inaccurate, false or misleading Personal Data are provided, we may delete such data or restrict access to our services. If you provide Personal Data relating to other persons, such as relatives or employees, you are responsible for the accuracy, completeness and currency of those data and for ensuring that you are entitled to provide them to us. We may ask you to confirm that you have the right to provide such data. If that person asks us about the source of their Personal Data, we will identify you as the person who provided them.

5. PERSONAL DATA RETENTION PERIODS

- 5.1. We will retain your Personal Data for as long as necessary for the purposes for which they were collected and processed, but no longer than required by applicable laws and regulations. At the end of the applicable period, the Personal Data will be deleted or destroyed so that they cannot be restored.

- 5.2. Where Lithuanian or international law does not prescribe a retention period, we determine the period having regard to the lawful purpose and legal basis for retention and the principles governing the processing of Personal Data.
- 5.3. The specific Personal Data retention periods are set out in the table in Section 2 of this Privacy Policy, Purposes and Legal Bases of Personal Data Processing, Retention Periods and Categories of Personal Data Processed.
- 5.4. Please note that in certain cases your Personal Data may be retained for longer:
 - 5.4.1. where necessary for us to defend against demands, claims or legal proceedings and to exercise our rights;
 - 5.4.2. where we have reasonable grounds to suspect unlawful activity that is under investigation;
 - 5.4.3. where the Personal Data are required for the proper resolution of a dispute or complaint;
 - 5.4.4. on other grounds provided for by law.

6. SECURITY OF PERSONAL DATA

- 6.1. To safeguard your Personal Data and prevent unlawful or accidental destruction, alteration or disclosure, as well as any other unauthorised processing, we implement various technical and organisational security measures. These include hardware and software, additional agreements with service providers, internal rules relating to Personal Data protection and other measures. In certain cases, transmitting information by electronic means, such as email or mobile communications, may be less secure for reasons beyond the technical or organisational measures selected by us. To protect the security of your confidential Personal Data, we recommend that you do not send such information through less secure electronic systems or systems that we do not use.

7. RECIPIENTS OF PERSONAL DATA

- 7.1. In conducting its activities, the Company may engage data processors, including providers of data storage, software development and maintenance, debt administration and communications services. Some of your Personal Data may be disclosed to such persons, but only where and to the extent necessary for the provision of the relevant services.
- 7.2. Recognising our obligation to process your Personal Data in strict compliance with applicable requirements, we engage only service providers that have implemented or undertaken to implement appropriate technical and organisational security measures. We ensure that those providers comply with appropriate Personal Data protection, security and confidentiality obligations set out in written agreements.
- 7.3. Recipients of your Personal Data may also include:
 - 7.3.1. payment and other service providers and financial institutions whose services the Company uses in its activities, such as UAB ONDATO;
 - 7.3.2. entities administering joint debtor databases, including Creditinfo and Okredo;
 - 7.3.3. public authorities and registers, including the Bank of Lithuania, Statistics Lithuania and law enforcement authorities;
 - 7.3.4. courts, notaries and bailiffs;
 - 7.3.5. auditors and legal and financial advisers;
 - 7.3.6. where necessary, companies intending to acquire or acquiring the Company's business;
 - 7.3.7. other third parties involved in providing the Company's services and/or having a lawful basis to receive the data.

8. DOES THE COMPANY TRANSFER YOUR PERSONAL DATA OUTSIDE THE EU OR EEA

- 8.1. The Company's activities do not require your Personal Data to be transferred to recipients established outside the European Union (EU) or European Economic Area (EEA).
- 8.2. However, if in exceptional circumstances some of your data need to be transferred to a recipient outside the EU/EEA, we will take all measures required by law to ensure that your Personal Data remain adequately protected.
- 8.3. Your Personal Data may be transferred outside the EEA only where:
 - 8.3.1. the recipient has entered into the standard contractual clauses approved by the European Commission; or
 - 8.3.2. the recipient is established in a country for which the European Commission has adopted an adequacy decision, meaning that a transfer to a recipient in that country is treated in the same way as a transfer within the European Union; or
 - 8.3.3. under Article 49 of the GDPR, you have consented to the transfer of your Personal Data outside the EEA.

9. THIRD PARTY WEBSITES

- 9.1. Our Website may contain links to or from the websites of partners, information sources or related persons. Please note that third-party websites accessed through links on our Website have their own privacy policies, for which we accept no responsibility. Before providing any Personal Data on another website, you should review that website's terms, privacy policy and other information.

10. IDENTITY VERIFICATION TOOLS USED BY THE COMPANY

- 10.1. To identify and verify you, we use UAB ONDATO, a service provider engaged by our partners. Through a dedicated website, this provider uses a camera to capture a photograph or video of your face and the identity document you submit. Further information about UAB ONDATO is available in its privacy policy.
- 10.2. The UAB ONDATO solution compares a live photograph or video of your face with the identity document you provide. This enables compliance with legal obligations, including requirements under the Lithuanian Law on the Prevention of Money Laundering and Terrorist Financing and other requirements aimed at preventing fraud and crime, as well as risk management obligations.
- 10.3. The facial similarity result, whether a match or non-match, will be retained for as long as necessary to complete the verification and for the period prescribed by legislation on the prevention of money laundering and terrorist financing.
- 10.4. The facial similarity check is a one-time user verification involving a comparison of images based on data obtained during the verification. No facial template is created, recorded or stored. The original data cannot be reconstructed from the retained information.
- 10.5. When UAB ONDATO services are used, Personal Data are processed to verify your identity by comparing the image in your identity document with the person captured in the photograph. This process enables us to establish your identity more accurately and makes verification faster and easier. If you are not comfortable with this method, you may contact us at info@florrid.com to request an alternative means of identification.

11. COOKIES USED BY THE COMPANY

- 11.1. The Company uses cookies on its Website. Further information about the cookies used, their purposes and how to manage them is provided in the Company's Cookie Policy.

12. DATA SUBJECT RIGHTS

12.1. As a Data Subject, you have the following rights:

- 12.1.1. to access your Personal Data and information about how they are processed. You have the right to obtain confirmation as to whether we process your Personal Data, access the Personal Data being processed and receive other related information;
- 12.1.2. to request the rectification of incorrect, inaccurate or incomplete data. If you believe that information we process about you is inaccurate or incorrect, you may request that it be changed, supplemented or corrected;
- 12.1.3. to request the erasure of your Personal Data (the “right to be forgotten”). In circumstances specified by law, including where Personal Data are processed unlawfully or the legal basis for processing no longer exists, you may request that we erase your Personal Data;
- 12.1.4. to request restriction of the processing of your Personal Data. In circumstances specified by law, including where Personal Data are processed unlawfully, you may request that we restrict their processing;
- 12.1.5. to request that your Personal Data be transmitted to another controller or provided directly to you in a convenient format. In certain cases, you have the right to transmit to another controller data that we process on the basis of your consent by automated means;
- 12.1.6. to object to the processing of Personal Data where they are processed on the basis of legitimate interests, unless there are compelling legitimate grounds for the processing or the processing is necessary for the establishment, exercise or defence of legal claims;
- 12.1.7. to withdraw your consent to the processing of your Personal Data. Where Personal Data are processed on the basis of separate consent, you may withdraw that consent at any time. We will then cease processing the relevant Personal Data.

12.2. Please submit requests concerning the exercise of data subject rights in writing by email to info@florrid.com.

12.3. If you believe that your Personal Data are being processed unlawfully or that your rights relating to the processing of Personal Data have been infringed, please contact us using the method specified in paragraph 12.2. We will comply with your request or reject it, stating the reasons, within 30 calendar days of receiving it. This period may be extended by a further 60 calendar days, with prior notice to you, if the request concerns a large volume of Personal Data. The response will be provided by the same means by which the request was received, except where a more detailed investigation is required, in which case the response may be sent by email. After examining the request, we will notify you of the outcome and the action taken, or explain what further steps you may take if your request has not been fulfilled or granted.

12.4. A request to exercise your rights must meet at least the following minimum requirements:

- 12.4.1. it must be in writing and be legible and understandable; a request submitted by the method specified in paragraph 12.2 will be treated as a written request;
- 12.4.2. it must state your full name and other contact details, including your email address and telephone number;
- 12.4.3. it must clearly and precisely identify which of the rights listed above you wish to exercise and to what extent;
- 12.4.4. if you exercise your rights through a representative, the request must state the representative's full name and contact details and be accompanied by a document confirming the representative's authority.

- 12.5. If you make an oral request to exercise your rights as a Data Subject, we may ask you to submit a written request and must inform you of all available methods for submitting it and the applicable minimum requirements.
- 12.6. You also have the right to lodge a complaint with the State Data Protection Inspectorate if you believe that your Personal Data are being processed in breach of your rights or legitimate interests under applicable law. Before contacting the Inspectorate, however, we encourage you to contact us without delay so that we can work together to find the quickest and most suitable solution.
- 12.7. Please note that the data subject rights described above may be restricted to ensure the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security, and in the other circumstances specified in Article 23 of the GDPR.

13. FINAL PROVISIONS

- 13.1. The Company reserves the right to update this Policy. You should review it regularly to remain informed of any changes.
- 13.2. When making changes, we will not reduce the scope of your rights under this Policy or applicable Personal Data protection laws. When the Policy is updated, we will publish the revised version on our Website. Previous versions of the Policy will also remain available on our Website.
- 13.3. Amendments and/or supplements to the Policy shall take effect upon publication on the Website.