

PRIVACY POLICY

The present privacy policy (“**Policy**”) of crowdfunding platform “Crowdpear” operator UAB Crowdpear (code of legal entity: 305888586, seat address: Kareivių g. 11B, Vilnius, Lithuania) (“**Company**” or “**we**”) defines the basic conditions for processing the personal data of the Company’s website visitors, clients (investors, project owners), their representatives and beneficiaries (“**You**”).

Email address of the Data Protection Officer of the Company: milda@crowdpear.com, phone No. +370 616 56776.

The present Policy has been drawn up in accordance with:

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

If you have questions related to your personal data protection or provisions of the present Policy, contact the Company by email address info@crowdpear.com.

The Company adheres to the principles of legality, fairness, transparency, purpose limitation, data volume reduction and data accuracy when processing your personal data. The Company also establishes security measures and procedures in its activities to protect your personal data from unauthorized access, disclosure, loss, alteration, destruction or other unauthorized processing.

1. DEFINITIONS

- 1.1. The capitalized definitions in the present Policy have the meanings set forth below, unless the context requires otherwise:
 - 1.1.1. **Personal data** – any information that can be used to identify a natural person directly or indirectly, as well as any information about a natural person that has already been identified;
 - 1.1.2. **Data subject** – a natural person who is a visitor of the Company’s website <https://crowdpear.com/lt/> (“**Website**”), a client of the Company, a sender of inquiries to the Company or another person related to the Company’s activities and/or provided services;
 - 1.1.3. **Processing** – any operation performed with Personal Data, including but not limited to collection, recording, systematization, storage, change, access, use, etc.
- 1.2. Other definitions used in the Policy are understood as defined in the GDPR, other applicable legislation and the Company’s internal legal acts.

2. PURPOSES AND GROUNDS OF PERSONAL DATA PROTECTION AND CATEGORIES OF PROCESSED PERSONAL DATA

- 2.1. The Company processes your personal data for the purposes and scope indicated below:

Purpose of data processing	Ground of data processing	Scope of data processing
1. Remote identification	Your consent	Name, surname, date of birth, personal code, citizenship, details of the personal identity document and copies of this document, photo, biometric data (such as your face image ("selfie") and video record), details of the permanent residence permit, phone number, email address, residential address, registration address or address for correspondence.
2. Continuous monitoring of business relations	Legal obligation	Data necessary for us to apply the necessary measures in the area of prevention of money laundering and terrorist financing and to ensure the implementation of international sanctions, including to determine the purpose of the business relationship with the client and whether the client is a politically exposed person, source of the origin of property, data on the client's transaction parties and business activities, data on participation in companies and other types of legal entities, data about managers and other persons with decisive voting rights or representatives of companies that use or intend to use our services, as well as information about their actual beneficiaries and representatives of companies that use or intend to use the services, IP address, login location, etc.
3. Credit Risk Assessment	Legal obligation, agreement execution	Data necessary for us to fulfil the requirements established in the Crowdfunding Regulation and the contract and which: a) are available in the systems: Register of Legal Entities, JADIS, JANGIS, TAAR, Mortgage Register, Creditinfo, public information, Register of Real Estate; b) are submitted by the client: contact details, approved financial statements of the legal entity for the last three years, projected cash flows, business plan, forecast financial statements, information of security measures (real estate valuation, estimate, permits, projects, PPS, PPS, payment proofs, etc.), if necessary, information confirming the cash flows, account statements, statements of the Social Insurance Fund Board, data on criminal convictions and offenses (certificates).
4. Reliability assessment	Legal obligation	Data on criminal convictions and offenses; data confirming whether the assessed person fulfills credit obligations; data of civil

		<p>lawsuits, administrative or criminal cases, investments or assumed risks and taken loans that may have a significant impact on the financial reliability of the person; data of the project owner in the register of convictions, as well as data verification in other reliable databases legally available to the Company.</p> <p>The processing of these data is based on the automatic creditworthiness calculation form approved by the Bank of Lithuania.</p>
5. Verification of investment experience and knowledge	Legal obligation	Name, surname, age, education, data on income, savings, liabilities, investment experience and investment goals, other related information.
6. Administration of crowdfunding transactions	Agreement execution, legal obligations.	Name, surname, registered place of residence (in case of legal entity – name, surname, personal code, email address, phone number of the manager or authorised person), phone number, email address, loan agreement number, date of agreement conclusion, date of termination, date of transfer and recovery of debt, investment data, loan purpose, amount, loan repayment schedule, information about security measures, investment data and other related information.
7. Prevention of money laundering and terrorist financing	Legal obligation Public interest	Name, surname, personal code, date of birth, registration address, residence address, citizenship, email address, phone number, number of shares of shareholders (beneficiaries), investment object, planned investment amount, income, main source of funds, real owner of funds, documentation of accounts and/or contracts, correspondence of business relations, documents and data confirming a monetary transaction or other legally valid documents and data related to the execution of monetary transactions or the conclusion of transactions, IP address, data verification in public and reliable registers, other data received from the Data Subject or submitted during the "Know Your Customer" procedure, data on a person's participation in political activities, etc.
8. Assurance of requirements for the implementation of international sanctions	Legal obligation Public interest	Name, surname, personal code, date of birth, registration address, residence address, citizenship, email address, phone number, number of shares of shareholders (beneficiaries), investment object, planned

		investment amount, income, main source of funds, real owner of funds, documentation of accounts and/or contracts, correspondence of business relations, documents and data confirming a monetary transaction or other legally valid documents and data related to the execution of monetary transactions or the conclusion of transactions, IP address, data verification in public and reliable registers, other data received from the Data Subject or submitted during the "Know Your Customer" procedure, data on a person's participation in political activities, inclusion in the lists of sanctions, etc.
9. Agreement conclusion and execution	Seeking to act before the conclusion of the agreement and execution of the agreement	Name, surname, phone number, email address, identification and background check data, and other data required for the provision of the Company's services and the conclusion/execution of the agreement. Please note that in certain cases we are entitled to process the personal data of your legal heirs (copy of the personal documents, copy of inheritance documents, bank account number and other information related to inheritance).
10. Improvement of the quality of provided services, including the handling of your submitted complaints and/or claims	Legal interest Legal obligation	Name, surname, phone number, email address, residence address, registration address or correspondence address, information about actions performed on the Website, related technical information, IP address used during the connection of the Internet user, operating system version and settings of the device used to access the content/services; login information – usage time and duration of your session; request terms entered on the Website, letters, emails, chats and other forms of communication messages and their content, etc.
11. Prevention, limitation and investigation of any abuse, fraud, unauthorized use or disruption of the services or assertion, enforcement and defence of legal claims	Legal interest Legal obligation	Name, surname, phone number, email address, residence address, registration address or correspondence address, letters, emails and other forms of communication messages and their content, personal identification data, data on available property, transactions, loans, liabilities, deposits made on the platform (Website), the account from which the deposit was made, etc.
12. Provision of responses to your inquiries	Your consent Agreement execution	Name, surname, phone number, email address, residence address, registration

		address or correspondence address, letters, emails, chats and other forms of communication messages and their content.
13. Processing of statistical data	Legal obligation	<p>Information about the project owner and the amount raised, summarized information about the investors and the invested amount divided by the investors' place of residence for tax purposes by separating experienced and inexperienced investors, other statistical information required to be processed by legislation applicable to the Company's activities.</p> <p>The said data are processed without leaving the possibility of identifying a specific Data Subject, i. e., the personal data is depersonalized.</p>
14. Debt recovery and administration	Agreement execution	Name, surname, personal code, date of birth, residence address, registration address or correspondence address, phone number, email address, debt amount, duration of delay, date of payment, data to assess the solvency, means of ensuring the fulfilment of the claim and other information related to the resulting indebtedness.
15. Informing investors	Legal obligations	Information about the project owner(s) and the crowdfunding project, management and contact details, all natural and legal persons responsible for the information provided in the basic investment information document, in case of natural persons, including members of the project owner's administrative, management or supervisory bodies, the name, surname and position of the natural person, property valuation reports are indicated, etc.

3. PERSONAL DATA PROCESSING FOR THE PURPOSE OF DIRECT MARKETING

- 3.1. If you are our client, we may use your contact details for the purpose of direct marketing or marketing of similar services (e.g. by sending short messages, newsletters) by providing you with a clear, free and easy-to-implement option to disagree to or opt out of such use of contact details for the above purposes, and if you have not initially disagreed to such use of data.
- 3.2. In all other cases, we may use your contact details for direct marketing purposes only with your prior consent.
- 3.3. We provide you with a clear, free and easy-to-implement option to withdraw your consent at any time. We inform you that you are entitled to opt out to receive direct marketing messages sent by us at any time by informing about your decision by email address info@crowdpear.com or using the opt-out link in the direct marketing message itself (in short messages, newsletters).

- 3.4. Sending e-mails (including the provision of informative messages in your account), calls, the content of which is related to the execution of concluded contracts, are not considered direct marketing activities.

4. PERSONAL DATA STORAGE TERMS

- 4.1. We will store your Personal Data as long as it is necessary for the purposes for which it was collected and processed, but no longer than required by applicable laws and other legislation. At the end of this period, the Personal Data is deleted/destroyed so that it cannot be reproduced.
- 4.2. If the laws of the Republic of Lithuania or international legislation do not establish any Personal Data storage period, we determine this period, considering the legitimate purpose of data storage, the legal basis and the principles of Personal Data processing.
- 4.3. Main storage terms of Personal Data:
- 4.3.1. In case of agreement conclusion and execution, the agreement is stored for 10 (ten) years after expiration;
 - 4.3.2. We store the data of potential clients (who were submitted an offer, but the agreement was not concluded) for 2 (two) years from the date of acceptance of the decision not to conclude the agreement;
 - 4.3.3. In the implementation of the requirements for the prevention of money laundering and terrorist financing, the copies of documents confirming the identity of the client, identity data of the beneficiary, other data obtained during the identification of the client, invoices and/or agreement documents are stored for 8 (eight) years from the date of end of transactions or business relations with the client. The correspondence of business relations with the client is stored for 5 (five) years from the date of the end of transactions or business relations with the client in paper form or in electronic media. The storage terms can be additionally extended for a maximum of 2 (two) years;
 - 4.3.4. The storage period of your personal data processed for the purpose of direct marketing (by sending short messages, newsletters) is 2 (two) years from the date of receipt of the relevant data, unless you opt out such processing of your Personal Data before the end of the specified storage period. Upon expiration of the mentioned term or if the person opts out to process Personal Data for the purpose of direct marketing before the end of this term, we will stop processing your data. At the end of this period, we may ask you to renew your consent to direct marketing and/or personal offers;
 - 4.3.5. Data of the project owners:
 - 4.3.5.1. The documents forming the project file (agreements and other documents justifying the fact of the debt, their annexes, communication with the project owner and other documents related to the debt and its security, documents related to the implementation of the project, the use of crowdfunding funds as intended, documents justifying the expenses, etc.) are stored for 10 (ten) years from the date of final and proper settlement;
 - 4.3.5.2. The information, data and documents collected (assessed) during the assessment of the project owner's credibility are stored for 10 (ten) years from the date of conclusion of the last financing transaction by the project owner;
 - 4.3.5.3. The data on real estate, the mortgage of which guarantees the fulfilment of contractual obligations, is stored for 8 (eight) years from the date of conclusion of the last financing transaction of the project owner;

- 4.3.6. The data of requests submitted to the company by phone/email/other electronic or physical means and the data of the persons who submitted the requests are stored for 2 (two) years from the date of submission of the request.
- 4.4. Please note that in certain cases your Personal Data may be stored longer:
 - 4.4.1. If it is necessary to defend ourselves against requirements, claims or lawsuits and to enforce our rights;
 - 4.4.2. If we have reasonable suspicions of illegal activity that is a subject of an investigation;
 - 4.4.3. If Personal data is necessary for the proper resolution of a dispute or complaint;
 - 4.4.4. In case of other grounds provided in legislation.

5. WHO MAY THE COMPANY TRANSFER YOUR PERSONAL DATA TO?

- 5.1. In the course of its activities, the Company may use certain data processors (service providers, for instance, the companies providing data storage services, software development and support companies, companies providing debt administration services, companies providing communication services, etc.). Some of your Personal Data may be transferred to relevant persons, but we ensure that your Personal Data is transferred to relevant persons only in such cases and only to the extent necessary for the provision of their respective services.
- 5.2. By understanding our obligation to process your Personal Data in strict accordance with the applicable requirements, we use only those service providers who have installed/committed to install appropriate technical and organizational security measures and we ensure that the said service providers comply with the appropriate Personal Data protection, security and confidentiality obligations established in the written agreement.
- 5.3. The following persons or institutions may also be the recipients of your Personal Data:
 - 5.3.1. The payment and other service providers and financial institutions whose services the Company uses in the course of its activities, for instance, AB "Mano bankas", Veriff OÜ;
 - 5.3.2. The persons administering joint data files of the debtors (for instance, UAB "Creditinfo Lietuva", UAB "Scorify", etc.);
 - 5.3.3. The state authorities and registers (Bank of Lithuania, Department of Statistics, law enforcement agencies, etc.);
 - 5.3.4. The courts, notaries and bailiffs;
 - 5.3.5. The auditors, law and finance consultants;
 - 5.3.6. If necessary, the companies that intend to buy or would buy the Company's business;
 - 5.3.7. Other third parties related to the provision of the Company's services and/or having a legal basis to receive this data.

6. DOES THE COMPANY TRANSFER YOUR PERSONAL DATA OUTSIDE THE EU/EEA?

- 6.1. It is not necessary to transfer your personal data to recipients located outside the European Union (EU)/European Economic Area (EEA) for the performance of the Company's activities.
- 6.2. However, if in exceptional cases it is necessary to transfer some of your data to a data recipient located outside the EU/EEA, we will take all necessary measures provided for by law to ensure that your Personal Data continues to be properly protected.
- 6.3. Your Personal Data may only be transferred outside the EEA subject to these conditions:

- 6.3.1. The standard contract conditions approved by the European Commission have been signed with the data recipient, or;
- 6.3.2. The data recipient is established in a country for which the European Commission has adopted an eligibility decision, i. e., the data transfer to a data recipient in such country will be treated as data transfer within the European Union, or;
- 6.3.3. Pursuant to provisions of Article 49 of GDPR, you have consented to such transfer of your Personal Data outside the EEA.

7. HOW DO WE GET YOUR PERSONAL DATA?

7.1. We process your Personal Data that:

- 7.1.1. You provide us yourselves;
- 7.1.2. Is submitted by our clients, if you are, for instance, their family member or representative, employee, contractor, founder, member, owner, owner of the mortgaged property, etc. of the client – legal entity;
- 7.1.3. We receive in the documents submitted by the clients, for instance, application - questionnaire, written explanations, payment documents, property valuation documents, purchase and sale and other agreements, insurance documents, court judgments, consents to refinance, etc.;
- 7.1.4. We receive from external sources, for instance:
 - 7.1.4.1. From other financial institutions;
 - 7.1.4.2. From supervision and other state authorities or institutions, for instance, the Bank of Lithuania;
 - 7.1.4.3. From the State Enterprise Centre of Registers (for instance, Population Register, Information system of participants of legal entities (JADIS), Subsystem of beneficiaries of the legal entities (JANGIS), Register of Legal Entities, etc.) and other registers;
 - 7.1.4.4. From the entities administering the joint data files of debtors (for instance, UAB "Creditinfo Lietuva");
 - 7.1.4.5. From law enforcement authorities;
 - 7.1.4.6. From natural persons or legal entities (notaries, bailiffs, lawyers, etc.), when they provide them in compliance with contractual or legal requirements;
- 7.1.5. We receive by monitoring the use of our systems and services.

7.2. The Company can also verify the publicly available information about you to check the data you provided and the transactions concluded, etc.

7.3. Please note that when providing Personal Data to us, you are responsible for the correctness, completeness and relevance of such data. If inaccurate, false or misleading Personal Data is provided, we are entitled to delete such data or limit access to services, etc. If you provide Personal Data about other persons (for instance, your relatives, employees, etc.), you are responsible for the correctness, completeness and relevance of such Personal Data, as well as for such person's consent for their Personal Data to be provided to us. It must be noted that when you provide such data, we may ask you to confirm that you are entitled to provide them. If such a person asks us about receiving his/her Personal Data, we will identify you as the provider of such data.

8. ASSURANCE OF PERSONAL DATA SECURITY

- 8.1. We implement various technical and organizational security measures to ensure the security of your Personal Data and to prevent illegal or accidental destruction, alteration, disclosure, as well as any other unauthorized data processing and to help achieve these goals. These measures include various hardware and software, additional agreements with used service providers, internal rules related to Personal Data Protection and other measures.
- 8.2. The transmission of information via electronic means of communication (e.g., email, mobile phone, etc.) may be less secure in individual cases for reasons beyond our control over the technical or organizational measures chosen by us. Therefore, to ensure the security of your confidential Personal Data, we recommend you not to provide us with information through various less secure and/or electronic systems that are not used by us.

9. THIRD-PARTY WEBSITES, COOKIES USED IN THE COMPANY'S WEBSITE

- 9.1. In our Website, we may provide links to or from the websites of partners, information sources, and related parties. Please note that third-party websites that you access by following links on our Website have their own privacy policies and we are not responsible for these privacy policies. Before submitting any Personal Data to another website, familiarize yourself with that the rules of the website, privacy policy and other information provided on that website.
- 9.2. The Website of the Company uses cookies. More information on how to manage cookies, browser settings or how to delete cookies can be found in our Cookie policy (https://crowdpear.com/wp-content/uploads/2024/08/Cookie_policy.pdf).

10. PERSONAL IDENTIFICATION TOOLS USED BY THE COMPANY

- 10.1. We use the services provided by Veriff OÜ to identify you and confirm your identity. This service provider captures a photo or video of your face and the identity document you provide through a special website with a camera. More information about Veriff OÜ can be found in the [Privacy Policy](#) of this company.
- 10.2. The solution of Veriff OÜ is used to compare live photos or video of your face with your provided ID to comply with legal obligations (for instance, to implement the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and other requirements to prevent fraud and crimes) and risk management obligations.
- 10.3. The result of the face similarity (match or non-match) will be stored for as long as it is necessary to carry out the verification and for the period established by the legislation on the prevention of money laundering and terrorist financing.
- 10.4. The verification of your face similarity is a one-time user authorization by comparing a person's photos with each other based on the data obtained during the verification. Your face template is not created, saved or stored. The original data cannot be recovered from the stored information.
- 10.5. When using the services of Veriff OÜ, the Personal Data is used to determine your identity, as Veriff OÜ compares the image of the person in the identity document and the person captured in the photo. This process allows us to identify you more accurately and the process itself is faster and easier to carry out. If you are not satisfied with this method of identification, you can contact us by email address info@crowdpear.com regarding another identification method.

11. WHAT ARE YOUR RIGHTS AS DATA SUBJECTS?

- 11.1. You have the following rights as data subjects:
 - 11.1.1. **To access your Personal Data and the method of their processing.** You are entitled to receive confirmation as to whether we are processing your Personal Data, as well as the right to access the processed Personal Data and other related information;

- 11.1.2. **To request the correction of incorrect, inaccurate or incomplete data.** If you believe that the information we process about you is inaccurate or incorrect, you are entitled to demand to change, clarify or correct this information;
- 11.1.3. **To demand the deletion of your Personal Data (“the right to be forgotten”).** In certain circumstances specified in legislation (for instance, when the Personal Data is processed illegally, the basis for data processing has disappeared, etc.), you are entitled to request to delete your Personal Data;
- 11.1.4. **To request to limit the processing of your Personal Data.** In case of certain circumstances specified in the legislation (for instance, when Personal data is processed illegally, etc.), you are entitled to request to limit the processing of your personal data;
- 11.1.5. **To request the transfer of your Personal Data to another data controller or provide it directly in a form convenient for you.** In certain cases, you are entitled to transfer the data that we process after receiving your consent and the processing of which is carried out using automated means to another data controller;
- 11.1.6. **To disagree with the processing of Personal Data, if processed on the basis of legitimate interest,** except in cases of legitimate reasons for such processing or the purpose is to assert, enforce or defend legal claims;
- 11.1.7. **To withdraw the given consent to the processing of your Personal Data.** In cases where Personal Data is processed on the basis of separate consent, you are entitled to withdraw your consent to the processing of your Personal Data at any time. In this case, we will stop processing your Personal Data.
- 11.2. Submit the requests regarding the execution of the rights of data subjects in writing by email address info@crowdpear.com. The candidate can also submit the requests about the exercise of his/her rights through the chat window on our website, through the social media accounts we use.
- 11.3. If you believe that your Personal Data is being processed illegally or your rights related to the processing of Personal Data are being violated, please contact us in the methods specified in Clause 11.2. Your requests will be fulfilled or rejected by indicating the reasons for the rejection within 30 (thirty) calendar days from the date of submission of the request. The specified term of 30 (thirty) calendar days can be extended by another 60 (sixty) calendar days with prior notice to you, if the request is related to a large volume of Personal Data. The response to the request will be provided in the same way as received (Clause 11.2), except in cases where a more detailed investigation is required and the response may be provided by email. Having examined your request, we will notify you of the results and the steps we have taken to fulfil your request, or provide you with information of further steps you can take if your request has not been fulfilled or satisfied.
- 11.4. Your request to exercise your rights must meet at least the following minimum requirements:
 - 11.4.1. The request must be written, legible and understandable (the request considered as a written request must be submitted in any of the methods specified in Clause 11.2);
 - 11.4.2. The request must indicate your name, surname, other contact details (email address, phone number);
 - 11.4.3. The request must contain clear and accurate information about which of the said rights and to what extent it is desired to exercise them;
 - 11.4.4. If you wish to exercise your rights through a representative, the request must include the name and surname of the representative, contact details for communication and a document confirming the representation must be attached.
- 11.5. If you contact us with a verbal request to exercise your rights as a Data Subject, we are entitled to ask you to submit a written request and we have the obligation to indicate all possible

methods of submitting a written request and the minimum requirements applicable to the request.

- 11.6. You are also entitled to apply to the [State Data Protection Inspectorate](#), if you believe that your Personal Data is being processed in violation of your rights or legitimate interests arising from relevant legislation. However, before contacting the State Data Protection Inspectorate, we encourage you to contact us immediately. Thus, we will be able to find the most prompt and optimal solution to the problem for both parties.
- 11.7. Please note that the said rights of data subjects may be limited to ensure the prevention, investigation, detection or prosecution of criminal offenses or the enforcement of criminal sanctions, including the protection against threats to public safety and their prevention, public safety, and in the cases of restriction of rights specified in the Article 23 of GDPR.

12. FINAL PROVISIONS

- 12.1. The present Policy was last updated on 22 August 2024.
- 12.2. The Company reserves the right to update the Policy, so it is recommended to review the present Policy regularly to be informed of any amendments.
- 12.3. By making amendments, we will not reduce the scope of your rights under the present Policy or applicable laws of Personal Data Protection. After the update of the Policy, we undertake to publish the updated version of the Policy on our Website. We also provide access to previously valid versions of the Policy on our Website.
- 12.4. The amendments and/or supplements to the Policy take effect after they are published on the Website.