DATA PROCESSING AND STORAGE POLICY

1. GENERAL PROVISIONS

1.1. The present Data processing and storage policy ("**Policy**") of UAB Crowdpear ("**Company**") establishes the internal procedures ensuring the proper processing of personal data and information received from the Company's Clients, fraud prevention and data protection, data storage and archiving methods.

1.2. The Policy has been prepared in accordance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**"), the Law on Legal Protection of Personal Data of the Republic of Lithuania ("**LLPPD**"), Index for the General Documents Storage Period, approved by the Order No. V-100 "Regarding the approval of the Index for the General Documents Storage Period" of the Senior Archivist of Lithuania of 9 March 2011 ("**Index**"), Regulation (ES) 2020/1503 of the European Parliament and of the Council ("**Regulation**") and other legislation applicable to the Company and regulating its activities.

1.3. This Policy applies to all processes and systems of the Company and to all information managed by the Company (in paper and electronic format). This Policy applies to all Company employees, representatives and service providers, whose duties include the data processing in the Company (including the processing of personal data and special personal data) also for the Clients of the Company.

2. DEFINITIONS

2.1. In the present Policy, the capitalized definitions have the meanings provided below, unless the context of their use requires otherwise:

2.1.1. **LLPPD** – the Law on Legal Protection of Personal Data of the Republic of Lithuania;

2.1.2. **GDPR** – the Regulation (EU) 2016/679 of the European Parliament and of the Council 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;

2.1.3. **Company** (Operator) – the operator of the crowdfunding platform UAB Crowdpear, the provider of crowdfunding services UAB Crowdpear, legal entity code 305888586, registered office address Kareivių st. 11B, Vilnius, Lithuania;

2.1.4. **Data Subject** – a natural person whose identity is determined or whose identity can be determined using Personal Data;

2.1.5. **Investor (Lender)** – a natural person or legal person (user) who has submitted an investment (financing) offer through the Platform and who has properly registered on the Platform;

2.1.6. **Client** – the Project Owner or Investor (Lender);

2.1.7. **Platform** – the crowdfunding platform administered by the Operator available at https://crowdpear.com/ through which the Lenders (Investors) provide the crowdfunding funds to the Borrower (Project Owner);

2.1.8. **Policy** – Data processing and storage policy of UAB Crowdpear;

2.1.9. **Project** – the project prepared and published on the Platform to satisfy the business needs, excluding the consumption, for the implementation of which the Project owner seeks to attract the Loan Amount from the Lenders (Investors);

2.1.10. **Project owner** – legal entity or natural person (together – the User) who initiates and publishes the Project through the Platform in order to attract Crowdfunding funds from the Lenders (Investors);

2.1.11. **Regulation** – the Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937;

2.1.12. **Index** – the Index for the General Documents Storage Period, approved by the Order No. V-100 "On approval of the Index for the General Documents Storage Period" of the Senior Archivist of Lithuania on 9 March 2011.

2.2. Other definitions used in the present Policy are understood as they are defined in the Regulation, GDPR, LLPPD, Index or other Company documents, unless the context requires otherwise.

3. DATA PROCESSING AND STORAGE PRINCIPLES

3.1. In processing and storing the personal data, the Company follows principles listed below and other principles established by the GDPR:

3.1.1. **Legality** – data is collected, processed and stored only if obtained legally, i.e. in one of the ways allowed by the GDPR, for example, after obtaining the consent of the Data subject, in the performance of a contract, when data collection is determined by legal acts and in other legal ways. Data is processed only for the purpose of implementing the goals set out in this Policy and established in legal acts;

3.1.2. **Transparency** – information and notices related to the processing of personal data are easily accessible and understandable, presented in clear and simple language;

3.1.3. **Data reduction** – only the data necessary to achieve the set purpose is collected and stored;

3.1.4. **Storage period limitation** – the data is stored no longer than it is necessary;

3.1.5. **Integrity and confidentiality** – the appropriate technical and organizational measures are applied during the data processing to ensure the security of personal data.

4. PURPOSES OF DATA PROCESSING

4.1. Personal data is processed for the following purposes:

Purpose and basis of data processing	Scope of data processing, source, storage periods
For the purpose of providing the crowdfunding services (in accordance with the Regulation and other legal acts) and for the purposes related to the provision of crowdfunding services: • Implementation of money laundering and terrorist financing prevention requirements provided for in the applicable legislation and the Company's internal policies; • Collection of debts owed to the Company or the Company's customers in accordance with concluded contracts; • Implementation of other requirements applicable to the Company's activities.	The Company processes the personal data **of Clients (Investors and Project owners) their representatives and beneficiaries** for the specified purposes: • Personal identification data (name, surname, personal code, personal image, citizenship, etc.); • Contact details (residential address, email address, phone number, etc.); • Data that the client (its representative) uses to log in to the client's account on the Company's website (client user ID, password, etc.); • Financial data (financial obligations, personal credit rating, income, data on property, loans, information about transactions concluded on the Company's platform, their scope, etc.); • Data on the knowledge and experience of the Client (Investor) in the field of investment;

	• Data collected during the reliability assessment of the Project owner; • Data on the progress of the Project realization and documents proving the proper use of the funds provided to the Project owner; • Documents and data related to the property pledged by the Project owner and other security measures provided; • Data on the data subject's relationships with legal entities (position in the represented company, data on a person's participation in the control of legal entities, etc.); • Other data necessary for the purpose of providing the crowdfunding services. The Company receives this personal data directly from Data subject (when Data subject provides personal data) and/or from other sources (for instance, state databases, such as the systems administered by SE "Centre of Registers", etc.). Personal data collected for the purpose of providing crowdfunding services are stored for the terms set out in the table in the Annex, except for cases where legal acts establish longer storage terms for such data.
For the purpose of statistics (in accordance with the Law on Crowdfunding)	The Law on Crowdfunding establishes a requirement for the Company to publish statistical data on the provided crowdfunding services on its website, therefore, personal data of Data subject is processed to implement this requirement: • Information about the number of concluded transactions; • Information about the amount of investments; • Other statistical information required to be processed by legislation applicable to the Company's activities. In all cases, data specified above is processed without leaving the possibility of identifying a specific Data subject, i. e., personal data is depersonalized. The storage period of the relevant personal data depends on the requirements of the applicable legislation regulating the Company's obligation to publish the statistical data.
For the purpose of administration of submitted candidacies for job positions offered by the Company (according to the consent of the Data Subject)	If the Data Subject applies for a job position offered by the Company, the Data Subject submits personal data (e.g. CV, motivation letter) together with the application, which will be processed on the basis of the Data Subject's consent, which the Data Subject expresses by submitting this personal data. Applying for a position, we ask Data subject to comply with at least the minimum data protection requirements. Company asks not to provide redundant information that is not related to the Data Subject's candidacy for current or future selections.

	The term of storage of the above-mentioned data always depends on the duration of the ongoing selection for a specific job position. After the end of this period, the personal data of the Data Subject will continue to be processed only after the Data Subject has given separate consent.
For the purposes of concluding employment contracts and other contracts, fulfilling contractual obligations, accounting	The Company collects and processes the following data for the purposes of concluding employment contracts and agreements, fulfilling contractual obligations, and accounting: • names and surnames of employees; • residential addresses of employees; • birth dates and/or personal identification numbers of employees; • information about the employee's marital status; • employees' bank account numbers to which wages are deposited; • employees' personal telephone numbers, personal e-mail addresses; • Names and surnames, positions and telephone number, e-mail address of clients, business partners' managers, authorized persons, contact persons and/or persons responsible for the fulfilment of contractual obligations, the client (if it is a natural person) or his representative (if it is a legal person)) name, work address, work phone number, work e-mail address.
For the purpose of ensuring suitable working conditions	In order to ensure suitable working conditions, the Company, with the employee's consent, processes information related to the employee's health condition, which directly affects the employee's work functions and the ability to perform them in accordance with the procedure established by legislation.
For the purpose of preparing commercial offers, as well as to ensure the legitimate interest of the Company	For the purpose of preparing commercial offers, as well as in order to ensure the legitimate interest of the Company, the Company collects and processes all necessary data, but not in a larger volume and not longer than is necessary to achieve the goal.
For the purpose of administering requests of Data subject (in accordance with the legitimate interest of the Company or legal obligation applicable to the Company)	When Data subject contacts the Company (by email, telephone, by submitting requests through social network accounts or in any other way), provided personal data will be processed for the purpose of administering the relevant requests. This data is processed to ensure the quality of the provided services, to defend the legitimate interests of the Company and to fulfil the requirements of the applicable legislation; therefore, the basis for processing the relevant data is usually the Company's legitimate interest or the Company's legal obligation. Data subject is required to ensure his/hers compliance with at least the minimum requirements for the protection of personal

	information when making inquiries to the Company – Data subject must not provide excess personal data that is not necessary for the processing of an inquiry, complaint, letter or request. Personal data of Data subject submitted together with requests are stored for up to 3 years, unless the legislation establishes a different storage period or the longer data storage is determined by the need to protect the rights and interests of the Company or other persons.

5. COLLECTION AND PROCESSING OF PERSONAL DATA

5.1. Personal data is processed and provided to the relevant institutions in accordance with GDPR, Regulation, ADTAĮ, the State Social Insurance Law of the Republic of Lithuania, the Personal Income Tax Law of the Republic of Lithuania and other laws and other normative legal acts of the Republic of Lithuania.

5.2. Personal data is obtained directly from the Data Subject or by officially contacting the entities, registers and information systems that process the necessary information and have the right to provide it, after properly informing the Data Subject.

5.3. Personal data has to be processed only by those persons for whom the Personal Data is necessary for the performance of functions, and only when it is necessary to achieve the respective goals and in accordance with the Policy.

5.4. Employees or other Responsible Persons, who have been granted the right to process Personal Data, adhere to the principle of confidentiality and keep secret any information related to Personal Data that they have become familiar with in the performance of their duties, unless such information is public in accordance with the provisions of applicable laws or other legal acts. The obligation to protect the confidentiality of Personal Data also applies in the event of a change of position, termination of the employment or contractual relationship.

6. COLLECTION AND MANAGEMENT SYSTEM OF DATA RELATED TO THE LOAN FINANCING

6.1. Providing crowdfunding services the Company collects and stores the data related to financing transactions concluded through the crowdfunding platform managed by the Company.

6.2. The data related to financing transactions consists of the Personal data specified in the first column of table 4.1, which is collected for the purpose of providing crowdfunding services.

6.3. The Company stores the data specified in the Clause 6.2 of the Policy in electronic format in all cases, but reserves the option to store paper copies of this data, if necessary.

6.4. The Project Owner's file is created in the Company for each Project Owner where the data related to the relevant Project Owner and specified in the Clause 6.2 of the Policy is stored. The Project Owner's file is stored in electronic format and the Company ensures the storage of duplicates of such information on the Company's internal or cloud servers used by the Company.

6.5. The Company is entitled to enter into agreements with the Project Owners, on the basis of which the Project Owners would undertake to collect and store the information on the progress of the Project realization and documents proving the proper use of the funds provided to the Project owner. In such cases, it is expected that at the request of the Company, the Project Owners will provide this information immediately, but in any case, no later than within 10 business days. The

Company stores such information provided by the Project Owners under the conditions provided for in the present Policy.

7. RIGHTS OF THE DATA SUBJECT

7.1. The Company ensures that the rights of the Data Subjects are ensured, properly implemented and that all information is provided correctly, on time and in a form acceptable to the Data Subjects.

7.2. Rights of Data subjects and means of their implementation:

7.2.1. **to know about the collection of his/hers Personal data**. When collecting Personal Data, the Company must inform the Data Subject what Personal Data is collected or what Personal Data the Data Subject must provide, for what purpose the relevant data is collected, to whom and for what purpose data may be provided and what the consequences of not providing Personal Data are;

7.2.2. **get acquainted with his/hers Personal data and find out how the data is processed**. The Data subject has the right to apply to the Company with a request to provide information about what his/hers Personal data and for what purpose is processed. This information is provided free of charge to the Data Subject once a year. If the Data Subject applies more than once a year for the provision of such information, the fee for providing this information cannot exceed the costs of providing such information;

7.2.3. **demand correction, destruction of his/hers Personal Data or stop the processing of his/hers Personal Data**. The Data subject has the right to apply to the Company with a request to destroy his Personal Data or to stop the processing of his Personal Data. The Company assesses the validity, grounds, reasons and legal regulation of such a request and makes a decision on the fulfilling or rejecting the request;

7.2.4. **not to consent to the processing of his/hers Personal Data**. The Data subject has the right not to consent to the processing of his/hers Personal Data in all cases, except for the purposes of data processing established in the GDPR, laws of the Republic of Lithuania or other normative legal acts. Such disagreement can be expressed by not filling out certain sections of the Data Subject's questionnaire or other documents to be filled out, as well as by later submitting a request to terminate the processing of optional Personal Data;

7.2.5. Data subjects have other rights granted to the Data Subject in the GDPR, the Law on Legal Protection of Personal Data and other legal acts regulating the processing of Personal Data.

7.3. The Data subject can submit a request for familiarization with his/hers Personal data, for non-mandatory processing of Personal data or other issues orally, by mail or e-mail. **info@crowdpear.com.**

7.4. Upon receipt of the Data Subject's request, the Company provides the requested data in writing, corrects violations of Personal Data processing or performs other necessary actions no later than within 1 month from the date of receipt of the Data Subject's request. The Company may not provide the requested data to the Data Subject, only in the cases specified in the GDPR, laws of the Republic of Lithuania or other normative legal acts and by submitting a substantiating, reasoned answer.

7.5. The Company, upon receiving a request to terminate the processing of processed non-mandatory Personal Data, immediately conducts an investigation of processing of Personal Data, if the investigation is necessary, and/or immediately terminates such processing, unless it contradicts the requirements of legal acts, and informs the Data Subject thereof.

8. DATA SECURITY MEASURES

8.1. The Company considers the depreciation of data storage and archiving media. If the Company chooses the electronic means of data storage, the Company ensures that procedures and systems will be implemented that would ensure the availability of information during the storage periods, as well as permanent protection against possible unauthorized access, unauthorized data correction, loss or other illegal actions.

8.2. The Company installs and uses the sufficient physical tools for the continuous security of the data processed by the Company.

8.3. The access to the data stored in the Company is granted only to those persons and only to the extent that familiarization with this data and/or other processing of such data is necessary for the proper performance of the work functions of these persons or the provision of services. The employees of the Company and other persons who are granted access to the data stored by the Company must ensure the confidentiality of this data and the secrecy of personal data.

8.4. The specific information and communication technology tools used to process and store data are described in the Operational risk management policy.

9. VIDEO SURVEILLANCE, ACCESS CONTROL

9.1. In order to protect the property and information managed by the Company, video surveillance of the Company's premises, control of access (entrance, passage) to the Company's premises and accumulation of video surveillance and access control data may be carried out.

9.2. Video surveillance tools are installed in such a way that, taking into account the established purpose of video surveillance, surveillance is carried out in no larger part of the Company than is necessary, and no more video data is collected than is necessary for the protection of property and information managed by the Company.

9.3. Data collected by video surveillance devices and access control are stored for the period specified in the Company's internal documents, but no longer than 30 calendar days, except in cases where it is suspected that a criminal act, other violation of the law may have been committed, or property of the Company, employees or third parties was damaged or destroyed.

9.4. Data collected by video surveillance devices and access control is automatically deleted after data's storage period has expired. The data accumulated by the video surveillance tools is deleted during the automatic rewriting of the video. When it is suspected that a criminal act, other violation of the law may have been committed, or the property of the Company, Employees or third parties has been destroyed or damaged, or information has been lost, video surveillance and access control data are stored to the extent required by the purposes of processing this data, and are destroyed manually without delay, when they are no longer needed for their management purposes.

9.5. Only the Responsible Person has the right to process (open, view, make copies and manually delete) data, collected by video surveillance devices and access control.

9.6. Data collected by video surveillance devices and access control can only be used to reveal and investigate suspected criminal acts, other violations of law, violations of work duties, or to determine and prove damage caused to the property of the Company, employees or third parties. In these cases, data collected by video surveillance devices and access control can be transferred only to third parties who have the right to receive this data in accordance with the procedure established by the laws of the Republic of Lithuania.

9.7. The Data Subjects are informed about video surveillance and the collection of video surveillance data in the Company's premises, territories and access points.

9.8. If the Company carries out video surveillance at the Employees' workplaces, these Employees must be informed by signature about such processing of their video data, indicating: for what purposes it is intended to process the video data, to whom and for what purposes it will be provided, also about the right to access their videos.

9.9. All Employees are informed about video surveillance and access control of entrances to the Company's premises in accordance with the procedure established by the Company's internal legal acts.

10. DATA STORAGE TERMS

10.1. Personal data specified in the Company's documents are stored taking into account the rights and obligations set out in the contractual obligations, the implementation deadlines, the requirements of legal acts and the GDPR, the data and document storage terms set out in the legal acts of the Republic of Lithuania.

10.2. Personal data is stored only to the extent and for as long as it is necessary to achieve the set goals.

10.3. When Personal data is no longer needed for the purposes of data processing, data is destroyed, except for data that must be transferred to the archive in cases established by law.

10.4. In the event that the storage term for a specific category of data (or documents) is not established in the applicable legal acts (e.g. Index), this Policy or other documents of the Company, the relevant data (documents) are stored by the Company for no longer than 5 (five) years from of creation or receipt.

10.5. The retention periods given in the Annex to this Policy may be extended, if at least one of the following criteria is met:

10.5.1. data (documents) is used for the protection and defence of the legitimate interests of the Company or other persons;

10.5.2. data (documents) is used as evidence in a civil, administrative or criminal case or data (documents) is transferred to law enforcement authorities until the end of the relevant inspection, investigation or trial or in other cases established by law;

10.5.3. Personal data processed by the Company is anonymized.

11. DATA DESTRUCTION

11.1. The data (documents) stored by the Company (in electronic and paper format) must be regularly reviewed to determine whether the data (documents) storage period specified in legislation or the Policy has not expired. If the data storage period has expired and there are no other reasons to store this data longer (for instance, in the case specified in the Clause 10.5 of the present Policy), such data is destroyed immediately.

11.2. The data (documents) is destroyed with a special document shredder or, if the data is stored in electronic form, data is deleted so that such data can no longer be recovered by reasonable means. An external provider of such services may also be used for data destruction.

11.3. Each person working with such data is directly responsible for the timely and proper destruction of such data.

11.4. The proper destruction of data means that their copies (backup) or historical versions are no longer available.

11.5. The data stored in electronic form cannot be destroyed only if such destruction could harm the integrity, security and management of other data stored in electronic form and as a result the Company would not be able to properly carry out its activities and/or it would breach the requirements set by applicable legislation related to data protection storage.

12. PERSONAL DATA PROCESSING USING A PERSONAL DATA PROCESSOR

12.1. If necessary, the Company may perform Personal Data processing with the help of a Personal Data Processor. In such cases, a written agreement on the processing of Personal data is concluded between the Company, as the controller of Personal data, and the external service provider, as the processor of Personal data. This agreement sets out the subject and duration of Personal data processing, the nature and purpose of data processing, the types of Personal data and Personal data subjects and/or their categories, as well as the obligations and rights of the Personal data manager.

12.2. Before entering into a written agreement with a potential Personal Data Processor, its capabilities to apply the necessary technical and organizational Personal Data Protection measures must be assessed.

13. FINAL PROVISIONS

13.1. The present Policy is approved and/or amended by the order of the Manager of the Company. The Policy or amendments to the Policy enters into force on the day following their adoption, unless another effective date is specified.

13.2. The Manager of the Company reviews and, if necessary, updates the present Policy regularly (at least once a year or when the legislation governing the data processing change).

13.3. The Company's employees are introduced to this Policy and its amendments in accordance with the procedure established by the Company.

DATA STORAGE TERMS

DATA	STORAGE PERIOD
Data of employees and candidates for employees	
Internal legal acts of the Company regarding the employment, transfer, replacement, dismissal, salary, child care leave and parental leave	50 years
Internal legal acts of the Company regarding the annual, unpaid, study and other leave	10 years
Internal legal acts of the Company regarding the business trips, additional days off, reduced working hours	10 years
Documents of personal file (documents or their copies related to the commencement, progress and end of work)	10 years (upon termination of employment or equivalent relationships)
Employment contracts and their annexes (agreements on additional conditions of the employment contract, etc.)	50 years (upon termination of contract)
Accounting documents for employee safety and health training (logs and others)	10 years (from the last entry in the accounting document)
Photos of employees (not classified as personal file documents)	Until the termination of employment (service provision) contract
Electronic communication data of employees (emails, browsing history, etc.)	Until the termination of employment (service provision) contract, except for individual cases when the content of the emails is necessary to ensure the continued operation and processes of the Company (in these cases, the specified data is stored for 2 years after the end of the employment relationship)
Curriculum vitae (CVs) of employee candidates, their motivational letters and other information received regarding the employment by the Company	Until the end of specific recruitment (upon receipt of consent, by the deadline specified in the consent)
Consents regarding the personal data processing	1 year (after the expiration of the storage period of personal data for which the consent was given)
Client data	
Agreements with clients	10 years (after the expiration of agreement)
Client contacts	8 years (from the last use of the Company's services)

Accounting documents confirming the economic transaction or economic event (invoices, payment orders, advance accounting, cash receipt and expense orders, etc.)	10 years
Data of the project owners	
Documents making up 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 guarantee)	10 years (upon final and proper settlement)
Documents related to the Project implementation (documents related to the Project implementation, the use of crowdfunding funds according to their intended purpose, documents justifying the expenses)	2 years (from the date of Project end)
Information, data and documents collected (assessed) during the creditworthiness assessment	10 years (from the date of conclusion of the last financing transaction of the Project Owner)
Data of the real estate, the mortgage of which ensures the fulfilment of obligations under the agreements	8 years (from the date of conclusion of the last financing transaction of the Project Owner)
Data of service providers	
Agreements concluded with the service providers	10 years (after the expiration of agreement)
Contacts of the service providers	5 years (after the expiration of agreement)
Other data	
Data of requests submitted to the Company by phone / email / other electronic or physical means and data of the persons who submitted the requests	3 years
Website visitor data (obtained with the help of cookies, if used)	According to the periods set in the Company's Privacy Policy