DATA RETENTION POLICY OF UAB "TREČIA DIENA"

1. GENERAL PROVISIONS

1.1. This Data Retention Policy ("**Policy"**) of Trečia diena UAB, legal entity code 304211859, registered office at Gynėjų g. 14-120, Vilnius, Republic of Lithuania (**"Company"**), establishes the retention periods for the data (documents) processed in the Company as well as the rules for their destruction.

1.2. The Policy has been prepared in accordance with 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 (**"LPPD"**), the index of general retention periods for documents approved by Order No V-100 of the Chief Archivist of Lithuania of 9 March 2011 ("**Index of Retention** Periods"), Regulation (EU) 2020/1503 ("**FRS**"), as well as other legal acts regulating personal data protection.

1.3. The terms used in the Policy are consistent with the terms used in the GDPR, the LPPD, the Storage Terms Index and other legislation.

1.4. The Policy applies to all processes and systems of the Company and to all information managed by the Company (whether in paper or electronic format). The Policy applies to all employees, agents and service providers of the Company whose duties involve the processing of data held by the Company (including the processing of personal data and sensitive personal data).

1.5. The exact terms of retention of data processed by the Company are set out in the Annex to the Policy, which is an integral part of the Policy.

2. DATA RETENTION PRINCIPLES

2.1. The following principles apply to the protection of personal data:

2.1.1. **data minimisation** - only the data necessary to achieve the stated purpose are collected and stored;

2.1.2. **limitation of the duration of storage** - data shall be stored for no longer than is necessary;

2.1.3. **integrity and confidentiality** - appropriate technical and organisational measures are in place to ensure the security of personal data.

2.2. In the event that the retention period for a specific category of data (or documents) is not set out in the applicable legislation (for example, the Index of Retention Periods), in this Policy, or in other internal procedures of the Company, such data (documents) shall be retained by the Company for 5 years from the date of their creation or receipt.

2.3. The retention periods set out in the Policy may be extended in the following circumstances:

2.3.1. if the data/documents are used to protect and defend the legitimate interests of the Company or other persons;

2.3.2. if the data/documents are used as evidence in a civil, administrative or criminal case, or if the data/documents are handed over to law enforcement authorities before the end of the relevant inspection, investigation or hearing, or in other cases provided for by law;

2.3.3. if the personal data processed by the Company has been anonymised.

3. DATA SECURITY MEASURES

3.1. The Company assesses the depreciation of data storage and archiving media. If electronic means of data storage are chosen, the Company shall ensure that procedures and systems are implemented to ensure the availability of the information for the retention periods, as well as permanent protection against possible unauthorised access, unauthorised modification, loss or other unauthorised actions.

3.2. The Company shall put in place and use sufficient physical measures to ensure the permanent security of the data processed by the Company (e.g. locked cabinets, etc.).

3.3. The Company shall ensure that access to the data stored by the Company is granted only to those persons and only to the extent that access to such data and/or other processing of such data is necessary for the proper performance of their job functions or the provision of services. Employees of the Company and other persons who are granted access to the data stored by the Company are obliged to ensure the confidentiality and secrecy of the personal data.

4. A SYSTEM FOR COLLECTING AND MANAGING DATA RELATING TO LOAN FINANCING

4.1. The Company, as a crowdfunding service provider under the SFR, collects and stores data relating to financing transactions concluded through the crowdfunding platform operated by the Company.

4.2. Data relating to financing transactions comprise:

4.2.1. information collected to identify the Company's customers;

4.2.2. information gathered during the assessment of the project owner's credibility;

4.2.3. the parties to the financing transaction, the date and amount;

4.2.4. information on the progress of the project and documents proving that the funds have been used properly;

4.2.5. documentation relating to the project owner's pledges and other collateral/guarantees provided;

4.2.6. any other relevant information relating to the financing transaction.

4.3. The data referred to in Company Policies point 4.2 shall in all cases be stored in electronic format, but may also store paper copies of such data.

4.4. For each Project Owner, the Company shall maintain a Project Owner File, which shall contain the Policy 4.2 and other data relating to the project owner concerned. The Project Owner's file shall be kept in electronic format and it shall be ensured that duplicates of such information are also stored on the Company's in-house or on trusted cloud servers used by the Company.

4.5. The Company shall have the right to enter into agreements with Project Owners whereby the Project Owners undertake to collect and store the Policy 4.2.4. In such cases, it is foreseen that the project owners will provide this information upon request of the Company without delay, but in any case within 10 working days at the latest. Such information provided by Project Owners shall be retained by the Company in accordance with the procedures set out in the Policy.

5. DELETION OF DATA

5.1. The data stored by the Company, both in electronic and paper format, shall be reviewed regularly to determine whether the retention period set out in the legislation or the Policy has expired. If the said retention period has expired and there is no other reason why the data should be retained for a longer period (e.g., 2.2 of the Policy), such data shall be destroyed immediately.

5.2. Data/documents that do not contain any sensitive information may be destroyed by throwing them in the trash or deleting them from the electronic file. The timely and proper destruction of such data

shall be the direct responsibility of each person working with the data.

5.3. Data/documents containing sensitive or confidential information, including personal data, shall be destroyed by means of a special document shredder or, in the case of data stored in electronic form, erased in such a way that such data can no longer be retrieved. An external service provider may also be used for such destruction.

5.4. The timely and proper destruction of data/documents containing sensitive or confidential information, including personal data, shall be the responsibility of a person designated by the Chief Executive Officer of the Company. The responsible person shall properly document the data destruction process, indicating which categories of data were destroyed, when and by what means.

5.5. Proper destruction of data means that (back-up) copies or historical versions are also no longer available.

5.6. Data stored in electronic form may not be destroyed only if such destruction would compromise the integrity, security and processing of other data stored in electronic form and would prevent the Company from conducting its business and/or would violate the data retention requirements of the applicable law.

6. FINAL PROVISIONS

6.1. This Policy shall enter into force on the date of its approval.

6.2. The policy is reviewed and updated once a year or when there are changes to the legislation governing data processing.

6.3. Employees and other persons shall be made aware of this Policy or any amendments thereto either by signature or by electronic means that ensure access.

DATA RETENTION PERIODS

DATA	STORAGE PERIODS
Staff and applicants for staff	
Company's internal legislation on recruitment, transfer, replacement, dismissal, remuneration, parental leave, parental leave	50 years
Company's internal legislation on annual, unpaid, study and other leave	10 years
Internal company legislation on business trips, additional rest days, reduced working hours	10 years
Personal file (documents or copies of documents relating to the beginning, progress and end of employment)	10 years (after the end of the employment or equivalent relationship)
Employment contracts and their annexes (agreements on additional terms and conditions of employment, etc.)	50 years (after contract expiry)
Records (logbooks, etc.) of occupational safety and health briefings	10 (from the last entry in the accounting document)
Photographs of employees (not part of the personal file)	Until the end of the employment/service contract
Employees' electronic communication data (emails, web browsing history, etc.)	Until the end of the contract of employment (provision of services), except in individual cases where the content of the email is necessary for the continued operation of the Company's activities and processes (in these cases, the data referred to above shall be retained for a period of 2 years after the end of the employment relationship)
CVs, cover letters and other information received from job applicants in order to apply for a job with the Company	Until the end of the specific selection (with consent, until the deadline specified in the consent)
Consents to the processing of personal data	1 year (after the expiry of the retention period of the personal data for which consent was given)
Customer data	
Contracts with customers	10 years (after contract expiry)
Customer contacts	8 years (from the last use of the Company's services)
Accounting documents supporting the economic operation or event (invoices, payment orders, imprest accounts, cash receipts and payment	10 years

orders, etc.)	
Identity documents, documents and information on activities, operations, supporting documents for funds, etc.	8 years (from the date of termination of the transaction or business relationship with the client)
Project owner details for the crowdfunding platform managed by the company	
Documents in the project file (contracts and other documents supporting the debt, their annexes, communications with the project owner and other documents related to the debt and its security)	10 years (after final and proper settlement)
Documentation relating to the implementation of the project (documents relating to the implementation of the project, the use of the crowdfunding funds for their intended purpose, documents justifying the expenditure)	8 years (from the date of project completion)
Information, data and documents collected/assessed in the course of the reputation and creditworthiness assessment	10 years (from the date of the last financing transaction by the project owner)
Real estate mortgaged to secure performance of obligations under the contract	8 years (from the date of the last financing transaction by the project owner)
Details of immovable property mortgaged to secure performance of contractual obligations	8 years (from the date of the last financing transaction by the project owner)
Data from service providers	
Contracts with service providers	10 years (after contract expiry)
Contacts for service providers	5 years (after the end of the contract)
Other data	
Data relating to enquiries made to the Company by telephone/email/other electronic or physical means and the data of the persons making the enquiries	3 years
Website visitor data (collected by cookies, if used)	In accordance with the terms set out in the Company's Privacy Policy

Data not referred to in the table of retention periods above or in other internal procedures of the Company shall be retained for the period set out in the Regulation, the Index of Retention Periods and/or other applicable law.