Last updated on 21 November 2023

RULES FOR THE PROCESSING OF PERSONAL DATA OF BENDRAS FINANSAVIMAS UAB

1. GENERAL PROVISIONS

1.1. The Rules for the Processing of Personal Data (hereinafter referred to as the "**Rules**") shall regulate the actions of Bendras finansavimas UAB, legal entity registration number 303259527, address Latvių g. 36A, Vilnius, Republic of Lithuania (hereinafter referred to as the "**Data Controller**" or the "**Company**") and its employees in collecting, using and storing personal data. The Rules shall be intended for shareholders, persons interested in the Company, its services, prospective and current investors, recipients of consumer credits (loans), persons who visit the website www.gosavy.com (or hereinafter referred to as the "**Website**"), use the Company'' electronic services or otherwise.

1.2. While processing personal data, the Company shall comply with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter referred to as the "**GDPR**").

1.3. These Rules shall be subject to amendments. Please visit the Company's website/mobile application from time to time and read the latest version of the Rules published there.

1.4. The data subject shall be a natural person who intends to commence or has started a business relationship (completed a loan application, registered on the Company's website to invest in loans, acquired the Company's shares, concluded a service provision agreement with the Company) with the Data Controller, or the business relationship has expired, however, the Dat a Controller shall process the Data Subject's data in accordance with the provisions of the legislation (hereinafter referred to as the "**Data Subject**" or the "**Consumer**").

1.5. The Rules must be observed by all persons employed by the Company under employment contracts who process personal data in the Company or become aware of them in the performance of their duties, and other persons providing services on a contractual basis who can process personal data.

1.6. The Data Controller shall ensure that it complies with the following fundamental principles of data protection and shall

1.6.1. collect personal data of the Data Subject for the defined purposes ("purpose");

1.6.2. process personal data of the Data Subject in a lawful, fair and transparent manner ("lawfulness, fairness and transparency");

1.6.3. the personal data of the Data Subject must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

1.6.4. personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");

1.6.5. the personal data of the Data Subject shall be kept for no longer than is necessary for the purposes of data processing and the legislation ("storage limitation");

1.6.6. the personal data of the Data Subject must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality");

1.6.7. The Data Controller shall be responsible for, and be able to demonstrate compliance with the

above principles ("accountability").

1.7. These Rules shall apply to the relationship between the Data Controller and the Data Subjects that use, used, indicated their intention to use, or are otherwise related to the services provided by the Company, their relationship, including the relationship with the Data Subjects before the entry into force of these Rules.

2. PURPOSE, SCOPE, LEGAL BASIS AND PERIODS FOR THE PROCESSING OF PERSONAL DATA

Data Subject	Purpose of data processing	Data processed	Legal basis	Period
Receivers of credit[1]/loan; shareholders, manager, beneficiaries of receivers of loans; spouses of receivers of credit; guarantors, issuers of promissory notes, collateral providers, investors.	Identification.	Name, surname, personal identification number, details of identity documents (photo, state, citizenship, document number, series, type of document, date of issue/expiry, issuing authority, signature), address of the place of residence, country of birth, gender, identification level (in case of investors), live video (live video streaming) recording, personal photo, video start and end time, face and identity document match result, details of qualified electronic signature certificate Security code for identification of the person, bank account number, IP address, details of the browser, publication of a search for a person, documents supporting representation (where the customer is a legal person), other data obtained during the customer identification.	We are legally bound (Article 6(1)(c) of the GDPR); In cases where biometric data are collected, the Company shall also follow Article 9(2)(f) of the GDPR, i.e. seek to meet the legal requirements applicable to the Company (Law on the Prevention of Money Laundering and Terrorist Financing).	The data of recipients of credit/loan/ spouses and other related persons shall be stored from the date of completion of an application and 10 years from the last date of completion of the contract between the Company, recipient of credit/loan and investor or 6 from the refusal to provide the financial service; Data of investors shall be stored from the date of registration on the Company's Website/mobile application and 10 years from the last day of completion of the contract between the Company, recipient of loan/credit and investor; if the investor does

[1]The term "credits" used throughout the text must be understood as consumer credits and credits pledged against real property.

				not conclude contracts, data shall be stored for 6 years from the date of registration. If the Company refuses to enter into a transaction due to the implementation of measures to prevent money laundering and terrorist financing, personal data shall be stored for 8 years from the date of such refusal in compliance with the Republic of Lithuania Law on the Prevention of Money Laundering and Terrorist Financing.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Receivers of credit/loan; shareholders, beneficiaries, manager of receivers of loans; guarantors, issuers of promissory notes, collateral providers, investors.	Prevention of money laundering and terrorist financing.	Name, surname, personal identification number, date of birth, address of registration, address of residence, citizenship, e-mail address, telephone number, number of shareholders (beneficiaries), object of investment, planned amount of investment, received average monthly income, main source of funds, beneficial owner of funds, documentation concerning accounts and/or contracts, correspondence of business relationship with the customer, documents	We are legally bound (Article 6(1)(c) of the GDPR); We seek to comply with the legal requirements applicable to the Company (Article 9(2)(f) of the GDPR).	The data of recipients of credit(loan) and other related persons shall be stored from the date of submission of an application and 10 years from the last day of completion of the contract between the Company, recipient of credit/loan and investor or 6 from the refusal to provide the financial service;

		evidencing the monetary operation or transaction and other documents with legal force and data relation to performance of monetary operations or conclusion of transactions, IP address, verifications in public and reliable registers, other data obtained from the customer or provided in the Know Your Customer questionnaire. Data on the consumer's participation in political activities, inclusion in the list of sanctions.		Data of investors shall be stored from the date of registration on the Company's Website/mobile application and 10 years from the last day of completion of the contract between the Company, recipient of loan/credit and investor; if the investor does not conclude contracts, data shall be stored for 6 years from the date of registration; If the Company refuses to enter into a transaction with you due to implementation of money laundering and terrorist financing prevention measures, personal data shall be stored for 8 years from the date of such refusal in compliance with the Republic of Lithuania Law on the Prevention of Money Laundering and Terrorist Financing.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Receivers of credit/loan;	Creditworthiness /solvency	Name, surname, personal identification number,	We are legally bound (Article	The data shall be stored from the

shareholders, manager of receivers of loans; guarantors, issuers of promissory notes, collateral providers.	assessment.	place of the registered place of residence, date of registration at the respective address, citizenship, marital status, name, surname, personal identification number of the spouse, number of minor children and dependents, receive income, evidence of income, employer, workplace, duration of receipt of income, total length of service, start/end date of employment relationship, area of work (activity), bank account statement, own real property and movable property, property rights and their restrictions, existing and former financial obligations and their data, credit rating, information on registration in the information system "List of Persons Regarding Whom Requests Not to Allow Them to Conclude Consumer Credit Agreements Have Been Submitted", data from bailiffs' information system on the enforcement cases, data from the register of incapacitated persons, other data necessary for proper creditworthiness assessment.	6(1)(c) of the GDPR); We conclude and perform a financial services agreement with you (Article 6(1)(b) of the GDPR).	date of completion of an application and 10 years from the last day of completion of the contract between the Company, recipient of credit/loan and investor or 6 from the refusal to provide the financial service;
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Recipients of credits/loans.	Conclusion and performance of credit/loan contracts with recipients of credit/loan.	Name, surname, personal identification number, place of residence, telephone number, e-mail address, bank account No, purpose of the credit/loan, amount of the credit/loan, where funds are provided	We conclude and perform a financial services agreement with you (Article 6(1)(b) of the GDPR).	The data shall be stored for the term of the contract and for 10 years from the termination of the contract and/or the

		for refinancing, details of the refinanced credit, date, time of conclusion of the credit/loan contract, contract No, physical or electronic signature, IP address, name, surname, position and physical or electronic signature of the representative (in case of legal persons).		fulfilment of the obligations under the contract.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Recipients of loans (owners of crowdfunding projects).	Assessment of reliability of the owners of crowdfunding projects and use of funds.	Certificate of conviction (non-conviction), other significant information to assess reputation, evidence of the use of funds.	We are legally bound (Article 6(1)(c) of the GDPR); We seek to comply with the legal requirements applicable to the Company (Article 9(2)(f) of the GDPR).	The data shall be stored from the date of completion of an application and 10 years from the last day of completion of the contract.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Investuotors.	Testing of investment experience and knowledge and loss modelling.	Name, surname, age, education, data on income, savings, liabilities, investment experience, data on the net asset value.	We are legally bound (Article 6(1)(c) of the GDPR).	The data of testing of investment experience and knowledge and loss modelling (if provided) shall be stored for 6 years from the date of provision thereof.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Recipients of credit/loan, guarantors, issuers of promissory notes, collateral providers.	Debt recovery and administration.	Name, surname, personal identification number, date of birth, place of residence (address), telephone number, e-mail, amount of the debt, duration of delay, due date, data necessary for evaluation of the debt solvency, performance securities.	Legitimate interest of the Data Controller and third parties (investors) to ensure performance of obligations (Article 6(1)(f) of the GDPR); and the data	The data shall be stored during the term of the contract and 10 years from the end of performance of the contractual relations and/or obligations, debt recovery or

		In order to properly evaluate the debtor's solvency and administer the debt recovery process, we may process the debtors' health data in order to create suitable conditions for the debtor to fulfil the obligation and/or defer the payment of the debt in the event of the debtor's illness.	subject's consent (Article 9(2)(a) of the GDPR). (debtors' health data shall be processed on the afore-mentioned basis); We conclude and perform a financial services agreement with you (Article 6(1)(b) of the GDPR).	obtaining a certificate that recovery of the debt is impossible.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Recipients of credit/loan.	Provision of information on a recipient of credit/loan to investors.	Crediting rating, number assigned in the system of the recipient of credit/loan, amount of the credit/loan, term of the credit/loan, purpose of the credit/loan, solvency information (main source of income, received income, assumed financial obligations and types of obligations, length of service, area of operational activity, debt history), gender, age, place of residence (city), marital status, joint family obligations and joint income (if a loan not for personal needs is taken), number of dependents), owned assets, level of education, due date.	Legitimate interest of the Data Controller and third parties to disclose sufficient information to the recipient of credit and investor in accordance with Article 25 of the Republic of Lithuania Law on Consumer Credit (Article 6(1)(f) of the GDPR).	The data shall be stored during the term of the contract and for 10 years from the termination of the contract and fulfilment of obligations under the contract.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**

Recipients of credit/loan (including prospective) (shareholders, beneficiaries, manager); Spouses; guarantors, issuers of promissory notes, collateral providers (including prospective).	Compliance with the requirements of laws and concluded contracts, including for internal administration purposes.	In case of the recipient of a credit/loan, the name, surname, registered place of residence (in case of a legal person, name, legal form, address of the registered office, registration number, name, surname, personal identification number, e-mail, telephone number of the manager or authorised person, telephone number, e-mail address, customer number, age, credit/loan contract number, date of conclusion of the contract, date of termination, date of transfer and recovery by the debt collection company, purpose, amount of the credit/loan, credit/loan repayment schedule, date of repayment, date of completion of the application and date, time of the last login, login data (connecting with a password – selected e-mail address) shall be processed. In case of investors, the name, surname, personal identification number, telephone number, e-mail, login data, investor's identification number, Paysera wallet number, active/inactive status, date and time of the last login, login data (when logging though Facebook account –e-mail address); history of transfers made inside SAVY, data of	Conclusion and performance of the contract (Article 6(1)(b) of the GDPR); We have a legitimate interest (to ensure proper performance of the contractual obligations) (Article 6(1)(f) of the GDPR).	The data of the investors shall be stored from the registration on the Company's Website/mobile application and for 10 years from the date of full completion of the credit (loan) contract; if the investor does not conclude contract, the data shall be stored for 6 years from the date of registration; the data of recipients of credit(loan) and other related persons shall be stored shall be stored from the date of submission of an application and 10 years from the last date of completion of the contract or for 6 years in case of refusal to provide the financial service.

		investments shall be stored.		
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**

Recipients of credit/loan (including prospective); investors (including prospective).	Ensuring the quality of provision of the services.	Name, surname, telephone number, date, start and end time of conversation, conversation recording. **IMPORTANT:** We shall record only the conversations which take place when addressing the company by telephone numbers: +370 (5) 272 0151, +370 (5) 216 0499, +370 6 610 5523, +442 0 3769 3039, and shall record the conversations when we address you by the afore-mentioned telephone numbers.	We have a legitimate interest (to ensure the quality of customer service, collect evidence for a dispute should it arise) (Article 6(1)(f) of the GDPR); Conclusion and performance of the contract (Article 6(1)(b) of the GDPR); Consent (Article 6(1)(a) of the GDPR).	Data shall be stored for 999 days from the date of recording of the telephone conversation. **IMPORTANT:** when there is reason to believe that a crime or other illegal actions are recorded in the conversation recording material, the necessary conversation recording data shall be transferred to secure media and stored for as long as there is an objective need, even after the expiration of the conversation recording storage period specified in this point.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Recipients of credit/loan (including prospective), their shareholders, manager); investors (including prospective); or other entities addressing with inquiries.	For the purposes of administration of inquiries sent by the Company by post including but not limited to complaints, requests or for the purposes of solving any problems of interested parties.	Name, surname, e-mail, date, time of submission/response, Content of inquiries/notifications/ responses.	Conclusion and performance of the contract (Article 6(1)(b) of the GDPR); We have a legitimate interest (to properly provide financial services, prevent	The data shall be stored for 6 years from the date of application. If a credit (loan) contract is concluded, the data shall be stored for 10 years from the date of conclusion of the credit/loan contract.

			provision of false data, fraud and ensure provision of such evidence to the respective authorities (the Financial Crime investigation Service, the Bank of Lithuania etc.) (Article 6(1)(f) of the GDPR).	
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Recipients of credit/loan (including prospective); investors (including prospective); other visitors of the website.	Ensuring smooth and secure operation, security of the Website/mobile application and access to services.	IP address, information on the browser and device.	Consent (Article 6(1)(a) of the GDPR); We have a legitimate interest to ensure the security of the Company's Website (Article 6(1)(f) of the GDPR).	Not more than 6 years from visiting the Company's Website/mobile application.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Investors.	Transfer of investors' mandatory fees to the State budget.	Personal data of investors (natural persons who granted loans): name, surname, personal identification number, date of birth, place of residence (address), permanent/non-permanent resident status of the Republic of Lithuania, amount of interest, amount of taxes.	Conclusion and performance of the contract (Article 6(1)(b) of the GDPR); We are legally bound (Article 6(1)(c) of the GDPR);	Data of investors shall be protected from the date of registration on the Company's Website / mobile application and 10 years after the last day of completion of the contract.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Recipients of credit/loan (including	Direct marketing.	Name, surname, e-mail address, telephone number, address.	Consent (Article 6(1)(a) of the GDPR); Article	The data of recipients of credit/loan shall

prospective); investors (including prospective).		In order to provide personal proposals to the customer, the Company shall use profiling by applying specific algorithms, it shall analyse the personal data provided by you. These actions do not have any legal or similar significant effect on the Customer.	69(1) of the Law on Electronic Communications); You purchased services from the Company Article 69(2) of the Law on Electronic Communications).	be stored from the date of giving the consent and 6 years from the last day of completion of the credit/loan contract, except for the cases where the Data Subject wishes to extend the term. If no credit(loan) contract is concluded, data shall be stored for 6 years from the date of receipt of the consent except for the cases if the Data Subject wishes to extent the term. In case of investors, data shall be stored for 6 years from the date of receipt of the consent, except for the cases if the Data Subject wishes to extend the term.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Investors.	For the purposes of concluding transactions, performing the function of an intermediary and providing financial services.	Name, surname, personal identification number, date of birth, citizenship, address, e-mail, telephone number, gender, IP address, level of identification level, unique Paysera account No which must be linked to the SAVY investor account, the balance of the linked account; investment	Conclusion and performance of the contract (Article 6(1)(b) of the GDPR).	The data shall be stored from the date of registration on the Company's Website/mobile application and 10 years from the last day of completion of the contract between the Company, if the

		data (Invested amount, earned interest earned and late fees, amount of outstanding investments, investment statuses (fully settled / overdue etc.)) and other data related to investments and available on the investor's account.		investor does not conclude contracts, data shall be stored for 6 years from the date of registration.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Persons submitting enquiries.	Communication with the Company through Olark.	IP address, if specified - name and e-mail, rating of the conversation, other information provided in the inquiry.	Consent (Article 6(1)(a) of the GDPR); (Olark).	The data shall be stored for 30 days from the date of submission of the enquiry.
Data Subject	**Purpose of data processing**	**Data processed**	**Legal basis**	**Period**
Partners of the Company and their representatives	Maintenance and development of business relations with partners.	Name, surname, position, workplace, address, telephone number, e-mail address, physical or electronic signature.	We have a legitimate interest in maintaining business relationships and administering contact information (Article 6(1)(f) of the GDPR).	During the term of the contract and 10 years from the end of relations with business partners.

The Company may process personal data of the Data Subjects for other purposes in accordance with the GDPR, and in accordance with the requirements and procedure of the Republic of Lithuania Law on Legal Protection of Personal Data of the Republic of Lithuania.

3. PROVISION AND RECEIPT OF PERSONAL DATA

3.1. The Data Controller shall be entitled to provide personal data processed for specified and legitimate purposes to the following third parties:

- personal data processors selected by the Company for the purpose of lawful processing of personal data on behalf of and/or at the instructions of the Company;
- investors, as the credit (loan) contract is concluded between the Company's investors;
- in the event of a breach of the terms and conditions of the contract concluded between the Data Subject and the Company, to third parties through which the rights and legitimate interests of the Company shall be safeguarded and protected;
- to third parties whose activities are related to debt collection, administration or use, with the aim of administering the Data Subject's debt and/or collecting the Data Subject's indebtedness to the Company;

- in case you express a wish to conclude a financial liability insurance contract, we shall transfer data (name, surname, personal identification number, telephone number, e-mail address, address of the place of residence, amount of the loan, amount of the instalment, information about personal property) for the conclusion and performance of insurance contracts for the afore-mentioned purpose to the insurance company Compensa Vienna Insurance Group ADB and the insurance intermediaries Inpacto UADBB;
- other persons (attorneys-at-law, consultants, auditors, companies developing IT systems, ensuring or supervising their operation or persons, etc.) that the Company uses to provide services necessary for the Company and/or the Data Subject;
- state institutions and bodies, other persons performing functions assigned to them by law (for example, supervisory authorities, law enforcement agencies, bailiffs, notaries, financial crime investigation bodies, etc.);
- persons who have provided performance securities (guarantors, collateral providers, issuers of promissory notes);
- companies or individuals providing direct marketing services;
- Information systems INFOBANKAS and KREDITŲ BIURAS administered by Creditinfo Lietuva UAB (the spouses' data shall also be transferred, if necessary);
- Paysera LT UAB;
- the Bank of Lithuania and other supervisory authorities;
- the Loan Risk Database administered by the Bank of Lithuania;
- the State Social Insurance Fund Board under the Ministry of Social Security and Labour;
- the State Tax Inspectorate;
- the Financial Crime Investigation Service;
- State Enterprise Centre of Registers;
- pre-trial data collection companies;
- DPD Lietuva UAB;
- Lietuvos pastas AB;
- Facebook Ireland Ltd;
- Ondato UAB;
- KiwiCONTACT MB;
- GoCardless SAS;
- Amlyze UAB;
- Compensa Vienna Insurance Group ADB and the insurance brokers Inpacto UADBB;
- after the Data Subject gives his consent, the Company may also transfer personal data to its partners who may contact and submit an alternative loan or credit offer to the Data Subject;
- if necessary, in case of restructuring of the Company or insolvency (bankruptcy) of the Company, data may also be transferred to other entities that would administer the Company's loan portfolio (including other credit companies in case of portfolio transfer/sale);
- if necessary – to companies or persons that intend to purchase or would purchase the Company's business;
- if necessary, to companies or persons to whom the rights, obligations and debts of the Company could be or would be transferred;
- other third parties having a legal basis for receiving the data.

3.2. The personal data of the Data Subject may be provided to third parties in the following ways: in writing, by electronic means of communication, by access to separate databases or information systems collecting

data or by other means agreed by the personal data controllers.

3.3. The personal data shall be obtained directly from the Customer when applying to the Company, filling the applications, requests or submitting other documents to the Company. Personal data of the Data Subject may also be obtained from the Bank of Lithuania; commercial banks; Paysera LT; State Social Insurance Fund Board; State Enterprise Centre of Registers (the Population Register, the Register of Property Seizure Acts, the Register of Contracts and Restrictions of Rights, the Real Property Cadastre and Register, the Register of Legal Entities, the Information System for Participants of Legal Entities, sub-system of beneficial owners, the Bailiffs Information System, etc.); other administrators of state and departmental registers: register of wanted persons, register of invalid documents; information systems INFOBANKAS and KREDITŲ BIURAS administered by Scorify UAB, Creditinfo Lietuva UAB if such data are necessary to make decision on credit rating, credit granting and loan management, subjects providing the services of personal identification, social media accounts linked to Company's system, etc.

3.4. Furthermore, we shall inform that if the Customer (recipient of credit) is late in fulfilling his obligations for more than 40 days, the Organiser may provide information about the identity of the Customer (recipient of credit), contact details and credit history, i.e., financial and property obligations and their execution, debts and payment of debts, to Credit Bureau Creditinfo Lietuva UAB (registration number: 111689163 address: A. Goštauto g. 40A, LT 01112 Vilnius, Lithuania, www.manocreditinfo.lt, tel.: (8 5) 2394131) and Scorify UAB (registration number: 302423183, address: Olimpiečių g. 1A-24 Vilnius, Lithuania, www.scorify.ai, tel.: +370 676 48676) for the purposes of debt and solvency management by giving a prior notice to the Customer (recipient of credit). The credit bureau Creditinfo Lietuva UAB and Scorify UAB shall process and provide information of the Customer (recipient of credit) to third parties (financial institutions, telecommunication companies, insurance companies, electricity and utility providers, trade companies, etc.) in pursuit of legitimate interests and objectives, i.e. to assess the creditworthiness and manage the debt. For the purposes of the creditworthiness assessment, the personal properties assessment by shall be carried out automatically (profiling); it may have an influence to possibility of the Customer (recipient of credit) to enter into transactions in the future. The assessment by automated means shall help to lend in a responsible manner, assess the information provided by the person, the credit history, public information, etc. Automatic assessment methods shall be reviewed regularly to ensure their fairness, efficiency and impartiality. The credit history data shall be processed 10 years from the performance of obligations. The Customer (recipient of credit) may get acquainted with his credit history by addressing directly Creditinfo Lietuva UAB or Scorify UAB (depending on which company has questions/requests/complaints). The Customer (recipient of credit) shall also have the right to request to correct or delete personal data, restrict their processing and the right to object to the processing of data, request for human intervention in automatic decision making, express own view and challenge the decision, as well as right to data portability. More information about exercise of the afore-mentioned rights, restrictions and automatic properties assessment (profiling) shall be provided at www.manocreditinfo.lt and www.scorify.ai. If the rights of the Customer (recipient of credit) are violated, you may apply to Data Protection Officer by e-mail (to contact Creditinfo Lietuva UAB) or duomenu.apsauga@scorify.ai (to contact Scorify UAB) or BY the previously indicated telephone numbers or to file a complaint with the State Data Protection Inspectorate or the court.

4. PROFILING AND AUTOMATED DECISION-MAKING

4.1. Profiling may be carried out by combining and grouping personal data obtained, i.e. it shall consist of any form of automated processing of personal data that results from the use of personal data for the purpose of assessing specific aspects related to the Consumer, in particular, by analysing or predicting creditworthiness aspects (including the fact that a person's creditworthiness rating may be formed and

provided to a you, on which the terms of the proposed consumer credit/loan may depend); profiling may be carried out in order to implement the requirements set out in the legal acts applicable to the Company (e.g. risk assessment in compliance with the requirements of legal acts of the Republic of Lithuania for the prevention of money laundering and terrorist financing); for direct marketing purposes on the basis of the consent of the data subjects or for other purposes related to the Company's legitimate interests, performance of the statutory obligations and performance of the contract concluded with the Customer.

4.2. In order to achieve the objectives set out in the Rules, such as providing your credit rating, submitting a credit/loan offer, implementing the requirements of the Republic of Lithuania Law on the Prevention of Money Laundering and Terrorist Financing, we may analyse personal data automatically, make automated decisions, divide data subjects into groups, after evaluating with data personal aspects related to subjects. We shall carry out automated decision-making, including profiling, in accordance with your consent, in order to conclude a contract with you or perform it, fulfil the requirements set by legal acts (accordingly, Article 6(1)(a), Article 6(1)(b), Article 6(1)(c), Article 22(2) of the GDPR).

4.3. In the case where the relevant decision is made only by automated means, the Customer shall have the right to request to review the decision by human intervention, as well as the right to express his point of view, obtain an explanation of the decision made following that assessment, and have the right to challenge that decision.

5. DIRECT MARKETING

5.1. By using the services provided by the Company, the Data Subject may freely agree to the use of the personal data provided by the Data Subject for marketing purposes of the Company and express his consent in the relevant column of the credit/loan application or, in the case of investors, by registering on the SAVY website, marking with a tick.

5.2. The Data Subject may exercise his right to refuse processing of his data for the purposes of direct marketing, including profiling, and may inform the Company in the following ways:

- by telephone +370 (5) 272 0151;
- by e-mail: labas@savy.lt / dap@savy.lt;
- by clicking "Unsubscribed" at the bottom of the newsletter;
- by logging in to your SAVY account and selecting "ACCOUNT" and "UPDATE INFORMATION".

5.3. The Company shall use the Data Subject's data for marketing activities permitted by law. For example, based on the information provided by the Data Subject, when the Data Subject visits the website www.gosavy.com, browses through third party websites and social networks, proposals tailored to the Data Subject may be displayed.

5.4. The Data Subject's e-mail as well as anonymised information about him may be provided to third parties who provide marketing services through online search engines, social networks, etc. Such third parties shall have their own privacy policies and the Data Subject may at any time disagree with the processing of his data in accordance with the third parties' privacy policies.

6. USE OF COOKIES

6.1. When you visit and browse our Company's Website, cookies shall be used. Cookies shall small text files (up to several KB) that your browser places on your computer, tablet or other smart device when visiting the Company's website. With cookies, the Company shall seek to ensure efficient and safe operation of the website and analyse your habits so that the operation of the website is convenient, effective and meets your needs and expectations.

6.2. For more information on cookies used on the Company's website, please see our Cookies Policy.

7. RIGHTS OF THE DATA SUBJECT

7.1. The rights of the Data Subject guaranteed by legislation relating to the processing of his personal data shall include the following rights:

7.1.1. the right to access personal data processed by the Company and to receive information from which sources and what personal data have been collected, for what purpose they are processed and to whom they are provided;

7.1.2. the right to request for rectification, destruction of personal data or limitation of the processing of his personal data, with the exception of storage, where the data are processed not in accordance with the GDPR or other statutory provisions;

7.1.3. the right to object, without giving reasons, to his personal data being processed for direct marketing purposes or for other purposes for which his consent is requested;

7.1.4. the right to object to application of processing of data by automated means only, including profiling;

7.1.5. the right to exercise his right to data portability;

7.1.6. the right to exercise the right to be "forgotten";

7.1.7. the right to lodge a complaint against the actions of the Company as a data controller to the State Data Protection Inspectorate of the Republic of Lithuania (hereinafter referred to as the "**Inspectorate**") (address of the website www.ada.lt, address of the registered office: L. Sapiegos st. 17, Vilnius, tel. (8-5) 279 1445) .

7.2. The Data Subject shall have the right to apply to the Company with a complaint/request regarding the actions of the Company as a data controller. The Data Subject may submit a complaint/request to the Company by e-mail dap@savy.lt. In case of disagreement with the Company's response, the Data Subject may apply to the Inspectorate. The actions (omissions) of the Data Controller may be complained to the Inspectorate within three months from the date of receipt of the response from the Data Controller or within three months from the date on which the deadline of thirty calendar days to reply expires.

7.3. The Company shall adjust, correct and update personal data on the initiative of the person whose data is being processed. Employees of the Company may correct the Data Subject's data if the data provided by the Data Subject contain grammatical errors.

7.4. The Data Controller shall have the right to refuse to allow (giving reasons) the Data Subject to exercise his rights or to charge a reasonable fee under the circumstances provided for in Article 12(5) of the GDPR.

8. TERRITORY OF PROCESSING OF THE CUSTOMER'S PERSONAL DATA

8.1. Customer's personal data shall be processed within the territory of European Union/European Economic Area (EU/EEA) but in some cases they may be transmitted and processed beyond the borders of the EU/EEE. If the Company transfers the Customer's personal data to such persons, the Company shall take all measures provided for in legal acts in order to ensure the security of the Customer's data.

9. SECURITY OF PERSONAL DATA

9.1. The organisational and technical data security measures implemented by the Data Controller shall ensure such level of security that is consistent with the nature of the data controlled by the Data Controller and the risks associated with its processing, including, but not limited to, those specified in this Section.

9.2. The Company shall provide hardware and software protection services (administration of information systems and databases, maintenance of workstations, protection of operating systems, monitoring of user access, protection against computer viruses, etc.).

9.3. The Company shall apply administrative security measures (secure document and computer data processing, personnel training, etc.).
9.4. Employees shall have the right to collect, manage, transmit, store, delete or otherwise use personal data only by performing their own direct functions and only in accordance with the procedure established in the law.
9.5. Employees of the Data Controller must observe the principle of confidentiality and keep confidential any information relating to personal data with which they have become aware in the course of their duties, unless such information is public in accordance with applicable laws or regulations.
9.6. Logins to the database of persons authorised to process personal data shall be recorded.
9.7. Personal data contained on laptops if used outside the data transmission network of the Data Controller are protected by appropriate means consistent with the risk of data processing.
9.8. Employees shall be granted access to personal data only to the extent necessary for the proper performance of their duties and for the performance of their functions.
9.9. Employees who automatically process personal data or from which computers the local network area can be accessed where personal data are stored must use passwords. Passwords must be changed periodically (at least every 3 (three) months), as well as under certain circumstances (for example, in case of a change of an employee, a threat of burglary, a suspicion that the password has become known to third parties, etc.). An employee working with the particular computer may only know his/her password. An employee loses the right to process personal data when an employee's employment or similar contract with the Company expires or when the head of the Company cancels the employee's appointment to process personal data.
9.10. Backups of personal data shall be made and stored elsewhere than the active database, and the lost data shall be restored from backups. This procedure shall described in detail in the Business Continuity Plan.
9.11. Employees who have noticed violations of personal data security, signs of criminal activity, and non-functioning measures of personal data security must immediately inform about it the head of the Company.
9.12. Having assessed the factors of risk of data breach, the degree, damage, and consequences of violation, the Data Controller shall take decisions based on relevant internal procedures on the measures necessary to eliminate the data breach and its consequences and inform the required entities.
9.13. The premises where the personal data shall be stored must be secured (only authorised persons shall have access to the relevant premises, the alarm system shall be installed in the premises, etc.).

10. LIABILITY

10.1. The Data Subject must provide the Company with complete and correct personal data of the Data Subject and inform about the relevant changes in the Data Subject's personal data.
10.2. The Company shall not be liable for any damage caused to the Data Subject and/or third parties if the Data Subject has provided incorrect and/or incomplete personal data or failed to inform about the changes.
10.3. The Data Subject shall warrant that all data provided while using the Company's services are correct.
10.4. The Data Subject who provided false information should be liable for damage caused by such information to the Company and/or other users as well as investors, including, but not limited to, cases where other users enter into an agreement with a Data Subject who provided such false information on the assumption that such information is correct.
10.5. The Company shall not be in a position to fully guarantee that the functioning of the Website/mobile application shall be uninterrupted and free from any malfunction or error, that Website/mobile

application shall be completely protected from viruses or other harmful components. The Data Subject is informed that any material that the Data Subject reads, downloads or otherwise accesses through the Company's website is exclusively obtained at the Data Subject's discretion and risk, and only the Data Subject is liable for any damage to the Data Subject and the computer system of the Data Subject.

10.6. If the Data Subject shall be a registered user of the Website/mobile application, the Data Subject shall assume all the risk and responsibility for third party actions performed on the Website/mobile application using the Data Subject's login data, and undertakes to fulfil all obligations undertaken using the Data Subject's access data, except where the Company has failed to fulfil its obligations properly.

11. FINAL PROVISIONS

11.1. Data Subjects shall access these Rules at https://gosavy.com/privatumo-politika/.

11.2. These Rules may be reviewed at least once every six months on the initiative of the Data Controller and/or in the event of amendment of legislation governing the processing of personal data.

11.3. The Data Controller shall have the right to change the Rules in full or in part.

11.4. Any supplements or amendments to the Rules shall come into force from the date of their publication on the Company's Website/mobile application.

11.5. If the Data Subject continues to use Website/mobile application and/or services provided by the Data Controller after supplement or amendment of the Rules, the Data Subject shall be deemed not to have objected to such supplements and/or amendments.

11.6. All disagreements arising from the implementation of these Rules shall be settled by negotiation. In case of a failure to reach an agreement, disputes shall be settled in accordance with the procedure established by legal acts of the Republic of Lithuania.

Should you have any questions related to these Rules and/or data protection, please contact:

Bendras finansavimas, UAB
Legal entity registration number 303259527
Address of the registered office Latvių g. 36A, Vilnius
E-mail: labas@savy.lt
Tel.: +370 (5) 272 015

E-mail of the Data Protection Officer:
dap@savy.lt