

UAB BENDRAS FINANSAVIMAS

RULES FOR PERSONAL DATA PROCESSING

1. GENERAL PROVISIONS

- 1.1. The Rules for the Processing of Personal Data (hereinafter referred to as the “**Rules**”) govern *UAB Bendras finansavimas*, legal entity code 303259527, address M. Valančiaus g. 1-1, Vilnius, Republic of Lithuania (hereinafter referred to as the “**Data Controller**” or the “**Company**”) and the actions of its employees in collecting, using and storing personal data. The Rules are intended for shareholders, persons interested in the Company, its services, potential and current investors, recipients of consumer credits (loans), persons who visit www.gosavy.com (or hereinafter referred to as the “**Website**”), use the Company’s electronic services or otherwise.
- 1.2. While processing its personal data, the Company complies 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 “GDPR”)
- 1.3. **These Rules may change. Please visit the Company's website from time to time and read the latest version of the Rules published there.**
- 1.4. The data subject is 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 Data 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 minimization”);

- 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. PURPOSES, SCOPE, LEGAL BASIS AND PERIODS FOR THE PROCESSING OF PERSONAL DATA

Data Subject	Purpose of data processing	Data processed	Legal basis	Period
Receivers of consumer credits (loans) / owners of crowdfunding projects (shareholders, manager, beneficiaries); investors	Identification	Name, surname, personal identification code (in case of a legal entity - company name, legal entity code, legal form, data of the manager, shareholders, beneficiaries), identity documents (photo, state, citizenship, document number, series, document type, validity date), residential address, gender, level of identification (in the case of investors), live video (live video) record, personal photo, video start and end time, face and identity document match result, qualified electronic signature certificate data, bank account number, IP address, signature, e-mail address, other data obtained during customer identification	We are legally binding (Article 6(1)(c) of the GDPR) In cases where biometric data are collected, the Company shall, in addition, follow Article 9(2)(f) of the GDPR, i. e. shall seek to meet legal requirements applicable to the Company (the Law on the Prevention of Money Laundering and Terrorist Financing, and the Law on Consumer Credit).	The data shall be stored from the day of completion of an application and for 10 years after the date of full discharge of obligations under the last agreement between the Company, the recipient of the loan and the issuer of the loan, or 6 years after the refusal to provide the financial service; Investors’ data shall be stored from the date of connection of Paysera to the Company Website and for 10 years after the date of full discharge of obligations under the last agreement between the Company, the recipient of the loan and the

				<p>issuer of the loan; if the investor does not conclude agreements, the data shall be stored for 6 years from the date of registration.</p> <p>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 Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania.</p>
<p>Receivers of consumer credits (loans) / owners of crowdfunding projects (shareholders, manager, beneficiaries); investors</p>	<p>Prevention of money laundering and terrorist financing</p>	<p>Name, surname, personal identification number, place of residence, citizenship, e-mail address, telephone number, address, object of investment, planned investment amount, average monthly income, main source of funds, beneficial owner of funds, personal document information, risk category to which customer and / or, geographical risk category, live video (live video broadcast) record (start and end time), identity document and face image match result, qualified electronic signature certificate data, other data obtained during customer identification, invoice and / or contract documentation, business relationship</p>	<p>We are legally binding (Article 6(1)(c) of the GDPR)</p> <p>We have a legitimate interest (to prevent money laundering and terrorist financing) (Article 6(1)(f) of the GDPR)</p>	<p>Data on consumer credit (loan) recipients shall be stored from the date of filling in the application and for 10 years after the full discharge of obligations under the last agreement between the Company, the recipient of the loan and the issuer of the loan, or for 6 years after the refusal to provide the financial service;</p> <p>Investors' data shall be stored from the date of registration on the Company's Website and for 10 years after the date of full discharge of obligations</p>

		<p>correspondence, documents and data confirming a monetary transaction or transaction or other legally valid documents and data related to the performance of monetary transactions or transactions, IP address (in case of a legal entity, additionally - company name legal entity code, date of registration, registered office, country of residence for tax purposes, number of employees, duration of activity, name of manager (representative), shareholders, beneficiaries, personal code (or date of birth), nationality, country of residence for tax purposes, number of shares, names and codes of business partner companies and countries).</p>		<p>under the last agreement between the Company, the recipient of the loan and the issuer of the loan; if the investor does not conclude agreements, the data shall be stored for 6 years from the date of registration.</p> <p>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 Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania.</p>
		<p>Data on the consumer's participation in political activities, inclusion in the list of sanctions</p>	<p>We are legally binding (Article 6(1)(c) of the GDPR);</p> <p>We collect information on public interest (Article 9 (2) (g) of the GDPR) and seek to comply with the legal requirements applicable to the Company (Article 9 (2) (f) of the GDPR).</p>	
<p>Receivers of consumer credits (loans) / Data on spouses of recipients of consumer credits</p>	<p>Creditworthiness / solvency assessment, debt management</p>	<p>Name, surname, personal identification number, address of registered place of residence (in the case of a legal person: company name, code of legal person, address of registered</p>	<p>We are legally binding (Article 6(1)(c) of GDPR);</p> <p>We shall conclude</p>	<p>Data shall be stored from the date of filling in the application and for 10 years after the full discharge of obligations under the last agreement between the</p>

<p>(loans); owners of crowdfunding projects (shareholders, manager, beneficiaries), warrantor</p>		<p>office, full name of the head and authorised person, their personal identification numbers; full name of shareholders, their personal identification numbers; other information provided below required for the assessment of creditworthiness): marital status; spouse's name, surname, personal ID number; number of minor children and dependents; income, non-employment income, employer, workplace, income duration, total length of service, start/end of employment relationship, work / activity area, individual or other economic activity, income received from it, other income, received/assigned periodical or lump sum benefits, bank account statement, certificates; sources, type, size, nature of incomes or other benefits; periods of receipt, social insurance policyholder, start and end of social insurance period, income tax return data, available real estate and movable property, property rights and restrictions thereof; data on current and past financial liabilities and their execution: number of contracts, counterparties, dates, types; financial liabilities, credit limit, account surplus, used credit, interest, total financial liabilities, contributions payable, method of payment; maturities for financial liabilities; terms, amounts of</p>	<p>with you and execute financial services contract (Article 6(1)(b) of GDPR);</p> <p>We have a legitimate interest in assessing creditworthiness and debt management (Article 6(1)(f) of GDPR)</p>	<p>Company, the recipient of the loan and the issuer of the loan, or for 6 years after the refusal to provide the financial service.</p>
---------------------------------------------------------------------------------------------------	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------

		<p>overdue payments, number of overdue payments; types of applications, amounts, other information relating to the aforesaid; credit rating, financial situation of the family (liabilities, income), mark of keeping or non-keeping accounting records, basic economic activity, direct payments and other support for agriculture and rural development, their type, amount, information and data on the registration in the information system of a list of persons in respect of which applications to prevent them from entering into consumer credit agreements are provided, data from the bailiffs' information system on enforcement cases initiated against the consumer credit (borrower) borrower / spouse, etc. data required to assess the creditworthiness of the customer.</p>		
<p>Owners of crowdfunding projects (shareholders, manager, beneficiaries)</p>	<p>Assessment of reliability of the owners of crowdfunding projects</p>	<p>Extract from the judicial record, other material information to assess reputation, uch as e.g. a person was the head of a legal entity, the right to engage in the provision of financial services of which was abolished, or another measure was applied for the serious infringement of law or other legislation governing the provision of financial services or activities of financial institutions.</p>	<p>We are legally binding (Article 6(1)(c) of the GDPR);</p> <p>We strive to fulfill the legal requirements applicable to the Company (Article 9(2)(f) of the GDPR);</p>	<p>Data shall be stored from the date of filling in the application and for 10 years after the full discharge of obligations under the last agreement between the Company, the recipient of the loan and the issuer of the loan, or for 6 years after the refusal to provide the financial service.</p>
<p>Receivers of consumer credits (loans) / Data on</p>	<p>Compliance with the requirements of laws and concluded contracts,</p>	<p>In the case of the recipient of the loan: name, surname, registered place of residence (in the case of a</p>	<p>Conclusion and execution of contracts (Article 6(1)(b) of the</p>	<p>Investors' data shall be stored from the date of registration on the</p>

<p>spouses of recipients of consumer credits (loans) (including potential); owners of crowdfunding projects (shareholders, manager, beneficiaries) (including potential); warrantor (including potential)</p>	<p>including for internal administration purposes</p>	<p>legal entity: name of the company, legal form, address of the registered office, entity code, name, surname of the head or authorized person, personal identification number, e-mail, phone number), phone number , e-mail, consumer number, age, consumer credit agreement, consumer credit agreement number, consumer credit agreement date, consumer credit termination date, date of transfer and recovery by the debt collection company; type and amount of consumer credit, repayment schedule of consumer credit, end of period, date of early repayment of consumer credit, premium repayment, amount of consumer credit, information provided in consumer credit agreement, signature, account number, number of personal document, bank name in which the account is opened, date and time of filling in the application, loan status, Paysera wallet number, active/inactive status, date and time of last login, automatic notifications related to the cause of rejection of the consumer's credit application, the application submitted for data adjustment, payment reminders, transfer to the debt recovery company, the court and the invoices for payment, other notifications that we are obliged to provide legally, the texts, subjects,</p>	<p>GDPR); We have a legitimate interest (proper administration of SAVY platform databases and proper and high quality provision of consumer credit (loan) services) (Article 6(1)(f) of the GDPR);</p>	<p>Company's Website and from 10 years after the day of full discharge of obligations under the last agreement between the Company, the receiver of the loan and the issuer of the loan; if the investor does not conclude contracts, the data shall be stored for 6 years from the date of registration; the data of the receivers of the loans shall be stored from the date of filling in the application and for 10 years after the day of full discharge of obligations under the last contract between the Company, the receiver of the loan and the issuer of the loan, or for 6 years after the refusal to provide the financial service.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>dispatch times and dates of these notifications.</p> <p>In the case of investors: name, surname, personal ID number, investor identification number, Paysera wallet number, active/inactive status, date and time of registration, date and time of last login, history of orders made within SAVY, texts, topics, sending times and dates of automatic notifications related to loans that the client invested in and internal updates of the legislation.</p>		
<p>Receivers of consumer credits (loans) / Data on spouses of recipients of consumer credits (loans) (including potential); owners of crowdfunding projects (shareholders, manager, beneficiaries) (including potential); warrantor (including potential)</p>	<p>Provision of services and quality assurance</p>	<p>Name, surname, telephone number, date of conversation, start and end time, conversation content.</p> <p>IMPORTANT: We will only record the conversations that take place when you call the Company by phone number <u>+370 (5) 272 0151</u>, as well as when we call you from the number assigned to the Company during the business hours of the Company.</p>	<p>We have a legitimate interest (to ensure the quality of consumer service, to collect evidence for a dispute in case it arises) (Article 6(1)(f) of the GDPR);</p>	<p>Data shall be stored for 999 days after the date of making the phone call record.</p> <p>IMPORTANT: When there is reason to believe that an offense or other illegal activity is recorded in the conversation record, the necessary data of the conversation record shall be transferred to secure media and stored at all times until there is an objective need, even after the expiration of the term for the storage of conversation records specified in this clause.</p>
<p>Receivers of consumer credits (loans) / Data on spouses of recipients of consumer credits</p>	<p>Inquiries sent by the Company's mail including, but not limited to, complaints, requests for administration purposes, or to resolve any issues that</p>	<p>Name, surname, email, date and time of submission, date and time of response; other data of the potential client provided voluntarily in the application, inquiry, request, complaint, content</p>	<p>The performance of the agreement or prior to the entry into the the agreement, it is intended to take actions at the request</p>	<p>Data shall be stored for 6 years from the date of application. In the event of a consumer credit (loan) agreement, the data shall be stored for 10 years after the</p>

<p>(loans) (including potential); owners of crowdfunding projects (shareholders, manager, beneficiaries) (including potential); warrantor (including potential)</p>	<p>require your data when you apply to the Company</p>	<p>of received and sent messages, history of correspondence.</p>	<p>of the Data Subject (Article 6(1)(b) of the GDPR);</p> <p>We have a legitimate interest (to properly provide financial services, prevent false data, fraud and provide such evidence to relevant institutions (Financial Crime Investigation Service (FCIS), Bank of Lithuania, etc.) (Article 6(1)(f) of the GDPR);</p>	<p>expiration of the loan agreement.</p>
<p>Receivers of consumer credits (loans) / Data on spouses of recipients of consumer credits (loans) (including potential); owners of crowdfunding projects (shareholders, manager, beneficiaries) (including potential); warrantor (including potential) and other website visitors</p>	<p>Ensuring smooth and secure operation of the web site and access to services</p>	<p>IP address, information on a browser and device (OS version, screen size), email address and password.</p>	<p>Consent (Article 6(1)(a) of the GDPR);</p> <p>Conclusion and performance of the agreement (Article 6(1)(b) of the GDPR).</p> <p>We have a legitimate interest to ensure the security of the Company's website (Article 6(1)(f) of the GDPR).</p>	<p>Not more than 6 years after visiting the Company's website.</p>
<p>Receivers of consumer credits (loans) / Data on</p>	<p>Defend the Company's rights and interests, if necessary, in legal</p>	<p>Information about the receiver of consumer credit (loan), which is listed above, including documents</p>	<p>We have a legitimate interest (to manage debts, to obtain</p>	<p>Data shall be stored from the date of filling in the application and for 10 years</p>

spouses of recipients of consumer credits (loans); owners of crowdfunding projects (shareholders, manager, beneficiaries), warrantor	proceedings or debt recovery	and their annexes sent to the consumer credit receiver, documents and their annexes, provided by the consumer credit receiver, procedural documents, court orders, rulings, decisions, bailiffs' orders and all others documents related to these processes.	compensation for damages, to defend rights in legal proceedings) (Article 6(1)(f) of the GDPR).	after the full discharge of obligations under the last agreement between the Company, the recipient of the loan and the issuer of the loan, or for 6 years after the refusal to provide the financial service.
		Information on criminal offenses and convictions	The data is needed to lodge, fulfil or defend legal claims in case of fraud (Article 9(2)(f) of the GDPR).	
Receivers of consumer credits (loans), investors, potential receivers of consumer credits (loans), potential investors who gave their consent to direct marketing	Direct marketing	<p>Name, surname, e-mail address, telephone number, address.</p> <p>If you agreed to receive direct marketing notifications by email to understand if the information we sent is relevant to you, we collect statistical information about the newsletters sent (whether you read the newsletter, when and how many times you read it or opened, or forwarded it to others, what operating system and email server (its location) you use).</p> <p>IMPORTANT: The Company uses profiling to make personal offers to the client - by applying specific algorithms it analyzes your personal data submitted. The actions taken by the Issuer of the Credit shall have no legal or similar material effect on the consumer.</p>	<p>Consent (Article 6 (1) (a) of the GDPR; Article 69 (1) of the Law on Electronic Communications)</p> <p>You have purchased the Company's services (Article 69 (2) of the Law on Electronic Communications)</p> <p>We have a legitimate interest to collect and use information about you (direct marketing and consumer satisfaction survey) (Article 6 (1) (f) of the GDPR).</p>	<p>Data of the recipients of loans shall be stored from the date of consent and for 6 years after the date of full discharge of obligations under the loan agreement between the Company, the recipient of the loan and the issuer of the loan, unless the Data Subject wishes to extend the term. In the absence of a loan agreement, the data shall be stored for 6 years from the date of receipt of the consent, unless the Data Subject wishes to extend the term.</p> <p>Investors' data shall be stored for 6 years from the date of receipt of the consent, unless the Data Subject wishes to extend the term.</p>

				Upon withdrawal of the consent, the Company shall store the data for 10 years after the end of the data processing deadline indicated in the consent or withdrawal of the consent for the establishment, exercise or defence of legal claims of the Company.
Investors	For the purpose of transactions, provision of intermediary functions and financial services	Name, surname, personal ID number, date of birth, nationality, address, e-mail, bank account number, card issuing organization and card number (if the account is linked to a card), phone number, email, sex, address, IP address, identification level, unique Paysera account number, which must be connected to the SAVY investor account to start investing; the balance of the connected account; investment data.	For the purpose of the performance of the agreement between the investor, the receiver of the loan and the Company (or, taking actions at the request of the investor for conclusion of the agreement (Article 6 (1) (b) of the GDPR).	Investors' data shall be stored from the connection of Paysera's wallet and for 10 years after the date of full discharge of obligations under the contract.
Receivers of consumer credits (loans) / Data on spouses of recipients of consumer credits (loans) (including potential); owners of crowdfunding projects (shareholders, manager, beneficiaries) (including potential);	Communication with the Company through OLARK	IP address, location, what sections of the SAVY page you have visited if you have specified your name and email, conversation rating, other voluntary information provided in the query	Consent (Article 6 (1) (a) of the GDPR ("Olark"))	Data shall be stored for 30 days from the date of the query.

warrantor (including potential) and other inquirers				
Investors seeking to create an account on the Company's website	Registration of the investor	<p>When resitering via a Facebook account, the following data shall be collected:</p> <ul style="list-style-type: none"> • Name • Surname • Email address • Facebook ID • IP address <p>If you do not wish to register via a Facebook account, you will be asked to enter the following information on the Company's website:</p> <ul style="list-style-type: none"> • Email address • Telephone number 	Consent (Article 6 (1) (a) of the GDPR)	<p>Investors' data shall be stored for 6 years from the date of registration if the investor does not connect the Paysera wallet.</p> <p>If the investor connects the Paysera wallet, the data shall be stored for 10 years after the date of full discharge of obligations under the last agreement between the Company, the receiver of the loan and the issuer of the loan.</p> <p>Upon withdrawal of the consent, the Company shall store the data for 10 years after the end of the data processing deadline indicated in the consent or withdrawal of the consent for the establishment, exercise or defence of legal claims of the Company.</p>

<p>Receivers of consumer credits (loans)</p>	<p>For the purpose of publicizing the quality of the Company's services on the website</p>	<p>First name, surname; loan ID and loan purpose; age, place of residence, email and feedback about the Company</p>	<p>Consent (Article 6 (1) (a) of the GDPR)</p>	<p>Data shall be stored for 6 years from the date of consent.</p> <p>Upon withdrawal of the consent, the Company shall store the data for 10 years after the end of the data processing deadline indicated in the consent or withdrawal of the consent in for the establishment, exercise or defence of legal legal claims of the Company.</p>
<p>Shareholders of the Company</p>	<p>Accounting for legal obligations applicable to the Company with respect to registration and processing of data on the Company's shareholders, shares, tax compliance and other obligations applicable to them.</p>	<p>Name, surname, personal identification number, date of birth, address, telephone number, email address</p>	<p>We are legally bound by the Law on Companies (Article 6(1)(c) of the GDPR).</p>	<p>Data shall be processed for no longer than is necessary for the purposes for which the processing is carried out or the law applicable, provided a longer storage period is provided therein. In order to determine the data storage period, the Company shall apply criteria that correspond to the obligations specified in the legal acts, also taking into account the rights provided by the person, for example, it provides for a data storage period during which the claims in relation to the performance of the contract may be provided, etc.</p>

Shareholders, employees or service providers of the Company who have given consent	Publicity of the Company's activities	First name, surname, position, description of work experience, photo	Consent (Article 6 (1) (a) of the GDPR)	Data shall be stored from the date of consent until the end of the business relationship with the Company or the date of withdrawal of the consent. Upon termination of business relations with the Company or withdrawal of the consent, the Company undertakes to delete personal data no later than within thirty days. Upon withdrawal of the consent, the Company shall store the data on consent for 10 years after the end of the data processing deadline indicated in the consent or withdrawal of the consent for the establishment, exercise or defence of the legal claims of the Company.
Representatives, employees of the Company's partners/suppliers	For the purpose of providing services	Name surname; personal identification number, address, representative (contact with the representative), position, workplace, phone number, email.	We have a legitimate interest (for the performance of a contract) (Article 6 (1) (f) of the GDPR).	During the validity of the contract and for 10 years after the end of the transaction.

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

3. SUPPLY AND RECEIPT OF PERSONAL DATA

3.1. The Data Controller may supply 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 consumer credit (loan) agreement is concluded between the Company's investors, the consumer credit (loan) recipient and the Company;
- Data on natural persons who have lent EUR 600 or more are disclosed to the owners of crowdfunding projects
- in the event of breach of the terms and conditions of the agreement concluded between the Data Subject and the Company, to third parties, through which the rights and legitimate interests of the Company will be safeguarded and protected;
- third parties whose activities are related to debt recovery, administration or use for the purpose of administering the Data Subject's debt and/or recovering the Data Subject's debt to the Company;
- other persons (lawyers, consultants, auditors, companies creating 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 bills of exchange);
- companies or individuals providing direct marketing execution services;
- Information systems INFOBANKAS and CREDIT OFFICE administered by UAB Creditinfo Lietuva (spouses' data are also transferred, if necessary);
- UAB SCORIFY;
- SEB Bank, AB; PAYSERA LT, UAB;
- The Bank of Lithuania and other supervisory authorities;
- Loan Risk Database administered by the Bank of Lithuania;
- The State Social Insurance Fund Board under the Ministry of Social Security and Labor;
- The State Tax Inspectorate;
- SE Centre of Registers;
- Debt collection companies;
- UAB DPD Lietuva;
- AB Lietuvos Paštas;
- Facebook Ireland Ltd;
- UAB ONDATO (identification);
- UAB BALTNETA;
- UAB IPF Digital Lietuva;
- 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);

- After giving the consent of the Data Subject, the Company may also transfer personal data to its partners, who may contact and submit an alternative loan or consumer credit offer to the Data Subject;
 - If necessary - to companies or persons that intend to buy or buy 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 supplied 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 are obtained directly from the Customer when applying to the Company, filling the applications, requests or submitting other documents to the Company. Personal data or data subject can also be obtained from the Bank of Lithuania; commercial banks; Paysera LT; State Social Insurance Fund Board; State Enterprise Centre of Registers (Population Register, Lien Register, Mortgage Register, Real Estate Register, Register of Legal Entities, Information System for Participants of Legal Entities, Bailiffs Information System, etc.); other administrators of state and departmental registers: register of wanted persons, register of invalid documents; UAB "Ondato"; UAB "Scorify"; UAB "DPD Lietuva"; UAB "Creditinfo Lietuva" administered information systems INFOBANKAS and KREDITŲ BIURAS, if such data are necessary to make decision on credit rating, credit granting and loan management, subjects providing the services of personal identification, social networks accounts linked to Company's system, etc.
- 3.4. In addition, we inform that if the Customer delays to fulfil its obligations to the Company more than 40 days, the Company may provide information about Customer's identity, contact details and credit history, i.e., financial and property obligations and their execution, debts and their payment, to Credit Office UAB "Creditinfo Lietuva" (company code: 111689163, address: A. Goštauto g. 40A, LT 01112 Vilnius, Lithuania, www.manocreditinfo.lt, ph.: (8 5) 2394131). Credit Office processes and submits the third parties (financial institutions, telecommunication companies, insurance companies, electricity and utility providers, trade companies, etc.) with your information pursuing legitimate interests and objectives – to assess the creditworthiness and manage the debt. During the creditworthiness assessment, the personal properties assessment is made automatically (profiling). It may have an influence to Customer's possibility to make transactions in the future. The automatic assessment helps to lend responsibly, assesses the information submitted by the person, credit history, public information, etc. Automatic assessment methods are reviewed regularly to ensure their fairness, efficiency and impartiality. Credit history data are processed 10 years after the execution of obligations. You may access your credit history by applying to Credit Office directly or using Finpass mobile app. You also have a right to ask to correct or delete personal data, restrict their processing and the right to object to the processing of data, require human intervention in automatic decision making, express your view and challenge the decision, as well as right to data portability. More information about implementation of these rights, restrictions and automatic properties assessment (profiling) is provided at www.manocreditinfo.lt. If your rights are violated, you can apply to Data Protection Officer by email duomenu.apsauga@creditinfo.lt or above phone number or submit the complaint to the State Data Protection Inspectorate or the court.

4. PROFILING AND AUTOMATED DECISION-MAKING

- 4.1. Profiling can be carried out by combining and grouping personal data obtained, i.e. it consists 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 analyzing 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 can 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 Consumer.
- 4.2. In the case where the relevant decision is made only by automated means, the Consumer shall have the right to request to review the decision by human intervention, as well as the right to express his or her point of view, to obtain an explanation of the decision made following that assessment, and to 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/her consent in the relevant column of the Consumer Credit/Loan Application or, in the case of Investors, by registering on the SAVY website.
- 5.2. The Data Subject may refuse his/her data to be processed for the purposes of direct marketing, including profiling, and may inform the Company in the following ways:
- by phone +370 (5) 272 0151;
 - by email: 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 www.gosavy.com, browses through third party websites and social networks, tailor-made proposals for the Data Subject may be displayed.
- 5.4. The Data Subject's email, as well as anonymised information about he/her, may be provided to third parties who provide marketing services through online search engines, social networks, and the like. Such third parties have their own privacy policies and the Data Subject at any time may disagree with the processing of his/her data in accordance with the third parties' privacy policies.

6. USE OF COOKIES

- 6.1. We use cookies when you visit and browse our Company's Website. Cookies are small text files (up to several KB) that your browser places on your computer, tablet or other smart device by visiting the Company's website. With cookies, the Company aims to ensure efficient and

safe operation of the website and to analyze 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/her personal data shall include the right to:

- 7.1.1. get acquainted with the 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. require rectification, destruction of personal data or limitation of the processing of his/her 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. disagree, without giving reasons, with his/her personal data being processed for direct marketing purposes or for other purposes for which his/her consent is requested;
- 7.1.4. refuse to apply only automated data processing, including profiling;
- 7.1.5. exercise his/her right to data portability;
- 7.1.6. exercise the right to be "forgotten";
- 7.1.7. 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 are provided with grammatical errors.

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

8. TERRITORY OF CUSTOMER'S PERSONAL DATA PROCESSING

8.1. Customer's personal data are processed within the territory of European Union / European Economic Area (EU/EEA), but in some cases they may be transmitted and processed beyond the border of EU/EEA.

8.2. After having submitted an application, the Customer can get more information about transmission of Customer's personal data beyond the borders of EU/EEA. If the Company transfers the Client's personal data to such persons, the Company will take all measures provided for in legal acts in order to ensure the security of the Client's data.

9. SECURITY OF PERSONAL DATA

- 9.1. The organizational and technical data security measures implemented by the Data Controller 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 provides 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 applies administrative security measures (secure document and computer data processing, personnel training, etc.).
- 9.4. Employees 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 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. Access to the database of persons authorized to process personal data is 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 are 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.). A computer worker can 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 are made and stored elsewhere than the active database, and the lost data are restored from backups. This procedure is 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 protection violation, the degree, damage, and consequences of violation, the Data Controller takes decisions based on relevant internal procedures on the measures necessary to remove the data protection violation and its consequences and inform the required entities.
- 9.13. The premises where the personal data are stored are secured (only authorized persons have access to the relevant premises, the alarm system is installed in the premises, etc.).

10. RESPONSIBILITY

- 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. The Company will 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 their changes.
- 10.2. The Data Subject warrants that all data provided while using the Company's services are correct.
- 10.3. 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.
- 10.4. The Company is not in a position to fully guarantee that the functioning of the www.gosavy.com website will be uninterrupted and free from any malfunction or error, that www.gosavy.com website will 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.
- 10.5. If the Data Subject is a registered user of the www.gosavy.com website, the Data Subject shall assume all the risk and responsibility for third party actions performed on the www.gosavy.com website using the Data Subject's login data, and undertakes to fulfill all obligations undertaken using the Data Subject's access data, except where the Company has failed to fulfill its obligations properly.

11. FINAL PROVISIONS

- 11.1. Data Subjects can access these Rules at www.gosavy.com.
- 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 change 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 additions or amendments to the Rules comes into force from the date of their publication on the Company's website www.gosavy.com.

- 11.5. If the Data Subject continues to use the www.gosavy.com website and/or services provided by the Data Controller after addition or amendment of the Rules, the Data Subject shall be deemed not to have objected to such additions and/or amendments.
- 11.6. All disagreements arising from the implementation of these Rules shall be settled by negotiation. In case of 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 us by the following emails and telephone:

Email: labas@savy.lt or dap@savy.lt

Phone No: +370 (5) 272 0151