Approved by
LTD „Bendras finansavimas“
Director 2018, August 20th
Order No. 2018/08/20

LTD „Bendras finansavimas“
PERSONAL DATA MANAGEMENT RULES

1. GENERAL PROVISIONS

1.1. Personal Data Management Rules (hereinafter **Rules**) regulates the LTD „Bendras finansavimas“, legal entity code 303259527, address M. Valančiaus g. 1-1, Vilnius, Republic of Lithuania (hereinafter - **Data Manager or the Company**), and the actions of its employees when managing personal data, using the Companies installed automatic and non-automatic personal data management tools, as well as it determines the rights of the Data Subject, personal data implementation tools and other issues related to personal data management.

1.2. Data subject is a natural person who is intending to begin or has begun a business relationship with the Data Manager, or when the business relationship have terminated, but the Data Subjects personal data is managed by the Data Manager according to the imperative regulations of legal acts, or one who has not begun a business relationship with the Data Subject by their own incentive, but the Data Manager manages his personal data according to the imperative regulations of legal acts (hereinafter - **Data Subject**).

1.3. Data manager respects the privacy of the Data subject. These rules explain the acceptable practice on privacy in our Company. It explains the ways that are used to gather and use Your personal data without the rights that You hold.

1.4. All of the Employees of the Company working in it according to the work agreements must adhere to the rule that manage the personal data in the Company or if they discover the data by performing their duties as well as the other persons providing services on a contractual basis, who are allowed to manage personal data.

1.5. The Data manager ensures that he matches these essential data security principals:

1.5.1. Collects the subject’s personal data with defined goals (principals of purpose);

1.5.2. The data subject’s personal data is managed in a legal, fair and transparent way (legality, fairness and transparency principal);

1.5.3. Data subject’s personal data has to be adequate, proper and only such, which is necessary to achieve goals, for which they are managed (data amount lowering principal);

1.5.4. Personal data has to be clear and renewed when needed; all justified measures should be taken in order to ensure that the Personal data, which are not definite, taking into account their purposes for management, would be immediately corrected or deleted (principal of preciseness);

1.5.5. Data subject’s personal data is stored for no longer than needed for the purposes of data management and basis of legal acts (storage period limitation principal);

1.5.6. Data subject’s personal data has to be managed in a way, that when adequate technical or organisational tools are applied, the proper Data

Subject's personal data safety would be ensured, including the safety from data management without permission or illegal data management, as well as from accidental loss, deletion or ruin. Data Subjects personal data is not disclosed by the Data Manager to third parties, except in the cases defined by law or when the Data Manager is obliged to do so / the Data Subject provides consent himself (solidity and confidentiality principal);

1.5.7. Data Manager is responsible for the compliance with the previously mentioned principals and has to be able to prove that they are followed (accountability principal).

1.5. These rules are applied to the Data Manager and Data Subjects that are or were using, expressed the intention to use or are in any other way related to the Companies provided services, interpersonal relationship, including relationships with the Data Subject before the validity of these Rules.

2. PURPOSES, BASIS AND SCOPE OF PERSONAL DATA MANAGEMENT

2.1. **Personal Data management purposes:**

2.1.1. **Identity determination purposes**

Performing the legal acts, related to, for example, the implementation of responsible borrowing principals, for the purposes of identity identifying, when it is mandatory for the Contract performance, seeking to take up actions on the request of the Data Subject before making up the agreement, performing legal duties or seeking Data Managers legal interest to ensure the proper management of risk.

2.1.2. **Money laundering and terrorist financing preventions, for the purpose of implementing know your customer (KYC) principal** Performing the implementation of principals related to legal acts, for example, with the responsible borrowing performance, "know your customer" principal implementation, performing market transparency insurance and data provision requirements for competitors institutions, plausible money laundering and terrorist financing prevention, the determination of such activity, research and information provision on the possible activities as such, applied financial sanctions or participation in politics to the Data Subject.

2.1.3. **Proper creditworthiness evaluation, making up of loan agreements, debt management, for the purposes of protecting the legal interests of the Data Subjects and Data manager's rights**

Seeking to determine what conditions can be offered to the Data subject when providing loans, performing duties provided in legal acts, related to solvency and commitment performance risk evaluation, to manage Data Subjects debt, perform internal calculations and analysis when that is necessary when performing the agreement, seeking to take actions on the request of the Data Subject before making up an agreement or performing legal duties, or seeking the Data Managers legal interest, ensuring the trustworthy management of risk.

2.1.4. **Direct marketing purposes**

Data subject's information (newsletters and offers sending via e-mail), for the purpose of opinion, questionnaire, market analysis and statistical data gathering, games and sales to Data Subjects, when the Data Subjects agreement is received. 2.1.5. **For the purpose of Data subjects and (or) Data Managers interest protection**

Seeking to protect the Data Subjects and (or) Data managers interest, to perform the Data Managers provided services quality check, provide transaction or other proof of communication (call recording), when it is necessary when performing the agreement or performing legal duty, seeking Data Managers legal interest to perform any improper or illegal usage of Data Managers services or the prevention of their breach.

2.1.6. **For the purposes of evaluating the natural person's solvency guaranteeing a natural person's loan**

Seeking to properly evaluate whether the guarantor can take up the financial risk and financially capable to perform the contract, if the natural person would not perform his duties according to the assumed obligations.

2.1.7. **For the purposes of transaction intermediary services and the provision of financial services**

Seeking to provide qualitative service to the investor.

2.2. **Scope of personal data management:**

2.2.1. According to aims provided in Chapter 2.1. Point2.1.1.the Company manages this Data Subjects personal data: name, surname, personal code, age, declared and actual place of residence (address), data subject's identity determination documents, bank account number, education, phone number, e-mail address, for the purposes of identification facial recognition systems might be used as well. This data is managed by the legal obligation basis of the Data Manager (General Data Protection Regulation Article 6 Part 1 Point C). Marital data is managed on the basis of consent (General Data Protection Regulation Article 6 Part 1 Point a).

2.2.2. According to aims provided in Chapter 2.1 Article 2.1.2 this Data Subjects personal data is managed: name, surname, personal code, age, declared, actual place of residence, address for correspondence, tax paying state, phone number, activity information, average monthly income received, main source of income, person participating in politics, name, surname and phone number of the contact person, in case of a interrupted contact with the Customer, the real name and surname of the beneficiary, personal code and other, in case of suspicion, proof demonstrating the origin of the investors income (General Data Protection Regulation Article 6 Part 1 Point d., c.).

2.2.3. According to aims provided in Chapter 2.1. Article2.1.3 this Data Subjects personal data is managed: marital status, fact of having dependents, place of employment data, position held, places of employment in the past 12 months, work experience, economic or individual activity performed, monthly work pay / other income, income tax declaration, work pay / other income or responsibilities substantiating certificates and documents, social national insurance benefits, monthly financial obligations to consumer credit or financial institutions, to other natural and legal persons and their types, missed or not covered debt, credit history (name of the creditor, code, amount of debt, dates of debt occurrence and coverage)the legal regime of the married persons assets, number of minors and dependent persons, assets held, the amount of loan agreements made, number of dates overdue, purpose of the loan, amount, agreement No. and date, return date, return schedule, unique user code, provided rating of creditability, information, that a person is listed amongst persons on behalf of whom requests are made not to allow them to draw up consumer credit agreements, the copies of all documents received, information from databases and etc. These documents will be managed for the purposes of

creditability evaluation according to the legal obligations applied to the Data Manager (General Data Protection Regulation Article 6 Part 1 Point c.). Spouse's data is managed for the purposes of creditability assessment with given consent (General Data Protection Regulation Article 6 Part 1 Point a.). For the purposes of protecting and defending legal interests of the made up loan agreements, debt management, clients and Company's rights, data is managed seeking legal Data Managers of third party's interests (General Data Protection Regulation Article 6 Part 1 Point f.).

2.2.4. According to aims provided in Chapter 2.1 Article 2.1.4, this Data Subjects personal data is managed: name, surname, phone number, e-mail address, Data Subjects voluntarily provided reviews on the usage of Company's services. This data is managed on the basis of the Data Subjects consent (General Data Protection Regulation Article 6 Part 1 Point a.).

2.2.5. According to aims provided in Chapter 2.1 Article 2.1.5, this Data Subjects personal data is managed: phone number, call recordings, date and time. This data is managed on the basis of the Data Subjects consent (General Data Protection Regulation Article 6 Part 1 Point a.). Data subjects financial experience and purposes for investment, which are achieved at the time when the Data Subject chooses and he is provided with the services, related to investment risk, about which he has to know. These documents are managed according to the applied legal obligation basis of the Data Manager (General Data Protection Regulation Article 6 Part 1 Point c.). Data on the assets pledged to the Company, beneficiaries, heirs, data, which is collected when the Data Subject interacts with the Company via e-mail, mail. This data is managed providing the legal Data Managers and third parties interests (General Data Protection Regulation Article 6 Part 1 Point f.)

2.2.6. According to aims provided in Chapter 2.1 Article 2.16, this Data Subjects personal data is managed: name, surname, personal code, ID document data, place of employment, date of birth, phone number, e-mail, place of residence (address), declared place of residence (address), education, duties, work pay, employments, dismissals, royalty income, economic or individual activity, income from it, marital status, number of minors and dependents, phone number, owned real estate or movable property, asset rights and their constraints, financial commitments (valid or expired financial commitments, date of agreement creation and termination, amount, monthly payment, payment schedules, date of last payment paid), overdue and unspent financial liabilities (overdue period, amount of debt, the amount of overdue debt to other companies, total amount of debt), creditor, name and code of the creditor, information on active loans (type of loans, date of application, amount of the requested loan). This data is managed on the basis of the Data Subjects consent (General Data Protection Regulation Article 6 Part 1 Point a).

2.2.7. According to aims provided in Chapter 2.1 Article 2.17, this Data Subjects personal data is managed: unique Paysera identification code, name, surname, personal code, date of birth, nationality, bank account No., name of bank card, card issuing organisation and No. (of the account is tied to the card), phone No., e-mail address, gender, address, level of identification, if the person is a person participating in politics. This data is managed on the basis of Data Subjects consent (General Data Protection Regulation Article 6 Part 1 Point a). This data is passed on by the data manager - Paysera LT, LTD (natural persons' personal code 300060819) - to the data manager - on the cooperation agreement

basis to LTD „Bendras finansavimas“. This personal data is also managed seeking to conclude the agreement, party of which is the Data Subject (General Data Protection Regulation Article 6 Part 1 Point b).

2.3. Personal data is gathered only on the basis determined by legal acts. Personal data can be obtained directly from the Data Subject, from the Data Subjects activities by him using services and external sources, such as public and private registers and other third parties.

2.4. Employees have the right to gather, manage, pass, store, destroy and to use data in other ways only by performing their direct employment functions and only on the basis determined by the legal acts.

2.5. Employees are not allowed to arbitrarily gather, pass, store, destroy on in other ways manage personal data and to use personal data for personal purposes, not related to work.

2.6. Data subjects voluntarily provided reviews on the usage of company's services can be published publicly on the company’s website when having written consent. The validity term of the agreement - no longer than 5 (five) years from the date of agreement provision.

3. PROVISION AND RECEIVAL OF PERSONAL DATA

3.1. The Data Manager can provide managed personal data to third parties in order to achieve defined and legal purposes:

a. On the agreed basis for natural persons providing IT services, seeking to ensure the safety of data present in the Company's administrated platform as well as the Companies provision of services to Data Subjects; LTD „Duomenų logistikos centras“, seeking to ensure the Data Subjects proper security of personal data back-ups; LTD „Baltnetos komunikacijos“, providing telephony services seeking proper provision of services to the Data Subject by the Company;

b. LTD „Creditinfo Lietuva“, LRD „Scorify“, with the help of which it would be possible to evaluate the Data Subjects solvency, commitments, Agreement conclusion, performance risks, as well as seeking to manage debt;

c. LTD „Creditinfo Lietuva“, if the person violates the Company's concluded agreement provisions, the data is transferred for the purpose to store and protect the violated rights of the Company and the legal interests, also, information, which is directly related to a specific breach of the agreement is provided;

d. To debt collection company LTD „Skolų rizikos sprendimai“, LTD „Julianus Inkasso“, LTD „Sergel“, LTD „Conlex“, lawyer Vincentas Zabulis, seeking to recover debt from the Data Subject and in such a way to protect the violated Company's and/or Company's investors rights and legal interests;

e. To national establishments and institutions, other persons, performing functions provided to them by law (for example, law enforcement agencies, bailiffs, notaries, tax authorities, financial crime investigation agencies, etc.);

f. A Company, having the Data Subjects consent, has the right to forward Data Subjects personal data to Company's partners which will be able to contact the Data Subject and to offer the Data Subject alternative loan or consumer credit provision offer;

g. Loan or consumer credit agreement is made up between the Company, Data subject and the Companies investors. Based on this provision, the investor can

see in his Paysera account the person's (name and surname), who was transferred the fund, the Data Subject can also see the person's (name and surname), who transferred the funds and to whom he was to return these funds. The investor also has the possibility to receive the Data Subjects name, surname, personal code;

h. To other third parties, if the data is transferred according to the requirements by legal acts.

3.2. Personal data can be received from the Lithuanian bank; commercial banks; State Social Insurance Fund Board; State Enterprise Centre of Registers; LTD „Creditinfo Lietuva";a public register of invalid personal documents, if such data is necessary to make a decision on the provision of creditworthiness rating, credit provision, provision of other services and management of debts.

3.3. When Data Managers access rights to data are revoked once the Personal Data management agreement was terminated, made up with the Data Manager, or when this agreement is no longer valid.

3.4. Data is transferred to data managers and data recipients, when the right and (or) duty to do so by a proper basis is provided by legal acts.

3.5. Personal Data can be provided in these cases: writing, electronic means of communication, connecting to separate data gathering databases and informational systems or in an another way agreed upon with the Data Manager.

3.6. Non-automatized provision of personal data when personal data is provided not the Data Subject itself, has to be approved by the Company's manager, except in those cases, when data is provided to the supervisory authority.

3.7. Data Subject can provide his personal data by coming to the Company's office, by connecting onto his user account, by registered mail or e-mail. The Data Subject can also transfer his personal data by making a payment transfer, together providing his personal code and other data of payment.

3.8. The Company must immediately inform the data recipients about the Data Subjects request to correct or destroy personal data, terminated personal data management activities, except in those cases, when information provision would be impossible or too difficult (due to the large amount of Data subjects, data period, unreasonably high costs). In this case the Company immediately informs the State Data Protection Inspectorate.

3.9. Personal data can be received from Paysera LT, LTD, seeking for the Company to properly manage intermediary functions and to provide financial services to the Company's administrated inter-lending and co-financing platform SAVY investors.

3.10. The Data Subject guarantees that all of his provided data, using the Company's services, is correct.

3.11. A Data Subject who provides false information is responsible for the Company's and / or other users and investors experienced damage, including, but not limiting to, cases when other users create such false information providing Data Subjects agreement.

4. PERSONAL DATA STORAGE

4.1. Persons data is managed no longer than necessary. Personal data storage period is defined by taking into account the nature of agreements made with the Data Subject, Company's legal interests or legal act requirements (for ex., regulating requirements for money laundering, limitation period and etc.)

4.2. For the purposes provided in Article 2 Part 2.1 Points2.1.1., 2.1.2., 2.1.3., 2.1.5., 2.1.6., 2.1.7, personal data can be stored during a business relationship and 10 (ten) years

after the end of a business relationship. In case the transaction was not made, personal data is stored for 5 (five) years from the moment of receiving, except if there is a received written request for the Company's managed personal data destruction. If such request is received, personal data is deleted immediately and the personal data subject is informed.

4.3. On the purpose provided in Article 3 Part 2.1 Point 2.14., the loan recipients personal data is stored during the business meetings and 1,5 (one and a half) years after the termination of business meetings. If the business relations were not started, then data is stored for 1,5 (one and a half) years from the date of agreement receiving. Investors personal data is stored from the day of agreement during the entire period of business relationships. In all cases, data is destroyed if a personal data subject's written request on the Company's managed personal data destruction is received. If such request is received, personal data is deleted immediately and the personal data subject is informed.

4.4. Employees performing personal data management functions, seeking to prevent accidental or unlawful destruction, change, revealing of personal data, as well as any other kind of illegal management, has to store documents and data files properly and safely, as well as to avoid the performance of unnecessary copies. Document copies that provide personal data have to be destroyed so, that it would not be possible to recover or recognise their content. Copies of Personal documents can be stored electronically as well.

4.5. Once the Terms provided to the rules come, the personal data stored in electronic format is destroyed by responsible employees performing certain actions in the system. The documents stored in physical format (for ex., documents with personal data) are destroyed by the Company's employees using technical tools (for ex., document shredders). Destruction means the inability to restore the shredded personal documents.

5. MARKETING AND CORRESPONDENCE

5.1. By using the Company's provided services, Data Subject can voluntarily agree that the Data Subjects provided personal data would be used for the Company's purposes or marketing, expressing their agreement in the proper part of the consumer credit / loan agreement filling, or, in the cases of investors, registering in the SAVY platform and ticking the box.

5.2. The Company also provides the Data Subject with the possibility to unsubscribe to the Company's sent information:

5.2.1. The Data Subject has the right to unsubscribe to the Company's sent information, newsletters or in another letter by Data Subject pressing the provided Company's offers and news unsubscribing link;

5.3. Data Subject has his right to reject that his data would be managed for the purposes of direct marketing, can implement by informing the Company by e-mail labas@savy.lt or by phone +370 (5) 272 0151.

5.4. Data Subjects provided data, which is used for the purposes of direct marketing, help to ensure the constant Company's websites and services perfection and development.

5.5. The Company uses the Data Subjects data for the marketing activities allowed by law. For example, based on the Data Subjects provided information, by the subject visiting www.gosavy.comwebsite, browsing third party websites and social sites, offers applied to the Data Subject directly can be shown.

6. RIGHTS OF THE DATA SUBJECT

6.1. By the legal acts of the Data subject he is guaranteed the rights related to his personal data management, taking up the right to:

6.1.1. Request to correct Data Subjects data if they are incorrect, incomplete or unprecise;

6.1.2. not agree that Data Subjects data would be managed if the Data Subjects data management basis are legal interests;

6.1.3. request to delete Data Subject's data which is managed only with his consent, if the Data Subjects cancels the proper agreement. This right is not applied, if the Data Subject's data, which is requested to be deleted, is managed or managed in another legal way, such as management mandatory for the performance of the agreement or by obligation of performance of applied legal acts;

6.1.4. limit Data Subjects data management according to proper legal acts, for ex., period, during which the Company will evaluate if the Data Subject has the right to request that the Data Subjects data would be deleted;

6.1.5. receive information in case the Company manages Data Subjects data and if it does, to be introduced with them;

6.1.6. receive Data Subjects provided Personal Data, which is managed with his consent or the basis of agreement performance, in writing or in general used in electronic for and in case of the request of Data Subject to transfer such documents to another service provider (data transfer);

6.1.7. cancel his agreement to manage Data Subject's data;

6.1.8. disagree that he wold be applied a decision made in a fully automatized way, including profiling, if the acceptance of such decisions applied and if such decision making has legal consequences or similar significant impact to the Data subject. This right is not applied in cases when suchdecision making is necessary for the making of an agreement with the Data Subject or performance purposes, is allowed according to applied legal acts or when Data Subject has provided a clear agreement to it.

6.2. The Company clarifies, corrects and renews personal data of the person's, who's personal data is managing, initiative. The Company's employees can correct the Data Subjects data if the data provided by the data subject himself have grammatical errors.

6.3. Data manager has the right to motivationally reject to allow the Data Subject to implement his rights or to take a reasonable payment in the cases of General Data Protection Regulation circumstances of Article 12 Part 5 d.

6.4. To provide a complaint on the actions of the Data manager (inaction) to the National Data Protection Inspection (website www.ada.lt) within 3 months when receiving an answer from the Data manager, when data management response term to the data subjects appeal is over (i.e. 30 calendar days from the Data subjects appeal date). The complaint / request can be provided to the Company by the Data subject by e-mail labas@savy.lt.

7. PERSONAL DATA SAFETY

7.1. Data managers implemented organisational and technical data storage tools ensure such safety which complies with the Data managers managed nature of data and the risk of their management, including, but not limitation to, the tools provided in this chapter.
7.2. Company's data subject data management is ensured by the second-level of safety.
7.3. The Company performs technical and software protection (informational systems and the administration of databases, workplace supervision, operating system protection, user access tracking (monitoring), protection against computer viruses, etc.).
7.4. The Company applies administrational safety measures (safe documentation and computer data and their archive management, staff coaching during employment and exit / dismissal, etc.).
7.5. Data manager commits not to reveal the Data Subjects personal data to third parties, except the Data manager's employees or if it is necessary according to the imperative regulations of legal acts or if there's a received written agreement of the Data Subject.
7.6. Data management employees have to comply with the principal of confidentiality and to keep in secret any information related to personal data, which they familiarised with when performing their duties, unless such information would be public according to the valid laws and provisions of other legal acts.
7.7. The connections to the databases of these persons who have the right to manage personal data recordings are traced: login identifier, date, time, duration, connection
7.8. result (successful, unsuccessful). These recordings are stored for no less than 1 (one) year.
7.9. It is ensured, that information system testing would not be performed with real personal data, except the cases when organisational and technical personal data storage tools are used, ensuring the safety of real person's data.
7.10. On laptops, if they are used not by the Data manager's internal data transfer network, existing Personal data is protected by proper tools that comply with the Data management risk.
7.11. The Employees are provided access to personal data only to the extent which is necessary for the proper performance of duties and the implementation of work functions.
7.12. Employees that manage personal data in an automatic way or from whose computers it would be possible to access local network areas where personal data is stored, must use passwords. The passwords have to be changed periodically (no less than every 3 (three) months), as well as when there are such circumstances (for ex., change of an employee, risk of hacking, in the event of suspecting that the password is known to third parties and etc.). The employee, working on a specific computer, can know only his own password. There is a defined maximum of 5 allowed failed attempts to connect to the software. Exceeding the previously mentioned allowed amount of attempts, the Employee has to contact the Company's manager.
7.13. The Employee loses his right to manage personal data when the employees work or similar agreement with the Company ends, or when the Company's manager cancels the employee's assignment to manage personal data.
7.14. Persons data back-up copies are created, stored in a different place than the active (working) database, while the lost documents are restored from back-up copies. In case of accidental person's data loss, the re-creation time of them is fixed, as well

as persons, who have performed these actions. This procedure is determined in detail in the Activity continuance plan.

7.15. Persons data, located in external storage and e-mail have to be properly protected, as well as immediately transferred to databases after their usage.

7.16. Persons data risk assessment is performed by determining the risk of threat possibility, taking into consideration the integrity, accessibility and confidentiality of the data, according to each personal data management purpose.

7.17. Employees, noticing the violations of personal data, features of criminal actions, non-working person's data safety insurance tools have to immediately inform the Company's manager about this issue.

7.18. Data manager, when evaluated the Data security violation risk factors, the level of violation effect, damage and consequences, in accordance with relevant internal procedures takes upon the decision on the tools, necessary for the elimination of the security breach and its consequences, informs necessary subjects.

7.19. The security of premises, where Persons data is stored, is ensured (the access to relevant premises is ensured only to authorized persons is ensured and etc.)

8. RESPONSIBILITY

8.1. Data subject must provide the Company with detailed and correct Data Subjects personal data, as well as to inform upon the relevant changes of the Data Subjects personal data. The Company will not be held liable for the damage that occurs to the Data subject and/or incomplete own personal data or when he did not inform about their changes properly and in time.

8.2. The Company does not have the right to fully guarantee that www.gosavy.com website functioning will be continuous and without any disruptions or mistakes, that the www.gosavy.comwebsite will be completely secured from viruses and other truthful components. Data Subject is informed that any kind of material, which the Data Subject reads, downloads or obtains in other ways by using the Company's website, is exclusively obtained at the discretion and risk of the Data Subject and inly the Data Subject is responsible for the damage done to the Data Subject and the Data Subject's computer system.

8.3. If the Data Subject is a registered user at www.gosavy.comwebsite, the Data Subject takes full risk and responsibility, except cases, when the Company improperly performed their duties, for the actions of third parties at the www.gosavy.com website, performed by using the Data Subjects log-in data, and commits to perform all duties taken upon by using the Data Subjects log-in data.

9. FINAL PROVISIONS

9.1. Data Subjects can get familiarised with these Rules at www.gosavy.com.

9.2. These Rules can be reviewed once per calendar year by the initiative of the Data Manager and (or) when legal acts are changing, regulating the management of personal data.

9.3. By these Rules and the relationship arising due to these Rules, the law of the Republic of Lithuania is applied.

9.4. All disagreements arising due to the performance of these Rules are solved by negotiations. If there is no agreement achieved, disputes are solved according to the odder or legal acts of the Republic of Lithuania.

9.5. These rules come into effect on the 25th of May, 2018.

All questions related to these Rules and/ or data security in general can be consulted by the contacts provided below:

E-mail: labas@savy.lt

Phone No.+370 (5) 272 0151

Last updated: August 20, 2018