UAB Ride Share

PRIVACY POLICY

Vilnius
2023

RIDE SHARE UAB
PERSONAL DATA PROCESSING POLICY

1. KEY DEFINITIONS

1.1. "**Responsible Person**" shall mean the Employee of the Data Controller who, by nature of his work, is entitled to fulfil the specific functions related to Processing.

1.2. "**GDPR**" shall mean 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)

1.3. "**Employee**" shall mean a person who has concluded an employment contract or a similar contract with the Data Controller.

1.4. "**Data/Personal Data**" shall mean any information relating to an identified or identifiable natural person (Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.5. "**Recipient**" shall mean a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

1.6. "**Data Subject**" shall mean a Client or any other person whose Personal Data is processed by the Data Controller.

1.7. "**Processing**" shall mean any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, blocking, erasure or destruction;

1.8. "**Processor**" shall mean a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

1.9. "**Controller**" shall mean Ride Share UAB, legal entity registration number 304136890, registered at the address Aukštaičių st. 7, Vilnius.

1.10. "**Client**" shall mean a person who uses or earlier used the services provided by the Controller.

1.11. "**Mobility Surveillance**" shall mean collection and processing of data on Clients using the vehicles belonging to the Controller irrespective of whether the data is recorded in a file or not.

1.12. "**Policy**" shall mean this Personal Data Processing Policy.

1.13. For the purposes of this Policy, other terms correspond to the terms used in the GDPR, the Republic of Lithuania Law on Legal Protection of Personal data (hereinafter referred to as the "**LLPPD**") and the Republic of Lithuania Law on Electronic Communications (hereinafter referred to as the "**LEC**").

2. GENERAL PROVISIONS

2.1. The Controller shall collect certain Personal Data for the purposes of administration, conduct of own business and exercise of the legal duties.

2.2. This Policy shall regulate the main principles of and procedure for collection, processing and storage of Personal Data of the user of the website www.spark.lt administered by the Controller

(hereinafter referred to as the "**Website**") and the SPARK mobile application (hereinafter referred to as the "**Mobile Application**") (Client). Before starting using the Website and/or the Mobile Application, you must carefully read and familiarize with this Policy. By using the services provided by the Controller you confirm that you agree to comply with this Policy.

2.3. The Data Subject shall not be entitled to use the Website and/or the Mobile Application if he has not familiarized himself with the Policy and/or do not accept it. In cases where the Data Subject does not agree with the Policy or the respective part thereof, he must not use the Website and/or the Mobile Application. Otherwise, the Client shall be deemed to have familiarized with and unconditionally accepted the Policy.

2.4. The Controller shall respect the privacy of the Data Subjects. This Policy shall explain the acceptable practice concerning privacy in our company. It explains the ways of collection and use of your Personal Data and the rights exercised by you.

2.5. Use of the services of third parties such as the social network Facebook services may be subject to the terms and conditions of third parties. For example, all users and visitors of Facebook are subject to the Data Policy. Therefore, for the purposes of use of the services of third parties, it is recommended to familiarize with their applicable conditions.

2.6. The Data Subject shall assure that he meets the following main data protection principles:

2.6.1. Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject (lawfulness, fairness and transparency);

2.6.2. Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing of Personal Data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (purpose limitation);

2.6.3. Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization);

2.6.4. Personal Data shall 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);

2.6.5. Personal Data kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the Data Subject (storage limitation);

2.6.6. Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (integrity and confidentiality).

2.6.7. The Controller shall be responsible for and be able to demonstrate compliance with the principles set out herein above (accountability).

2.7. Data shall be processed by giving a due notice to the Data Subjects.

2.8. Data shall be stored for the periods specified for each type of Personal Data provided herein. Storage shall be carried out according to the procedures provided for in Section 6 hereof.

2.9. The Controller's rights of access to the data shall be withdrawn in case of termination of the agreement on processing of Personal Data concluded with the Controller or upon expiry of the agreement.

2.10. Data shall be transmitted to the Controllers and the Recipients where the legal acts provide for the right and/or the duty to do this on the respective grounds.

2.11. The Controller shall be entitled to provide Personal Data to the pre-trial investigation institution, prosecutor, or court for the purposes of administrative, civil, criminal proceedings as evidence or in other cases established in the law.

3. PROCESSING OF PERSONAL DATA FOR THE PURPOSE OF PROVISION OF ELECTRIC CAR SHARING SERVICE

3.1. The Controller shall provide to its Clients the electric car sharing service for the provision of which the following groups of Data of the Clients shall be processed:

3.1.1. Name;

3.1.2. Surname;

3.1.3. Personal identification number;

3.1.4. Place of residence (address);

3.1.5. E-mail address;

3.1.6. Telephone number;

3.1.7. Driving license photo (front side photo), No, date and place of issue, validity;

3.1.8. Certain data on the payment cards used by the Client received from the company providing the card handling service (type of the card, part of the card No);

3.1.9. Biometric data – photo of Clients' face.

3.2. The Data referred to in paragraphs 3.1.1 – 3.1.9 hereof shall be received directly from the Client, but a part of Data recorded in the system may also be received from the Client's employer if the Client uses the services of the Controller as a client or employee of the respective company.

3.3. In order to provide services, The Controller must collect afore-mentioned Data.

3.4. For the purposes of registration and recording of the Clients, conclusion, administration and performance of a contract, protection and control of the assets held by the company, the Controller shall additionally provide the following Data:

3.4.1. Number, date and place of issue and expiry date of the identity card (where other identification measures are not sufficient, they were unreliable etc.);

3.4.2. Categories of the vehicles which the Data Subject is entitled to drive, the date of granting thereof and the date of expiry;

3.4.3. Location of the vehicle, distance covered, date, time and duration of use of the vehicle;

3.4.4. Moment of unlocking and locking of the vehicle;

3.4.5. Change in the vehicle battery charge level while the Client uses the vehicle;

3.4.6. Charged fee;

3.4.7. Data on the debt;

3.4.8. Data on debts (level of the debt, amount of the debt, date of incurring the debt, time limit, date of payment).

3.5. The Controller shall not transmit the afore-mentioned Data of the Clients to the Recipients. The Data of former Clients shall be provided only to law enforcement authorities under the procedure established in the law.

3.6. The legal grounds for processing of Personal Data shall be Article 6(1)(b) and Article 6(1)(c) of the GDPR.

3.7. To check the validity of the driving licence, the Controller shall provide certain Personal Data (such as the number of the driving licence and personal identification number) to the manager of the Register of Drivers of Road Vehicles of the Republic of Lithuania, i.e. State Enterprise Regitra.

3.8. In order to ensure the quality of the services provided, to promptly respond to the Clients' questions, the employees of the Data Controller acting as customer service specialists are responsible for the Clients' calls and provide consultations by phone 24/7. The data manager records the records of conversations between the data manager and the client, which are kept for 180 (one hundred and eighty) days.

3.9. In pursuance of providing services and ensuring proper provision thereof, the Controller shall subcontract UAB RUPTELA as the Processor providing information, allowing to establish the location of the vehicle, parking time, speed of the vehicle, distance covered, date, time and duration of use of the vehicle, the moment of unlocking and locking of the vehicle, the change in the vehicle battery charge level while the Client uses the vehicle, information on whether the vehicle is being charged and if the door of the vehicle is closed.

3.10. In order to ensure smooth and high quality settlement for the provided services, the Controller shall subcontract the payment operation administrators Adyen and Paysera which mediate in performance of the payment operations. The Controllers have implemented payment card security standard (PCI DSS). For the accounting purposes the Controller shall subcontract accountants and internal accountant systems.

3.11. In cases where the Client violates the car use contract and/or does not pay for the services provided by the Data Controller and has other overdue payments, and the Data Controller seeks to recover the incurred debt, the Data Controller collects data about the debtor (name, surname, personal identification number, e-mail, phone No., address,) and data on indebtedness (debt amount, amount of debt, date of occurrence, term, date of payment, account or claim number) are transferred to Data Processors - debt collection companies with whom separate personal data processing agreements have been concluded. For this purpose, the Data Controller may transfer the data of the Client and his debt to the following Data Processors: UAB Legal Balance, legal entity code 302528679, UAB "Julianus Inkaso", legal entity code 300115639, UAB "Gelvorasergel", legal entity code 125164834, UAB EASY DEBT SERVICE, legal entity code 304406834.

3.12. In order to ensure functioning of the electric car rental system of the appropriate quality, the Controller shall subcontract Processors which shall carry out administration of the electric car rental platform, system programming and maintenance works.

3.13. In order to prevent fraud and ensure high quality of the providing services and security of the assets belonging to the Controller, the Controller shall ask to provide Data Subject his selfie and the photo of driving licence in accordance with identification of Data Subject. This data is not stored by the Data Controller. To achieve this goal, the Data Controller has used the Data Sub-Processor JUMIO Corporation, which has implemented the security standard (PCI DSS). When the Client's account is cancelled, the biometric data is securely deleted from JUMIO's systems. The Controller shall not transmit the Data to the third parties.

3.14. The data Sub-Processor JUMIO Corporation is located and acting in the United States of America, thereof the Data is transmitting over European Union boundaries. Such Data transmit is executed by providing high quality Data security. Data Controller and Processor is implemented the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. A copy of these terms and conditions may be obtained by contacting the Data Controller by contacts specified in this Policy.

3.15. The Controller shall also subcontract Amazon Web Services Limited as the Data Subject performing the server rent and placement services. This sub-Processor is located and operates

in the United States of America, so the data might be transferred outside the European Economic Area. This Data Processor is certified according to the requirements of the data protection agreement between the European Union and the United States of America (also known as Privacy Shield). Amazon Web Services Limited certification can be found by clicking on the following link: https://www.privacyshield.gov/participant?id=a2zt0000000TOWQAA4&status=Active.

3.16. Into account to, if the Client for any reason does not have the opportunity or does not agree to provide an image of his face so that it can be compared with the photo on his driver's license, such a person is given the opportunity to come to the office of the Data Controller at Paupio st. 50, Vilnius, where the Client's identity would be determined upon presentation of the driver's license. In such cases, a copy of the driver's license, if the driver's license was issued in the Republic of Lithuania, is not stored.

4. PROCESSING OF PERSONAL DATA FOR THE PURPOSES OF DIRECT MARKETING

4.1. The Controller shall carry out direct marketing in respect of the Clients.

4.2. In order to receive proposals for the services provided by the Controller, the Client shall market his consent to processing of Data for the purposes of direct marketing at the moment of registration or log in to his personal account and choose the newsletter receipt function.

4.3. The Controller shall process the following Personal Data of the Clients for the purposes of direct marketing:

4.3.1. Name;

4.3.2. Surname;

4.3.3. E-mail address;

4.3.4. Telephone number;

4.3.5. Address.

4.4. The Controller shall also carry out direct marketing (sending of newsletters and proposals by e-mail) in respect of the persons who have entered their e-mail on the Controller's website www.spark.lt and/or in the Mobile Application and expressed their willingness to receive such notices. In such case, the Controller shall process the e-mail address of such person.

4.5. The Data processed for the purposes of direct marketing shall not be transmitted by the Controller to the Recipients.

4.6. The legal grounds for processing of Data shall be Article 6(1)(a) of the GDPR.

4.7. When processing Data for the purpose of direct marketing, the Data Controller uses the Airship platform, through which newsletters are sent to Data Subjects, as well as Amazon Web Services Limited as a Data Sub-Processor, performing workstation rental and hosting services. Amazon Web Services Limited's certification can be found by clicking on the link on clause 3.15 of this Policy, and Airship's data protection can be found here: https://www.airship.com/legal/data-processing-addendum/

4.8. If, for any reason, the Client is unable or unwilling to submit his / her face image to be compared with the photograph on his / her driving license, such person shall be given the opportunity to visit the Controller's office at Paupio st. 50, Vilnius, where the Customer shall be identified. In such cases, a copy of the driving license, if issued in the Republic of Lithuania, shall not be kept.

5. DATA PROCESSING BY GOOGLE ANALYTICS FOR ADVERTISING PURPOSES

5.1. The Data Controller, based on the need to segment and better understand its Clients and their use of Data Controller's services, uses Google Analytics 4 (formerly known as Google Universal Analytics) advertising features to display personalized ads to Clients in the Mobile application.

5.2. By using the Google Analytics 4, the Data Controller grants the right to collect Customer Mobile application data through the "Google Signals" controller. More information about Google's privacy and data collection can be found here: Google Safety Center - Stay Safer Online.

5.3. By using Google Analytics 4 and enabling the "Google Signals" controller, the Data Controller does not transmit any individual's Personal data to Google that could identify a specific person. For this specific purpose, the Data Controller only shares the following Client Mobile Application data:

5.3.1. Google-generated Client Mobile Application ID (hereinafter - Mobile Application ID);

5.3.2. The country where the Mobile Application is being opened based in the Mobile Application ID;

5.3.3. The date when the Mobile Application was first launched based on Mobile Application ID;

5.3.4. The date when the registration was made using the Mobile Application based on Mobile Application ID;

5.3.5. Information on whether a payment card is attached to the Mobile Application based on Mobile Application ID;

5.3.6. Information on whether a valid driver's license is attached to the Mobile Application based on Mobile Application ID;

5.3.7. Information on when the Mobile Application is opened based on Mobile Application ID;

5.3.8. Information on when the Mobile Application is logged in based on Mobile Application ID;

5.3.9. Information about payments made through the Mobile Application (amount, currency, purpose of payment (type of service, membership extensions, and suspensions)) based on Mobile Application ID.

5.4. In all cases, the Data Controller implements technical and organizational measures for the security of personal data, as specified in Section 12 of this Policy.

6. DATA COLLECTED BY THE MOBILE APPLICATION

6.1. The Data Controller allows the Mobile Application to collect and process the location of the Client's mobile device, but only for those Clients who have given the Mobile Application access to such information on their mobile device. Clients, controlling the processing of their personal data using the Mobile Application, can choose which mobile device data the Clients allows the Mobile Application to access or otherwise use. With the Client's permission, the Mobile Application only gets access to the location of the Client's mobile device.

6.2. The Data Controller collects data on the location of the Client's mobile device in order to increase and improve the availability of the services provided by the Data Controller.

6.3. Client mobile device location data is not transmitted to the Data Recipients.

6.4. In all cases, the Data Controller implements technical and organizational measures for the security of personal data, as specified in Section 12 of this Policy.

7. MOBILITY SURVEILLANCE

7.1. The Controller shall carry out mobility surveillance of the vehicles transferred to the Clients for use.

7.2. Mobility surveillance shall be aimed at ensuring security of the assets belonging to the Controller, use of the provided services by the Clients in a good faith and proper manner and provision of the services of the appropriate quality.

7.3. Mobility surveillance shall be carried out by means of the GPS transmitters installed in the vehicles belonging to the Controller.

7.4. Mobility surveillance data shall not be transmitted to the Recipients.

7.5. The legal grounds for processing of Data shall be Article 6(1)(b) and Article 6(1)(f) of the GDPR.

7.6. To carry out mobility surveillance, the Controller shall subcontract RUPTELA UAB as the Controller providing information allowing determining the location of the vehicle, itinerary and distance covered.

8. PERIODS OF RETENTION OF DATA

8.1. The Controller shall apply different periods of retention of Personal Data depending on the categories of processed Personal Data.

8.2. The Controller shall apply the following periods of retention of Personal data:

No	Categories of Personal Data	Period of retention
1.	Personal Data of the Clients processed for the purposes of provision of the electric car sharing service	2 years from the later of the date of termination of the agreement or the date of redemption of the debt. Data of the Clients whose accounts are inactive shall be stored for 3 years from the date of the last login to the system.
2.	Data used for the purposes of direct marketing	2 years from the date of the last login to the system.
3.	Mobility surveillance data	2 years from the later of the date of termination of the agreement or the date of redemption of the debt. Data of the Clients whose accounts are inactive shall be stored for 2 years from the date of the last login to the system.
4.	Client mobile device location data	1 year from the last connection to the Mobile Application.

8.3. Exceptions to the afore-mentioned periods of retention may be established insofar as such deviations do not infringe the rights of the Data Subjects, meet the legal requirements and are properly documented.

8.4. The documents in respect of which the Controller has issued an order on suspension due to litigation shall be stored and destroyed according to the instructions of the law department.

9. RIGHTS OF THE DATA SUBJECTS

9.1. The Data Subject shall be entitled to exercise the following rights under the procedure established in the GDPR and the LLPPD:

9.1.1. Right to be informed;

9.1.2. Right of access;

9.1.3. Right to erasure;

9.1.4. Right to update;

9.1.5. Right to restrict processing of data;

9.1.6. Right to data portability;

9.1.7. Right to object;

9.1.8. Rights related to automatic adoption and profiling of decisions.

9.2. If Data Subject is not satisfied with Data Collector's answer or believe that Data Collector process Data Subject's personal data not in accordance with the legal requirements, Data Subject may lodge a complaint to the State Data Protection Inspectorate of the Republic of Lithuania.

9.3. The rights referred to in paragraphs 9.1.2 - 9.1.8 hereof shall be exercised within the periods set forth in the GDPR.

9.4. The afore-mentioned periods set forth in the GDPR shall be as follows:

Request of the Data Subject	**Period**
Right to be informed	When Data is collected (if Data is provided by the Data Subject) or within one month (if Data is provided not by the Data Subject)
Right of access	One month
Right to update	One month
Right to erasure	Without undue delay
Right to restrict Processing	Without undue delay
Right to data portability	One month
Right to object	After receipt of an objection
Rights related to automatic adoption and profiling of decisions	Not specified

9.5. The Data Subject shall have the right to reasonably refuse to allow the Data Subject to exercis circumstances provided for in Article 12(5)(b) of the GDPR.

10. DATA PROTECTION OFFICER

10.1. Pursuant to the GDPR, in cases where the core activities of the Controller consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data, the Data Protection Officer shall be obligatory.

10.2. The rights and duties of the Data Protection Officer shall be detailed in the GDPR, the annexes to the Policy, the job descriptions if the position is occupied by an employee of the Controller or in the service contract if the position of the Data Protection Officer is occupied by an external service provider.

10.3. In the light of the afore-mentioned criteria and the activities carried out by the Controller, the Controller is appointed Data Protection Officer with whom you could contact by email legal@spark.lt.

11. PROCEDURE FOR MANAGEMENT OF PERSONAL DATA BREACHES AND ADDRESSING SUCH BREACHES

11.1. Should the Employees of the Controller having the right of access to Data notice any Data breaches (omission of action or actions by the persons which may result or result in Data security risk), they shall notify the Responsible Employee and/or their line manager.

11.2. Having considered the data protection breach risk factors, the degree of impact of the breach, damage and consequences, following the respective internal procedures, the Controller shall take decisions on the measures necessary for remedy of the Data breach and consequences thereof and notification of the respective entities.

12. TECHNICAL AND ORGANIZATIONAL PERSONAL DATA SECURITY MEASURES

12.1. The organizational and technical data security measures implemented by the Controller shall en such security level which corresponds to the nature of the Data processed by the Controller and Data processing risk including, but not limited to the measures set out in this Section.

12.2. The Personal Data security measures shall be as follows:

12.2.1. Administrative (establishment of the procedure for secure document and computer data and archives thereof and organization of work of different areas of activity, briefing of the personnel at the moment of employment and leaving the job/dismissal etc.);

12.2.2. Technical and software protection (administration of servers, information systems and databases, maintenance of workplaces, protection of operating systems, surveillance (monitoring) of users' access, protection against computer viruses etc.);

12.2.3. Administration of information systems and databases, maintenance of workplaces, protection of operating systems, protection against computer viruses etc.;

12.2.4. Protections of communications and computer networks (technical and software measures of encoding and transmission of common use data, applications, Personal Data, filtering of undesirable data packages etc.).

12.2.5. Two-factor authentication (2FA), which acts as an additional security measure, is designed to ensure that the Client is the only person who can access their account, even if others know the Client's password. For all clients registered after 10th August 2022 2FA is mandatory, but after successful registration, the Client has the right to refuse it through the Mobile Application. Client registered until 210th August 2022 can turn on 2FA in Mobile application by going to my account -> settings -> turn on 2FA.

12.3. The afore-mentioned Personal Data protection measures shall ensure: 1) equipment of a repository of copies of operating systems and databases, control of keeping of copying equipment; 2) uninterrupted data handling (processing) process technology; 3) strategy for restoration of functioning of the systems in emergency cases (management of uncertainties); 4) unique user identification and password system; 5) physical (logical) separation of the application testing environment from the operational mode processes; 6) registered use of data and inviolability of data.

12.4. The Controller shall ensure the procedure of restoration of Personal data in cases of emergency loss of the Data. The Controller shall make backup copies of the data available in the system. Data shall be retrieved according to the internal procedure using Amazon Web Services software from the backup copying equipment libraries. In all cases, backup of Data shall be stored without prejudice to the Data retention period set out in the Policy.

12.5. The Controller shall also apply other measures ensuring security of Personal Data:

12.5.1. VPN technology shall be used for remote connection to the Controller's internal network, digital certificate shall be used for identification of the user;

12.5.2. Access to Personal Data by organizational and technical data security measures recording and controlling the efforts of registration and acquisition of rights shall be controlled;

12.5.3. The following entries of login to the database by the persons granted the right to process Personal Data shall be recorded: login identifier, date, time, duration, login result (successful, unsuccessful). The afore-mentioned entries shall be stored at least for 1 (one) year;

12.5.4. Security of the premises in which Personal Data is stored shall be ensured (only access pf authorized persons to the respective premises shall be ensured etc.);

12.5.5. The enquiries for search of provided Personal Data shall be aimed at identifying the person and checking the validity of his driving license;

12.5.6. Attempts to ensure use of secure protocols and/or passwords by providing Personal Data through external data transmission networks shall be made;

12.5.7. Control of security of Personal data in external data carriers and e-mail and deletion thereof after use of Personal Data by transferring them to the databases shall be ensured;

12.5.8. Emergency Personal Data restoration actions (when and who carried out the Personal Data restoration actions by automatic and non-automatic means) shall be recorded;

12.5.9. It shall be ensured that testing of information systems was not carried out with real Personal Data except for the cases where organizational and technical Personal Data security measures ensuring real security of Personal Data shall be used;

12.5.10. Personal Data in portable computers if they are used not in the Controller's data transmission network shall be protected by the respective measures corresponding to the Processing risk.

12.6. The Controller shall implement appropriate technical and organizational measures ensuring standardized processing of Personal Data which is required for the particular data processing purpose. The afore-mentioned obligation shall be applicable for the quantity of collected Personal Data, the scope of processing thereof, the period of retention of Personal Data and accessibility of Personal Data.

13. CONTACT DETAILS

13.1. You may contact for the issues concerning this Policy and/or protection of data in general according to the following contact details:

E-mail: info@spark.lt

Tel. 8 700 77275

14. FINAL PROVISIONS

14.1. The Policy shall be revised on a calendar year basis on the initiative of the Controller and/or in case of any amendments to the legal acts regulating processing of Personal Data.

14.2. The Policy and amendments thereto shall come into force as of the date of approval thereof.