Ride Share UAB

WEBSITE PRIVACY POLICY

Vilnius
2019

Table of contents

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 Employee of the Data Controller 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, organisation, 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 Konstitucijos pr. 21C, 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 the Employees and 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.espark.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 familiarise 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 familiarised 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 familiarised 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 familiarise 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 minimisation);

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 organisational 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 unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational 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 for herein. Storage shall be carried out according to the procedures provided for in Section a 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. Date of birth;

3.1.5. Place of residence (address);

3.1.6. E-mail address;

3.1.7. Telephone number;

3.1.8. Driving licence photo, No, date and place of issue, validity;

3.1.9. 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);

3.1.10. Biometric data – photo of Customers' face.

3.2. The Data referred to in paragraphs 3.1.1 - 3.1.8 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. 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:

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

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

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

3.3.4. Moment of unlocking and locking of the vehicle;

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

3.3.6. Charged fee;

3.3.7. Data on the debt;

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

3.4. 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.

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

3.6. 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.

3.7. In pursuance of providing services and ensuring proper provision thereof, the Controller shall subcontract RUPTELA UAB 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.

3.8. In order to ensure smooth and high quality settlement for the provided services, the Controller shall subcontract the payment operation administrators Adyen and Braintree which mediate in performance of the payment operations. The Controller has implemented payment card security standard (PCI DSS).

3.9. In order to 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. For this purpose, the Controller shall subcontract the Processor JUMIO which has implemented data security standard (PCI Level1). The Controller shall not transmit the Data to the third parties.

3.10. In order to ensure functioning of the electric car rental system of the appropriate quality, the Controller shall subcontract Media park UAB as the Processor which shall carry out administration of the electric car rental platform, system programming and maintenance works.

3.11. In the light of the fact that the Controller provides car rental services in the Republic of Bulgaria in which the company providing the electric car sharing service Ride Share Bulgaria AD is established, the persons employed by the afore-mentioned company have access to the common car rental system. The Controller shall confirm that in order to ensure protection of data, all technical and organisational data protection measures have been implemented.

3.12. The Controller shall also subcontract Amazon Web Services Limited as the Data Subject performing the server rent and placement services.

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 espark.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 purposes of direct marketing, the Controller shall use Mixpanel platform through which newsletters are sent to the Data Subjects and Amazon Web Services Limited as the Processor performing the server rent and placement services.

5. MOBILITY SURVEILLANCE

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

5.2. 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.

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

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

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

5.6. 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.

6. PERIODS OF RETENTION OF DATA

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

6.2. 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.

6.3. 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.

6.4. 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.

7. RIGHTS OF THE DATA SUBJECTS

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

7.1.1. Right to be informed;

7.1.2. Right of access;

7.1.3. Right to erasure;

7.1.4. Right to update;

7.1.5. Right to restrict processing of data;

7.1.6. Right to data portability;

7.1.7. Right to object;

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

7.2. The rights referred to in paragraphs 7.1.2 - 7.1.8 hereof shall be exercised within the periods set forth in the GDPR.

7.3. 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

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

8. DATA PROTECTION OFFICER

8.1. 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.

8.2. 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.

8.3. 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@nnv.lt.

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

9.1. 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.

9.2. 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.

10. TECHNICAL AND ORGANISATIONAL PERSONAL DATA SECURITY MEASURES

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

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

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

10.2.2. 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.);

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

10.2.4. 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.).

10.3. 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.

10.4. 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.

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

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

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

10.5.3. 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;

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

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

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

10.5.7. 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;

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

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

10.5.10. 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.

10.6. The Controller shall implement appropriate technical and organisational measures ensuring standardised 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.

11. CONTACT DETAILS

11.1. 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@espark.lt

Tel. 8 700 77275

12. FINAL PROVISIONS

12.1. 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.

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

UAB RIDE SHARE
COOKIES POLICY

1. MAIN DEFINITIONS

Cookies – a small text file saved by the Website in the User's computer or mobile device when the User accesses the Website. Cookies help the Website to recognize the User's device. Cookies are used to ensure quality performance of the Website and more pleasant experience for Users.

SPARK – UAB Ride Share, legal entity code 304136890, registered address Konstitucijos pr. 21C, Vilnius.

User – a private individual who uses the Website.

Website – the website accessible at www.espark.lt

Policy means this Cookie Policy.

2. TYPES OF COOKIES

2.1. Cookies used on the SPARK Website are intended to ensure quality performance of the Website. These cookies are necessary for the Website to function properly and cannot be switched off. These cookies do not store any data which can identify the User and are deleted when the User leaves the Website. Furthermore, to ensure more effective assess to the Website, functional cookies are used. Functional cookies apply with respect to the User who repeatedly visits the Website as they remember settings made by the User on the Website. These cookies allow us to calculate the number of Website visitors and traffic sources so that we can measure and improve the performance of the Website. They help us to keep track of which pages are the most popular and how the User uses the Website. For this purpose, SPARK uses the Google Analytics statistics. SPARK does not disseminate the collected information. The collected information is completely anonymous and does not identify the User.

2.2. The following cookies are used on the Website:

Name	Provider	Description	Duration	Moment of creation
PHPSESSID	espark.lt	Standard cookie for upholding the user session.	Until closing the Website page	Entering the website first time
_utmb, _utmc, _utma	espark.lt	Google Analytics session cookies. Information is sent to the	30 minutes, 6 months and 2 years, respectively	Entering the website

		server anonymously. Cookies identify unique visitors and monitors user sessions. For more information, see Google website.		
__utmt	espark.lt	Google Analytics cookie that provides information on how the user accesses the web page.	6 months from installation/upgrade	Entering the website
__utmz	espark.lt	Google Analytics session cookies. Information is sent to the server anonymously.	Until closing the Website page	Entering the website
_fbp	espark.lt	Used by Facebook to provide a series of advertisement products such as real-time bidding from third-party advertisers.	1 day	Entering the website
_icl_current_language	espark.lt	A cookie used to store the user language preference.	24 hours	Entering the website
1P_JAR, CONSENT	gstatic.com	Google Analytics cookie for enabling session.	Most of the cookies expire 1 month after visiting a page which contains a Google Map.	Entering the website

3. USER CONSENT AND REFUSAL OF COOKIES

3.1. When the User enters the Website for the first time, a notification table on Website cookies is provided. By clicking an "Accept" button the User agrees to our use of cookies on the Website. The Website remembers this consent of the User for the use of cookies and this question is not asked each time the User visits the Website.

3.2. The User may at any time withdraw his consent to the use of cookies by turning them off by way of changing his browser settings. It should be noted that using the browser settings which block cookies (including the necessary cookies) may cause problems in using all or part of the Website functions.

3.3. If the User deletes the cookies, all User settings made prior to it will be deleted.

4. GENERAL PROVISIONS

4.1. If necessity, SPARK may amend the Policy by publishing its updated version on the Website. Any supplements and amendments to the Policy shall enter into force on the day when they are published on the Website.

4.2. SPARK shall not be liable for any damage, including the damage caused by an act or omission of the User or third parties acting with the User's knowledge, including false data input, other errors, deliberate damage, other misuse of the Website, electricity supply or internet access failures, etc.

4.3. For any further queries regarding the Policy, please contact SPARK by email: info@espark.lt.