SPARK CAR SHARING S.R.L.

PRIVACY POLICY

Bucharest
August 2022

Content

KEY DEFINITIONS

GENERAL PROVISIONS

PROCESSING OF PERSONAL DATA FOR THE PURPOSE OF PROVIDING AN ELECTRIC VEHICLE SHARING SERVICE

PROCESSING OF PERSONAL DATA FOR THE PURPOSE OF DIRECT MARKETING MOBILITY MONITORING

DATA STORAGE PERIODS

RIGHTS OF THE DATA SUBJECT

DATA PROTECTION OFFICER

PROCEDURE FOR MANAGING PERSONAL DATA SECURITY BREACHES AND DEALING WITH SUCH BREACHES

TECHNICAL AND ORGANIZATIONAL MEASURES FOR PERSONAL DATA SECURITY

CONTACT DETAILS

FINAL PROVISIONS

1. KEY DEFINITIONS

1.1. **"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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).

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

1.3. "**DPA**" means a data processing agreement to be entered into with each Processor in accordance with the terms set out in section 3 below.

1.4. **"Recipient"** means the individuals or legal entity, public body, agency, or other structure to which the Personal Data is disclosed, whether or not it is a third party.

1.5. **"Data subject"** means a Customer or employee of the Controller as well as any other person whose Personal Data is processed by the Controller.

1.6. **"Processing"** means any operation or set of operations performed on Personal Data or a set of Data by automatic or other means such as collection, recording, organization, structuring, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, distribution, or other way in which the data is made available, arranged, or combined, restricted, deleted or destroyed.

1.7. **"Processor"** means individuals or legal entities, public bodies, agencies, or other structures that processes Personal Data on behalf of the Controller.

1.8. "**Controller**" means SPARK CAR SHARING S.R.L., a limited company legally registered under the Romanian laws, having its registered office in Bucharest, District 1, 175 Calea Floreasca, 5th Floor, B side, www.espark.ro, email: office@espark.ro, registration no within the Trade Register: J40/17015/2018, VAT code: RO40219027.

1.9. **"Customer"** means a person who uses or has used the services provided by the Controller.

1.10. **"Mobility Monitoring"** means the collection and processing of data about employees and Customers using the vehicles belonging to the Controller, whether or not the data is recorded in a file.

1.11. **"Policy"** means this Privacy Policy.

1.12. **"Owner of the Mobile Application"** means **UAB SPARK TECHNOLOGIES**, a limited liability company established and existing under the laws of Lithuania, legal entity code 304953141, Vilnius, Lithuania. As far as the Data Subjects on the territory of Romania use the SPARK mobile application, SPARK CAR SHARING S.R.L. acts as a **joint controller** with the Owner of the Mobile Application**; for avoiding any misunderstandings, the owner of the website espark.ro is** SPARK CAR SHARING S.R.L..

1.13. For the purposes of this Policy, the remaining terms correspond to the terms used in the GDPR, the Romanian Personal Data Protection Laws and the Romanian Electronic Document and Electronic Signature Laws.

2. GENERAL PROVISIONS

2.1. The Controller processes certain Personal Data for the purposes of conducting its activity, exercising its rights and legal interests, and complying with its legal and contractual obligations.
2.2. This Policy contains the basic principles and procedures for the processing of Personal Data of the Data Subjects of the **website http://espark.ro**, administered by the Controller (hereinafter referred to as the "**Website"**) and the SPARK mobile application (hereinafter referred to "**Mobile Application"**). Before starting to use the Website and/or Mobile Application, the Data Subjects should carefully read and familiarize themselves with this Policy. By using the services provided by the Controller, the Data Subjects confirm that they read, understood, and agree to comply with this Policy.
2.3. In cases where the Data Subjects do not agree with the Policy or the relevant part thereof, it is strongly recommended that they should not use the Website and/or the Mobile Application. Otherwise, it is considered that the Data Subjects have familiarized themselves with and unconditionally accepted the Policy, which they expressly agreed to upon registration.
2.4. The Controller values and respects the privacy of the Personal Data. This Policy explains the ways of collecting and using the Personal Data and the rights of the Data Subjects.
2.5. Use of third-party services, such as the services of the social network Facebook, etc. may be subject to the third-party terms and conditions. For example, all Facebook users and visitors are subject to their Data Privacy Policy. Therefore, for the purpose of using the services of third parties, it is recommended that the Data Subjects familiarize themselves with their applicable terms.
2.6. The Controller shall ensure that it complies with the following basic data protection principles:
2.6.1. Personal Data are processed lawfully, in good faith and in a transparent manner with respect to the Data Subjects (lawfulness, good faith and transparency);
2.6.2. Personal Data is collected for specific, explicit and legitimate purposes and is not processed in a way that is incompatible with these purposes; the subsequent processing of Personal Data for the purposes of archiving in the public interest, scientific or historical research or statistical purposes is not considered incompatible with the original purposes (purpose limitation);
2.6.3. Personal Data must be relevant, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation);
2.6.4. Personal Data must be accurate and, if necessary, updated; all reasonable steps must be taken to ensure that Personal Data which are inaccurate, having regard to the purposes for which they are processed, are deleted or rectified immediately (accuracy);
2.6.5. Personal Data stored in a form that allows the identification of Data Subjects is stored no longer than is necessary for the purposes for which the Personal Data is processed; Personal Data may be stored for longer periods insofar as they will be processed solely for the purpose of archiving for public interest, scientific or historical research or statistical purposes in accordance with Article 89, paragraph 1 of the GDPR provided that appropriate technical and organizational measures required by the GDPR to protect the rights and freedoms of the Data Subject (restriction of storage);
2.6.6. Personal Data is processed in a way that ensures adequate protection of 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 is responsible and should be able to prove compliance with the principles set out above (accountability).
2.7. Users of the mobile application must expressly read and agree to the Controller's privacy notice before registering to use the Mobile Application and/or the Website.
2.8. The Data is stored for the periods indicated for each type of Personal Data provided for in this policy. Storage is carried out in accordance with the procedures provided in this policy.
2.9. The rights of the Processor to access the Data shall be revoked in the event of termination of the DPA concluded with the Controller or upon expiry of the term of the agreement.
2.10. The Data is transferred to other Recipients when the legal acts provide the right and/or the obligation to do so on the relevant grounds.
2.11. The Controller will have the right to provide Personal Data to the state and/or local authorities for the purposes of administrative, civil, criminal proceedings, as evidence, or in other cases established by law.

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

3.1. The Controller provides its Customers with the service of sharing the use of electric cars, for the provision of which the following groups of Data are processed:
3.1.1. First name;
3.1.2. Last name;
3.1.3. Personal identification number;
3.1.4. Date of birth;
3.1.5. Place of domicile or residence (address);
3.1.6. E-mail address;
3.1.7. Phone number;
3.1.8. Driving license number, date and place of issue/issuing authority, validity;
3.1.9. Certain data about the payment cards used by the Customer, received from the company providing the card processing service, namely the card type and part of the card number; under no circumstances and by no means, the Controller retains, stores, or archives the whole card number and/or the CVV number, and has any access to such information before and after the moment the User Account registration application is submitted.
3.2. The data specified in paragraphs 3.1.1 - 3.1.9 are usually received directly from the Customer; however, part of the data recorded in the system might also be received from the Customer's employer or similar, if the latter contracted the services of the Controller.
3.3. For the purposes of registration, recording and reporting of Customers, conclusion, administration and execution of a contract, compliance with legal obligations (e.g. cars to be provided only to legally competent persons, compliance with accounting reporting requirements, reporting of violations, ensuring the accuracy of data), protection and control over the assets owned by the company, the Controller additionally processes the following Data:

3.3.1. Categories of vehicles that the Data Subjects have the right to drive, the date this right was granted and the date it expires;
3.3.2. Vehicle location, distance travelled, date, time, vehicle speed and duration of vehicle use;
3.3.3. time of unlocking and locking the vehicle;
3.3.4. change in the vehicle's battery charge level while the Customer is using the vehicle;
3.3.5. Fee charged;
3.3.6. Obligation data / Payments due;
3.3.7. Transaction data such as history of services used, data on obligations (level of obligation, amount of obligation, date of occurrence of obligation, deadline, date of payment) credit rating, accumulated eGo points, referral programmes points, rewards;
3.3.8. Correspondence regarding complaints, requests, opinions, evaluation of the services or of other users, etc.;
3.3.9. IT management data such as IP address, operating system, communication data and other metadata from the use of the application, location of the mobile device while in use;
3.3.10. Data related to legal or insurance claims: data on damage to the electric vehicles, security incidents/traffic accidents or other violations in case they occurred while you were using the electric vehicles (date, place, time of the traffic accident/violation, amount of damages, faults, etc.), unpaid debts, accrued penalties, etc.
3.4. Unless otherwise prescribed herein or within the Service Contract and the Vehicle Use Agreement, the Controller shall not transmit to the Recipients the above-mentioned data of the Customers, except the case when they are requested by the entitled authorities or are provided to the said authorities according to the relevant laws.
3.5. The legal grounds for the processing of Personal Data for the purposes specified in item 3.1. and 3.3 above, are mainly Article 6, paragraph1, letter "b" and Article 6, paragraph1, letter "c" of the GDPR, as well as Article 6 paragraph 1, letters ''a'' and ''f'', as the case may be.
3.6. On the basis of the Controller's legitimate interest in business development (Article 6, paragraph 1, letter "f" of the GDPR), anonymized aggregated data about the services used by Customers may also be used for the purposes of statistical analysis and marketing research after complete removal of the identifying customers Personal Data.
3.7. With the consent of the Data Subjects, data on the location of their mobile device may also be obtained while using the Mobile Application for the purpose of notification of available electric vehicles in the immediate vicinity and reporting of services while using the Mobile Application. The Data Subjects have the right to withdraw their consent so given at any time by changing the settings of their mobile device.

3.8. In order to verify the validity of the driving license, the Controller must provide certain Personal Data (such as the driving license number and personal identification number) to the Processors responsible for verifying the registered Personal Data and for technical and administrative Customer support.
3.9. When providing services and ensuring their proper performance, the Owner of the Mobile Application provides to and receives from **RUPTELA UAB** (a company registered under the Lithuanian laws, having its registered office at 6 Perkūnkiemio Str, LT-12130 Vilnius, Lithuania**,** LT100003432316, www.ruptela.com, info@ruptela.com) and to

LEMATICS UAB (a company registered under the Lithuanian laws, having its registered office at 25 Lvovo Str, LT-09320, Vilnius, Lithuania, LT100010749217, www.lematics.com, info@lematics.com), as Processors, information that allows to establish the location of the vehicle, the period of parking, the speed of the Vehicles, the distance travelled, the date, the time and duration of the use of the Vehicles, the time the Vehicle are unlocked and locked, the change in the charge level of the Vehicles' battery, while the Customers are using the Vehicles, information whether the Vehicles are being charged and whether the Vehicles' doors are closed.

3.10. In order to ensure a smooth and high-quality payment settlement for the services provided, the Owner of the Mobile Application entered into a subcontract with the payment operations provider **Adyen N.V.** (a company registered with the Dutch Chamber of Commerce under number 34259528 and having its seat at Simon Carmiggeltstraat 6-50, 1011 DJ in Amsterdam, the Netherlands, www.adyen.com), which processes the payment operations.

3.11. The Owner of the Mobile Application also contracted **Amazon Web Services** as a Processor to perform the server rental and installation services.

3.12. The Controller concluded an agreement with the Owner of the Mobile Application as joint Controllers, which defines the respective responsibilities for the protection of Personal Data. According to this agreement, SPARK CAR SHARING S.R.L. is responsible for providing the information required by law and for processing the requests of Data Subjects, provided for in the GDPR, in Romania.

3.13. The Controller confirms that, in order to ensure data protection, all available and reasonable justified technical and organizational data protection measures have been implemented.

3.14. The Controller and/or the Owner of the Mobile Application, on behalf of the Controller, enter/s into agreements with Processors, which. process Personal Data only on behalf of the Controller for the purposes set out in the DPAs. In particular, each Processor shall:

- process Personal Data only in accordance with the Controller's documented instructions, including in relation to the transfer of Personal Data to a third country or international organization, unless required to deviate from such instructions to comply with the requirements of the GDPR and/or other mandatory legal requirements to which the Processor is subject. In such a case, the Processor must, without unreasonable delay, inform the Controller of the relevant requirement prior to the processing of Personal Data;
- ensure that the persons authorized to process the Personal Data have undertaken the obligation of confidentiality and compliance with the applicable data protection regulation within the EU or are bound by an appropriate legal obligation of confidentiality;
- support the Controller upon his express written request, with a view to ensuring the fulfilment of its legal obligations, such as those related to data security with the Controller, the assessment of the impact on data protection and prior consultation laid down in the GDPR, and, in particular, to implemented appropriate technical and organizational measures to protect the Personal Data covered by the DPA from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the Personal Data. The Processor shall be obliged to perform all of its obligations as a Personal Data Processor, in full compliance with the relevant laws, at its own expenses;

- support the Controller by implementing appropriate technical and organizational measures to fulfil the Controller's obligations in this capacity, namely: to respond to requests to exercise the rights of Data Subjects under the GDPR. The Processor must immediately notify the Controller of any request made by any Data Subject and not respond to the relevant request before receiving the Controller's instructions;
- provide the Controller with all the information necessary to prove compliance with the obligations of the Processor as specified in the DPAs and in the GDPR, and to allow and assist in audits, including inspections carried out by the Controller or another auditor authorized by the Controller;
- maintain accurate records of all processing activities under the DPAs in accordance with the requirements set out in the GDPR and provide the Controller with the relevant records within ten (10) working days of receiving the request from the Controller;
- ensures that no Personal Data is transferred, released, assigned, disclosed or otherwise made available to a third party without the prior express written consent of the Controller;
- ensures that data protection obligations similar to those set out in this document are imposed on other Processors of Personal Data who are engaged by the Processor by means of a contract. The Processor is responsible to the Controller for the fulfilment of these obligations by the other Processors;
- shall inform the Controller immediately if an instruction of the Controller violates the Data Protection Regulation or if Personal Data is or will be processed in violation of the Data Protection Regulation or the Agreement and informs the Controller immediately about complaints or audits by data protection supervisory authorities of the data related to the processing of Personal Data;
- shall inform the Controller without undue delay (but no later than 48 hours) after becoming aware of any security breach of Personal Data, which means, for instance, any security breach resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data that is transmitted, stored or otherwise processed. The notification must describe the nature of the violation, the number of Data Subjects affected, the likely consequences of the violation, the measure taken or proposed, as well as other data related to the violation listed in Article 33, paragraph 3 of the GDPR; and
- upon termination of the processing contract or at the Controller's written request, to destroy or return all Personal Data, unless otherwise provided for in the GDPR or mandatory national legislation within the EU to which the Processor is subject.

4. PROCESSING OF BIOMETRIC DATA FOR THE PURPOSE OF UNIQUELY AND ACCURATE IDENTIFICATION

4.1. The Controller processes, directly or indirectly, through Processors, the Customers' photo/s biometric Data for the purpose of:

- uniquely and accurate identification of the Customers during the User's Accounts' registration procedures;
- preventing unlawful use of the Vehicles, frauds and/or traffic accidents, as well as for the protection and control of the Controller's property and the establishment and exercise of legal claims, during and/or in relation to the Vehicle Use Periods,

when and where closed-circuit television cameras are installed and functioning into the Vehicles and/or outside of them.

4.2. The legal grounds for processing biometric data are the establishment and exercise of legal claims (Article 9, paragraph 2, letter f) of the GDPR).
4.3. For the purpose of collecting, processing and storing Customers' biometric data, the Owner of the Mobile Application entered into a biometric data processing contract with **JUMIO** Corporation (395 Page Mill Road, Suite 150, Palo Alto, CA 94306, USA, www.jumio.com), which is certified with the PCI DSS data protection certificate and provides a high level of protection equivalent to bank protection information.

4.4. The Processor is obliged to process the data solely for the purposes of accurate customer identification and for no other purposes. Although the check for data validation and confirmation of the Customers' identities is done by automated means, decisions to refuse registration are made only after human intervention and additional validation of documents.

5. PROCESSING OF PERSONAL DATA FOR DIRECT MARKETING PURPOSES
5.1. The Controller carries out direct marketing in relation to the Customers.
5.2. In order to receive direct marketing communications (i.e., special offers, promotional campaigns, adverts, coupons, and/or similar) for the services provided by the Controller, the Customers are asked to give their consent to the processing of Data for the purposes of direct marketing at the time of registration or enter their personal profile and select the option of receiving newsletters.
The communications, irrespective the way they are transmitted, including newsletters, by which the Customers are properly informed, from time to time, about the amendments to the General Terms and Conditions, the Rules for Vehicle Use, the Pricelist, The Vehicle Use Agreement, and/or the Policy, as well as those concerning temporary access limitations to the Mobile Application or the Website, safety issues and/or similar are not and shall be not deemed and/or constructed as being direct marketing communications. In such case, the processing is necessary for the performance of the contract between the Parties (art 6 para 1, point (b) of the GDPR), for compliance with the legal obligations prescribed by the customers' protection legislation, which the Controller is subject to (art 6 para 1, point (c) of the GDPR), as well as for the purposes of the legitimate interests pursued by the Controller (art 6 para 1, point (f) of the GDPR).
5.3. The Controller processes the following Personal Data of the Customers for the purposes of direct marketing:
5.3.1. Name;
5.3.2. Surname;
5.3.3. Email address;
5.3.4. Phone number;
5.3.5. Address.
5.4. The Controller also carries out direct marketing (sending newsletters and offers by e-mail) to persons who have entered their e-mail address on the Controller's web site espark.ro and/or in the Mobile Application and have expressed their agreement to receive

such communications. In such a case, the Controller processes the e-mail address of the relevant person.
5.5. The Data Subjects can withdraw their consent to the processing of Data for the purposes of direct marketing, at any time, and refuse to receive direct marketing communications by clicking on the "unsubscribe" link in the e-mail messages received, changing the notification settings from their account, or sending a targeted message requesting this.
5.6. The Data processed for the purposes of direct marketing is not transmitted by the Controller to the Recipients.
5.7. The legal grounds for Data processing for the purposes of direct marketing is Article 6, paragraph 1, letter “a” of the GDPR.
5.8. When processing Data for direct marketing purposes, the Controller uses the **Airship** platform, through which newsletters are sent to Data Subjects, as well as **Amazon Web Services,** as a Processor.

6. MOBILITY MONITORING
6.1. The Controller monitors the mobility of the vehicles provided to the Customers for use.
6.2. Mobility Monitoring aims to ensure the security of the assets belonging to the Controller, the use of the services provided, by the Customers, in good faith and in an appropriate manner, and the provision of the services with due quality, guaranteeing the security of the Customers and third parties.
6.3. Mobility Monitoring is carried out by means of GPS transmitters installed in the vehicles belonging to the Controller. The Data include information about the distance travelled, speed, route, and location of the vehicle.
6.4. Mobility Monitoring data are not transmitted to Recipients, unless otherwise prescribed by the relevant laws and/or provided herein, the Service Contract and the Vehicle Use Agreement.
6.5. The legal grounds for data processing are Article 6, paragraph 1, letters “b” and “f” of the GDPR.
6.6. In order to carry out Mobility Monitoring, the Controller contracted LEMATICS UAB, afore-identified.

7. AUTOMATED DECISION-MAKING
7.1. In order to provide high-quality services and rewards, the Controller uses automated decision-making to calculate e-Go points in a completely objective and non-discriminatory manner based on the Customer's kilometres travelled. The charged fee for the use of the services is also calculated in an automated manner based on the duration and the distance for which the electric car is used. The Controller values the Customers' privacy and does not use the Customers' Personal Data to profile them.

8. DATA SHARING
8.1. The Controller protects the privacy of the subjects' Personal Data and does not disclose Personal Data to third parties, except with the subject's consent and in cases permitted by law, the Privacy Policy, the Service Contract, and the Vehicle Use Agreement.
8.2. With guaranteed protection and control measures, disclosure is possible with other companies part of the Controller’s corporate group or with its service providers in order to

ensure the smooth functioning of the electric car sharing system and high quality of services (e.g. with server providers, telemetry services, data validation, technical and administrative customer support, EV Mobility Monitoring, car sharing platform, statistical data analysis, etc.). In this case, the service providers are required to strictly comply with their contractual obligations and applicable data protection legislation, including taking the necessary measures to protect the confidentiality of the subjects' Personal Data.

8.3. It is also possible for Customers' data to be shared with third parties if there is a justified need:

- public bodies such as traffic and local police, courts, prosecutors, Customers' Protection National Agency, etc. in order to fulfil the Controller's legal obligations, including to report possible law infringements, rimes, and misdemenours, to prevent fraud and traffic accidents or to fulfil other legal requirements e.g. for accounting reporting;
- insurers, law firms, bailiffs, debt collection companies - as **eCollect AG**, with address Neuhofstrasse 21, 6340 Baar, Zug, Switzerland, with registration number: CHE – 180.481.291, - etc., in order to enforce the Service Contract and the Vehicle Use Agreement and to guarantee the property of the Controller and its other rights and legal interests;
- to protect the security, rights, and interests of other Customers and/or third parties.

9. DATA TRANSFER OUTSIDE THE EU

9.1. Transfer of Personal Data to a third country or an international organization outside the European Union and the European Economic Area can only take place if one of the following conditions is met:

9.1.1. The company is based in the USA and is certified under the US-EU Privacy Shield (https://www.privacyshield.gov);

9.1.2. There is a decision of the European Commission regarding the adequate level of Personal Data protection that the third country in which the data is received provides;

9.1.3. There is an explicit consent of the data subject, after being informed of the possible risks associated with the transfer due to the absence of a decision on the adequate level of protection and of adequate guarantees;

9.1.4. The transmission is necessary for the performance of a contract between the Data Subjects and the Controller or for the performance of pre-contractual measures taken at the request of the Data Subjects;

9.1.5. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller or the group it is part of and another natural or legal person;

9.1.6. The transfer is necessary for the establishment, exercise or defence of legal claims;

9.1.7. The transmission is carried out by a public register.

9.2. In case of need for manual data verification during Customer's registration, data transfer is also done by the **JUMIO** validation service providers who have companies in the USA and India. The transfer is carried out on the basis of standard contractual clauses (Article 46, paragraph 2, letter "c") of the GDPR) with the necessary level of data protection, insofar as **JUMIO** is certified according to the PCI DSS standard and is subject to an annual audit for its compliance.

10. DATA STORAGE PERIODS

10.1. The Controller applies different Personal Data storage periods depending on the categories of Personal Data processed and the purposes of processing.
10.2. If the registration process has not been successfully completed and, so, the Customers have not being granted the right to use the electric car sharing services, their Personal Data are usually stored for a period of 3 years then after; however, they shall be deleted or anonymized immediately in case the Customers select the **"Forget me"** button through the Mobile Application, unless the Controller justifies a legitimate interest in continuing their processing (e.g., to defence against complaints, etc).
10.3. Upon completion of a successful registration with the right to use the services for the shared use of electric cars, the Controller applies the following Personal Data storage periods:

No	Personal Data Categories	Storage period
1.	Data related to fiscal duties, accounting and insurance claims	6 years from the date of issue of the document or occurrence of the insured event.
2.	Personal Identification Data from the Customer User Account, processed for the purposes of providing the electric car sharing services	3 years from the later of the following dates: the date of termination of the contract or the date of payment the last outstanding due debt. Data of Customers whose accounts are not active will be stored for 3 years from the date of the last login provided that no outstanding due debts still exist.
3.	Biometric Data	The Data processed for the purpose of uniquely and accurate identification of the Customers during the User's Accounts' registration procedures are deleted immediately from the database of the Controller, after establishing the identity/after the successful registration of the account. The biometric Data are then stored in specialized **JUMIO** servers for a period of 5 years, starting from the date on which the Customer's identity verification process was successfully completed. The Data processed for the purpose of preventing unlawful use of the Vehicles, frauds and/or traffic accidents, as well as for the protection and control of the Controller's property and the establishment and exercise of legal claims are stored for 1 year since the footage is taken, unless mandatory legal provisions prescribe otherwise or they are evidence or in any other way necessary in pending legal proceedings.
4.	Data used for direct marketing purposes	2 years from the later of the following dates: the date of termination of the contract or the date of

		payment of the obligation. Data of Customers whose accounts are not active will be stored for 3 years from the date of the last login.
5.	Mobility control data	2 years from the later of the following dates: the date of termination of the contract or the date of payment of the last outstanding due debt. Data of Customers whose accounts are not active will be stored for 2 years from the date of the last login, provided that no outstanding due debts still exist.

10.4. Exceptions to the above storage periods may be established insofar as the relevant deviations do not violate the rights of the Data Subjects, comply with legal requirements and are duly documented.
10.5. Documents and Data about Customers, in respect of which the Controller has initiated administrative or judicial proceedings, are stored and destroyed according to the instructions of the legal department for a period of 5 years after the conclusion of the proceedings with an effective court decision or final payment of the debt.
10.6. After the expiration of the established terms, the Data are anonymized or destroyed in a secure way by deleting them from the information systems or by shredding if they are on paper.

11. RIGHTS OF THE DATA SUBJECTS

11.1. The Data Subjects have the right to exercise the following rights according to the procedure established in the GDPR and the additional relevant laws:
11.1.1. **Right to information:** before processing the Data, the Controller is obliged to provide the Data Subjects with information in the form of a privacy notice about what Personal Data it collects, on what grounds and for what purposes it uses it, with whom it shares it, the Controller's intention to transfer the Data to third countries outside the EU, if any, the storage period and security measures, the consequences of not providing the Data, the presence of automated decision-making, the rights of the Data Subjects, including their right to lodge a complaint with a supervisory authority. Before registering as a user and installing the mobile application, the Data Subject is obliged to read and agree to the Privacy Policy in order to be able to use the Mobile Application;
11.1.2. **Right of access:** this right enables the Data Subjects to obtain copies of the Personal Data that the Controller stores about them, as well as information related to the processing. The history of the services used by the Data Subjects and the Data provided during registration can be accessed through the User Account in the mobile application, and a special access request can also be submitted;
11.1.3. **Right to erasure**: this right enables the Data Subjects to request their Personal Data to be deleted when there is no valid reason for the Controller to continue processing it e.g. if the purpose for which the Data were collected has been achieved or if the Data Subjects have withdrawn consent. If the legal requirements are met, the Controller should delete the

Personal Data within 1 month, unless other term prescribed by mandatory laws or there is a legal obligation to continue processing them or the retention of the Data is necessary for the establishment, exercise or defence of legal claims;

11.1.4. **Right to have Personal Data concerning them rectified:** this right enables the Data Subjects to request that any incomplete or inaccurate Data of them be corrected. The Data Subjects are obliged to promptly note any change in their Personal Data in their User Account and/or to notify the Controller thereof;

11.1.5. **Right to restriction of Data processing**: this right enables the Data Subjects to request the Controller to temporarily suspend the processing of Personal Data if, for example, they wish to establish the accuracy of the Data or the reasons for its processing

11.1.6. **Right to Data portability**: this right is limited to cases where the Data is processed in an automated manner and is provided by the Data Subjects on the basis of their consent or for the purposes of the performance of a contract, giving the possibility to require the Controller to provide the Personal Data stored in electronic form to the Data Subjects or a third party;

11.1.7. Right to object: in cases where the Controller relies on its legitimate interests as a basis for processing, the Data Subjects may object to this processing on grounds related to their particular situation. They also have the right to object when the processing is for direct marketing purposes or the Data is processed for statistical purposes;

11.1.8. Rights related to automated decision-making, including profiling: the Data Subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which gives rise to legal consequences for the Data Subjects or similarly significantly affects them;

11.1.9. Withdraw of consent: the Data Subjects have the right to withdraw their consent at any time in case they have given it without affecting the processing up to that point. Where consent has been given for direct marketing purposes, the Data Subjects may opt-out of receiving newsletters at any time by clicking on the "unsubscribe" link in email messages sent by the Controller or by changing the settings of their mobile application. If the Data Subjects have provided access to their location through the mobile device in order to find electric vehicles in the vicinity, they can change the settings thus selected;

11.1.10. Lodging a complaint: If the Data Subjects believe that any of their rights have been violated, they have the right to file complaints with the Controller and/or with the Authority for Personal Data Protection - www.dataprotection.ro.

11.2. Requests may be submitted by the Data Subjects or any person authorized by the Data Subjects, with the Controller taking measures to confirm their identity, for the purpose of data protection. The Controller is obliged to process such requests within the following terms, unless otherwise prescribed by the relevant laws:

Request from the data subject	**Period**
Right to information	When the data is collected (if the data is provided by the Data Subject) or within one month (if the data is not provided by the Data Subject)
Right of access	One month
Right to update	One month
Right to erasure	No undue delay
Right to restriction of data processing	No undue delay
Right to data portability	One month

Right to object	No undue delay

11.4. The Controller has the right to reasonably deny the Data Subject the exercise of his/her rights or impose a reasonable fee under the conditions provided for in Article 12, paragraph 5 of the GDPR.

12. DATA PROTECTION OFFICER

12.1. The rights and obligations of the Data Protection Officer are described in detail in the GDPR, the job descriptions, if the position is held by an employee of the Controller, or in the service contract, if the position of Data Protection Officer is held by an external service provider.

12.2. In general, the duties of the DPO include being responsible for the proper implementation of the Controller's Privacy Policy in accordance with the standards and requirements of the applicable legislation, participating in raising awareness and training of employees processing Personal Data, conducting the relevant audits, reports data processing risks, reacts to data security violations, assists the Authority for Personal Data Protection and Data Subjects in exercising their rights, keeps a register of processing activities, etc. tasks assigned by the Controller, insofar as they do not conflict with his duties as a DPO.

12.3. For DPO related matters you can use the following e-mail address: gdpr@espark.ro.

13. PROCEDURE FOR MANAGING PERSONAL DATA SECURITY BREACHES AND DEALING WITH SUCH BREACHES

13.1. If the Controller's employees having the right to access the Data notice or are notified of Data security violations (inaction or actions by persons that may lead to or have led to a risk to Data security), they are hold to notify immediately the Data Protection Officer and the immediate supervisor.

13.2. Taking into account the risk factors for breach of Data security, the degree of impact of the breach, damages and consequences, following the relevant internal procedures, the Controller makes decisions on the necessary measures to remedy the breach of data security and its consequences and to notify the Public Authority for the Data Protection and the affected individuals, if there is a high risk to their rights and freedoms.

14. TECHNICAL AND ORGANIZATIONAL MEASURES FOR PERSONAL DATA SECURITY

14.1. The organizational and technical data security measures implemented by the Controller ensure a level of security that corresponds to the nature of the data processed by the Data Controller and the risk of data processing, including, but not limited to, the measures specified in this section.

14.2. Personal Data security measures include the following:

14.2.1. Administrative measures as implementing appropriate procedures for the security of documents and computer data and their archives and organization of work in various spheres of activity, mandatory training of Personal Data protection personnel currently employed and upon leaving work/dismissal, duties on confidentiality and prohibition of disclosure of Personal Data, procedures for providing access to data, etc.;

14.2.2. Technical and software protection measures as administration of servers, information systems and databases, workplace support, protection of operating systems, monitoring (control) of user access, protection from computer viruses, etc.;
14.2.3. Administration of information systems and databases, job support, protection of operating systems, protection from computer viruses, etc.;
14.2.4. Protections for communication and computer networks (technical and software measures for coding and transmission of data for general use, applications, Personal Data, filtering of unwanted data packets, etc.).
14.3. The above-mentioned measures for the protection of Personal Data ensure: 1) storage equipment for copies of operating systems and databases, control of the storage of copying equipment; 2) technology for continuous work with data (processing); 3) strategy for restoring the functioning of 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 processes in operational mode; 6) registered data use and data privacy.
14.4. The Controller set up a procedure for the recovery of Personal Data in case of accidental loss of Data. The Controller makes backup copies of the data available in the system. Data is retrieved according to the internal procedure using **Amazon Web Services** software from the backup equipment libraries. In all cases, data archives are stored without prejudice to the data storage period specified in the Policy.
14.5. The Controller applies other measures guaranteeing the security of Personal Data:
14.5.1. VPN technology is used to remotely connect to the Controller's internal network, and a digital certificate is used to identify the user;
14.5.2. Access to Personal Data through organizational and technical data security measures that register and control efforts to register and acquire rights are subject to due control;
14.5.3. The following records are kept when entering the database by the persons who are granted the right to process Personal Data: login identifier, date, time, duration, result of the entry (successful, unsuccessful). The above records are kept for at least 1 (one) year;
14.5.4. The security of the premises where Personal Data are stored (access to the relevant premises only by authorized persons, locking, etc.) is ensured;
14.5.5. Efforts are made to ensure the use of security protocols and/or passwords when providing Personal Data via external data transmission networks;
14.5.6. The Controller does its best efforts to ensure control over the security of Personal Data on external data carriers and e-mail and their deletion after use of Personal Data by transferring them to databases;
14.5.7 Urgent Personal Data recovery actions (when and who performed Personal Data recovery actions by automatic and non-automatic means) are recorded;
14.5.8. The Controller does its best efforts to ensure that the testing of information systems is not carried out with real Personal Data, except in cases where organizational and technical measures for the protection of Personal Data are used, guaranteeing real security of Personal Data;
14.5.9. Personal Data in portable computers, if the latter are not used in the data transmission network of the Controller are protected by appropriate measures appropriate to the risk of processing.

14.6. The Controller implements appropriate technical and organizational measures ensuring standardized processing of Personal Data that is necessary for the specific purpose of data processing. The above obligation applies to the corresponding amount of Personal Data collected, the scope of their processing, the period of storage of Personal Data and the accessibility of Personal Data.

15. CONTACT DETAILS

15.1. The Controller can be contacted with questions related to this Policy and/or data protection in general using the following contact details:
Email: gdpr@espark.ro
Phone number: 0759888602

16. FINAL PROVISIONS

16.1. The policy is usually revised annually at the initiative of the Controller and anytime else needed including in case of changes in the legal acts regulating the processing of Personal Data.
16.2 The Policy and amendments to it come into force from the date of their publication on the Controller's Website.