MYBEE LATVIA PRIVACY POLICY

MyBee Latvia SIA (hereinafter – **we** or the **Company**) values and protects the privacy and security of personal data, therefore, in this MyBee Privacy Policy (hereinafter – the **Privacy Policy**) we explain how we handle the personal data of our clients (hereinafter – the Client) and other data subjects (hereinafter collectively referred to as – **you,** the **data subject**) when using: (a) the Mybee account (hereinafter – the **Account**); (b) you enter into a Subscription Agreement with us, (c) you use MyBee vehicles – cars (hereinafter – the **Vehicles**); (d) you provide us with your personal data in other informed ways.

We implement appropriate measures to ensure that the personal data provided to us – meaning any information that can be used to identify an individual – is always secure and that we process personal data in compliance with Regulation (EU) 2016/679) (hereinafter – the **GDPR**) applicable data protection legislation and our internal policies, guidelines, and procedures.

In this Privacy Policy, we provide the most important structured information regarding the protection of your personal data: i.e., what personal data we collect, how and why we use it, on what legal basis we process it, how long we retain it, to whom we disclose it, as well as information about our obligations in the processing of your personal data, your rights, and the methods for exercising those rights.

The most important information regarding the processing of your personal data is provided in the tables in **Section 15 of this Privacy Policy**. Please take the time to carefully review this Privacy Policy, and if you have any questions, please contact us.

If you use the Account, the MyBee Services, we will assume that you are familiar with this Privacy Policy and the purposes, methods, and procedures for the processing of your personal data specified in it. If you do not want your personal data to be processed as described in this Privacy Policy, please do not use the Account, our Services, and do not provide us with your personal data in any other way.

The Privacy Policy is a constantly changing document, so we can improve, modify, or update it if necessary. For this reason, please visit the website or Account from time to time, where you will always find the most recent version of the Privacy Policy. We will also additionally inform you about the most significant changes to the Privacy Policy and will always publish the updated version on our Website and your Account.

The latest changes to the Privacy Policy have been made and are valid from 4 th of May, 2026.

1. DEFINITIONS

The following terms are defined in this Privacy Policy:

We or the **Company** means MyBee Latvia SIA, a limited liability company, established and operating in accordance with the laws of the Republic of Latvia, legal entity registration number: 40203431136, registered office: Zemitāna iela 9 k-1, LV-1012, Riga, Republic of Latvia, that is the controller of your personal data.

Services or **MyBee Services** shall mean all services and service plans, that the Company offers and provides to you, including, but not limited to:

(i) rent (use) of the Vehicle; (ii) maintenance of the Vehicle and assets therein, insurance as specified in the Subscription Agreement; (iii) other services provided in the Account and/or on the Website.

Client shall mean the natural person who concluded the Subscription Agreement with us, or if a legal person concluded the Subscription Agreement with us, then the natural person representing them.

Website means the website available at https://mybee.lv/en/

Account – a digital account on the Website intended for access to and use of the Website services, information and content. The account is created in accordance with the procedure set out in the Website Terms of Use, which are published on the Website at https://mybee.lv/en/webservices-terms-of-use (hereinafter referred to as the Terms of Use).

Subscription Agreement shall mean the Vehicle Subscription Agreement, consisting of Special Terms and Conditions and General Terms (provided here: https://mybee.lv/en/motor-vehicle-subscription-agreement).

EEA means the European Economic Area, which consists of the European Union states and Liechtenstein, Iceland, and Norway.

Other terms shall have the meanings assigned to them and defined in the GDPR and/or the Subscription Agreement.

2. ON WHAT LEGAL BASIS DO WE PROCESS YOUR PERSONAL DATA?

We process your personal data specified in this Privacy Policy based on the following legal bases:

- for the conclusion, performance, amendment, and administration of the Subscription Agreement (Article 6(1)(b) of the GDPR);
- for the fulfilment of legal obligations and the requirements of applicable legislation binding upon us (Article 6(1)(c) of the GDPR);
- for the purposes of pursuing our legitimate interests and those of third parties (Article 6(1)(f) of the GDPR);
- on the basis of your consent (Article 6(1)(a) of the GDPR and Article 9(2)(a) of the GDPR).

To the extent and under the circumstances established by applicable legislation, one or more of the above legal bases may apply to the processing of your personal data.

The legal bases for the processing of your personal data are described in detail and presented in Chapter 15 of this Privacy Policy.

3. FOR WHAT PURPOSES AND WHAT PERSONAL DATA DO WE COLLECT?

We collect and process only your personal data that are sufficient and necessary to achieve the purposes for which they are processed. **The purposes for processing your personal data and the list of collected personal data are described in detail and presented in Chapter 15 of this Privacy Policy.**

We may combine personal data we have received from you (when you are using the Account, the Services, and/or the Website) with the personal data we have collected from other public or accessible sources (e.g., with data obtained using the website cookies, or with data legally obtained from third parties, etc.).

4. CAN YOU NOT PROVIDE YOUR PERSONAL DATA AND/OR NOT CONSENT TO THE PROCESSING OF YOUR PERSONAL DATA?

Your personal data is collected and processed to conclude or fulfill the Subscription Agreement with you and/or enable us to provide the Services and respond to your requests and complaints promptly and adequately. Suppose you do not provide your data, provide it with errors, or refuse to provide it further. In that case, we probably will not be able to conclude and/or execute the Subscription Agreement, provide the Services, and adequately respond to your requests, complaints, and/or other requirements that require our action. Accordingly, failure to provide personal data or refusal to continue to provide certain personal data will mean that the Subscription Agreement with you will not be concluded or will be terminated.

In cases where we process personal data based on your consent, you have the right to withdraw your consent at any time, and data processing based on your consent will be terminated.

Chapter 11 of the Privacy Policy outlines more information about your rights.

5. FROM WHAT SOURCES DO WE GET YOUR DATA?

We receive almost all your personal data from you; when you enter into a Subscription Agreement with us, use the Services, the Website, and receive your personal data in other informed ways.

Also, when it is allowed by legal acts, and when it is necessary for the execution of the Subscription Agreement and/or to achieve other purposes of processing your personal data, the Company collects or becomes known to the Company various information about you from the following multiple sources:

- from appointed institutions - data on the validity of the driver's license;
- from the police and municipalities - information about the violation of road traffic rules, other violations, and traffic incidents;
- from insurance companies and other official institutions or persons - information about traffic incidents, damage to the Company's Vehicles or third parties;
- from payment service providers – information about your payment transactions;
- from debt collection companies, claims management and/or credit rating companies - data of your financial obligations to us;
- from public registers – various legally available information;
- from other official institutions (e.g., various police units, Tax and Customs boards, etc.) - information on ongoing investigations;
- from service providers, partners (data processors), and other data controllers – various Service related information.

6. DO WE SHARE YOUR PERSONAL DATA WITH OTHERS?

Yes, the Company discloses all or part of your personal data to the following data recipients: various service providers with whom we have entered into service and data processing agreements, the companies belonging to the same group as the Company, competent authorities, and other data controllers who have a right to information in accordance with the applicable law, agreements and/or our legitimate interests. Also, with your consent, your personal data may be disclosed to persons and/or companies specified by you. More specifically:

The Company uses various service providers (for example, providers of server and cloud computing services, IT services, identity verification services, payment collection services, audit services, accounting services, legal services, tax advisory services, claims administration services, debt collection services, analytics services, direct marketing services, customer service providers, and other service providers). All service providers have concluded service and data processing agreements with us and are considered processors of your personal data, who may process your personal data only in accordance with our instructions and strictly in compliance with the purposes of processing. All data processors, like us, must ensure the security of your personal data in accordance with applicable laws and the agreements entered into with us.

In order to ensure the uninterrupted provision and quality of the Services, it may be necessary to transfer some of your personal data to other companies belonging to the same group of companies as the Company. Intra-group companies, like other service providers, are considered data processors and are subject to all terms and conditions applicable to data processors.

Where necessary and on legally justified grounds, we may also disclose your personal data to service providers who act as independent data controllers, as well as to various institutions, organizations, and other data controllers who are entitled to receive such information in accordance with applicable legislation, agreements and/or our legitimate interests. For example:

- In the event of an incident and/or a traffic accident, your data will be provided to insurance companies and, if necessary, to other parties involved in the incident.
- Upon receipt of fines for violations of traffic regulations, we have the right, and in certain cases also the obligation, based on the vehicle data available to us, to disclose to the relevant authorities (for example, the police) information about the person who committed the traffic violation.

- We have the right, and in certain cases also the obligation, to provide information about you to competent authorities (for example, law enforcement authorities, courts, or other dispute resolution bodies) for the purposes of investigating fraud, criminal offences, preventing crimes, and carrying out other investigations.
- Upon receipt of penalties for parking violations, we have the right, and in some cases also the obligation, to provide your data to parking facility owners or to designated collection companies that contact us on their behalf.
- If you fail to fulfil your financial obligations under the Subscription Agreement and do not settle the debt within the deadline specified in the debt notice, we have the right to transfer your personal data to debt collection companies, bailiffs, and courts in order to initiate debt recovery proceeding; debtor data file managers.
- If a guarantor is used when concluding or performing the Subscription Agreement, both the Subscription Agreement and debt-related documents may be provided to the guarantor for the purpose of direct debt recovery.
- Your personal data may also be transferred to other data controllers (such as insurance companies, vehicle maintenance service providers, or other additional service providers).
- Your personal data may also be transferred to other service providers acting as independent data controllers, whose offers, promotional campaigns, and game campaigns you have agreed to receive.
- Your personal data may also be provided to social media platform operators if you engage in active activities on our social media profiles (for example, Facebook or LinkedIn).

7. DO WE TRANSFER DATA OUTSIDE THE EEA?

The data processors and independent data controllers with whom we share your personal data are generally located in European Union Member States or store the data entrusted to us within the European Union. However, in some cases, carefully selected service providers (e.g., Google, Microsoft Azure, etc.) and controllers (e.g., operators of social media platforms such as LinkedIn, Facebook, etc.) process personal data outside the EEA.

In such cases, we carefully follow the practices and guidelines of supervisory authorities regarding the transfer of personal data outside the EEA and thoroughly assess the conditions under which the data is transferred and may be processed and stored after transfer outside the EEA. Furthermore, in order to ensure an adequate level of data security and guarantee lawful data transfers, where possible, we sign the European Commission’s approved Standard Contractual Clauses for transfers outside the EEA or otherwise ensure compliance with the provisions of the General Data Protection Regulation (GDPR) standards.

If you would like to receive more information about how we ensure the security of your personal data when transferring it outside the EEA, don't hesitate to contact us using the contact details provided in Chapter 14 of the Privacy Policy.

8. DO WE CARRY OUT AUTOMATED DECISION-MAKING AND/OR PROFILING?

The Company uses automated decision-making, including profiling, to perform the terms of the Agreement (e.g., granting benefits, etc.) and to provide tailored direct marketing services (e.g., sending newsletters only to interested customers). Accordingly, the Company may collect, analyze, and process personal data using specific algorithms and predictive models relating to your choices, behaviour, criteria for using the Services, amounts spent, and similar characteristics. None of these activities produce legal or similarly significant effects for you.

9. HOW LONG DO WE RETAIN YOUR PERSONAL DATA?

We process and retain your personal data no longer than required for the purpose(s) of processing or as required by law. Detailed information about the possible purposes of processing your personal data and the retention periods applicable to such purposes is provided in Chapter 15 of this Privacy Policy.

Upon expiry of the specified processing and retention period, we delete your personal data or reliably and irreversibly anonymize it as soon as reasonably possible within the time necessary to perform such actions.

Your personal data may be retained longer than stated in this Privacy Policy only if:

- your data is necessary for the proper administration of debt or damage (e.g., you failed to fulfil your financial and/or property obligations or caused damage to the Company or other persons) for the investigation of a dispute, complaint, to ensure Company‘s or third parties' legal interests;
- the Company requires the data in order to defend itself against existing or potential claims or legal proceedings, or to exercise its rights;
- there are reasonable suspicions of violations or unlawful activities that are or may be subject to investigation;
- the data is necessary to ensure the security, integrity, and resilience of information systems (e.g., upon detecting suspicious activity in the Account, Website, etc.);
- there are other grounds provided for by applicable laws.

10. HOW DO WE ENSURE THE SECURITY OF YOUR PERSONAL DATA?

We handle your personal data responsibly and securely, following internal data processing rules and implementing appropriate technical and organizational measures to protect data from unauthorized processing, accidental loss, destruction, damage, alteration, disclosure, or any other unlawful processing activities. Key principles we follow include:

- Collecting personal data only for specific and lawful purposes.
- Processing personal data fairly and only for the primary purpose.
- Retaining personal data no longer than necessary for the defined purpose or as required by law.
- Allowing access to personal data only to employees with authorized rights.
- Applying appropriate technical and organizational measures to process data securely.
- Disclosing personal data to third parties only when legally justified.
- Informing the Data State Inspectorate about registered or potential security breaches when relevant.
- Conducting regular data protection training for employees.
- Performing internal and/or external IT security audits periodically.
- Continuously updating and improving processes to ensure safe collection, receipt, transfer, and use of personal data.

We regularly monitor our systems for potential breaches or attacks, but complete internet security cannot be guaranteed. Users assume risks when submitting personal data using the Internet connection through the Account or Website. You also maintain the entire risk related to the voluntary disclosure of your Account data to others and/or the careless use of your personal data you receive directly from us.

11. WHAT ARE YOUR RIGHTS?

If we process your personal data for the purposes described in this Privacy Policy, or if you have reason to believe that we are processing your personal data, you, as a data subject, have the following rights under the GDPR:

11.1. The right to know – to know (be informed) about the processing of your personal data: In this Privacy Policy, we try to provide you with relevant information about processing your personal data as simply and in detail as possible. The most important information for you can be found in Chapter 15 of the Privacy Policy, which details the purposes of processing personal data, categories of data, legal grounds for the processing, storage terms, etc.

11.2. The right to access the processed data - obtain confirmation whether your personal data is being processed, and if so, request access to your personal data and a copy of it:

In order to exercise this right, contact us via e-mail dpo@mybee.group.

11.3. The right to correct personal data - request that inaccurate or incomplete personal data be corrected:
If the personal data you provided has changed (surname, e-mail address, telephone, driver's license, etc.), or you believe that the information we process about you is inaccurate, you have the right to demand to change, clarify, or correct information. You can make some changes to your personal data yourself in your Account (e.g., upload a new driver's license, change your address, etc.). In other cases, you must contact us via contacts stated in Chapter 14 of the Privacy Policy.

11.4. The right to object personal data processing:
Suppose you have reason to believe that our data processing violates your fundamental rights and freedoms and / or is being processed against GDPR or other legal requirements, in that case, you can exercise your right as a data subject and limit the data processed. However, we must point out that this may lead to us being unable to guarantee you all the Services, which may lead to the suspension or termination of your Subscription Agreement. To exercise this right, you must contact us via contacts stated in Chapter 14 of the Privacy Policy.

11.5. The right to withdraw your consent - when we process data with your consent:
In cases where we process personal data based on your consent, you have the right to withdraw your consent at any time, and data processing based on your consent will be terminated. For example, you can withdraw your consent to receive marketing offers and various information anytime through any channels we provide (e.g., newsletters, SMS messages, notifications, etc.).

Withdrawing your consent will not prevent you from continuing to use our Services, but it may mean that we are unable to provide you with valuable offers related to our Services. Please note that withdrawing consent does not affect the lawfulness of data processing prior to the withdrawal.

To exercise this right, you can conveniently do so in the following ways:

- you can unsubscribe from the newsletter at any time by clicking the e-mail the "Unsubscribe from newsletters" link in the letter;
- you can easily manage and change newsletters options, in your Account settings (by clicking on "My Profile" and then by clicking on "Subscription to offers");
- by changing the operating system settings of your device (in case of Cookies);
- By contacting us using the contact details provided in Chapter 14 of the Privacy Policy.

11.6. The right to restrict data processing - request that excessive or unlawful processing of personal data be restricted:
According to Article 18 of the GDPR, if at least one of the above circumstances exists, you have the right to restrict our ability to process your personal data. Once you restrict the processing of your personal data, we will no longer carry out any active processing operations with your personal data, except for the storage of such personal data. However, restricting the processing of personal data may mean that during the restriction period we will not be able to provide you with the Services, which may result in the suspension or termination of the Subscription Agreement.

You may restrict the processing of personal data in at least one of the following cases:

- your personal data is inaccurate (in this case, personal data processing operations will be restricted until the accuracy of the personal data has been verified)
- your personal data is being processed unlawfully, but you do not agree to the deletion of the data;

- the Company no longer requires your personal data for the specified purposes, but you require it in order to establish, exercise, or defend legal claims;
- your personal data is processed on the basis of legitimate interests, and you object to such processing of your personal data. In such a case, the processing of the data will be restricted until it is verified whether the grounds for which we process your personal data override your interests. To exercise this right, you must contact us using the contact details provided in Chapter 14 of this Privacy Policy.

11.7. Right to delete data (right to be forgotten) - request the deletion of unlawfully processed personal data, or personal data that are no longer necessary to achieve the purposes for which they were collected or otherwise processed:
You have the right to request that we no longer process your personal data (and delete it in some cases) in the event of at least one of the following circumstances:

- personal data are no longer necessary to achieve the purposes for which they were collected or otherwise processed;
- you revoke the consent on which the data processing was based, and there is no other legal basis for processing the data;
- your personal data is processed illegally;
- you have submitted an objection to the processing of personal data on the basis of our legitimate interest, and it is proven that your interests are superior in a particular case.

We will consider your request to delete your personal data (e.g., request to delete your Account) as a request also to terminate the Subscription Agreement, which will be terminated in accordance with the procedure provided in the Subscription Agreement terms. A request to delete only certain scope of your personal data may also result in the suspension or termination of the Subscription Agreement or the fact that we will not be able to provide you with all Services.

If you express a wish to delete all or part of your data, we will no longer actively process your data, which will no longer be necessary for the purposes for which they were collected or otherwise processed, but personal data will be stored according to the established terms, for the following reasons:

- For **accounting and tax purposes**, personal data will continue to be processed in accordance with **Article 6(1)(c) of the GDPR** – processing is necessary for the Company to comply with its legal obligations;
- **GPS (location) data** will continue to be processed in accordance with **Article 6(1)(f) of the GDPR** – processing is necessary for the legitimate interests of the Company or a third party;
- To **handle customer complaints and other disputes**, personal data will be processed in accordance with **Article 6(1)(b) of the GDPR** – processing is necessary for the performance of a contract to which the data subject is a party;
- To **implement a blacklist to prevent future use of the Services**, processing will be carried out in accordance with **Article 6(1)(f) of the GDPR** – processing is necessary for the legitimate interests of the Company or a third party;
- In the case of **dispute, claim, or debt administration**, personal data will be processed to ensure compliance with other legal obligations and to protect rights in accordance with **Article 11 of the Civil Code**, and in accordance with **Article 6(1)(f) of the GDPR** – processing is necessary for the legitimate interests of the Company or a third party.

To exercise these rights, you must contact us using the contact details provided in Chapter 14 of the Privacy Policy.

11.8. Right to data portability - receive your personal data in a structured, machine-readable format and transmit that data to another data controller:

When data processing is based on your consent or a Subscription agreement and is carried out by automated means, you have the right to receive the data you have provided and or created to us in a structured, commonly used, and computer-readable format. Also, if it is technically possible at your request, your data may be forwarded directly to another data controller specified by you.

11.9. Right to file a complaint - file a complaint with the State Data Protection Inspectorate: If you believe that we are processing your data in violation of the requirements of data protection law, you should first contact us directly. We are confident that, acting in good faith and with due diligence, we will be able to resolve any concerns, answer your questions, satisfy your requests, and correct any errors. If you are not satisfied with the solution we offer, or if you believe that we will not take the necessary actions in response to your request, you have the right to lodge a complaint with the **Data State Inspectorate** (Elijas iela 17, Riga, LV-1050, e-mail: pasts@dvi.gov.lv, telephone: +371 67223131).

12. HOW CAN YOU EXERCISE YOUR RIGHTS?

You can submit your requests to exercise your rights in the following ways:

- You can exercise your rights by **contacting us via e-mail** dpo@mybee.group and submitting a free-form request. Your request will be accepted and processed only if e-mail from which you contact us matches the e-mail that is linked with your Account.
- You can also exercise your rights by **coming to our Company** and filling out the application form, in which case we will ask you to show your identity document (we will not retain a copy of the document).

Additional verification measures: If doubts arise regarding your identity before performing any active steps, we may request that you provide additional documents or evidence, submit your request in writing only and/or sign it with a qualified electronic signature, etc. For example, this may apply in cases where you do not have an account or no longer have access to the e-mail address listed in your account's phone number.

13. HOW DO WE PROCESS YOUR REQUESTS TO EXERCISE YOUR RIGHTS?

To protect our clients' data from **unauthorized disclosure**, we will need to verify your identity when we receive a request to exercise your rights. To confirm personal identity, we primarily use the methods described in Chapter 12 of this Privacy Policy. After receiving your request to exercise your right(s) and when the identity mentioned above verification procedure was successful, we undertake to provide you with information about the actions we took/or did not take in response to your request as soon as possible, but in any case, no later than within 1 (one) month from the date of receipt of your request.

Please note that your rights are not absolute, and we reserve the right to refuse to comply with your request, providing a justified written response in accordance with the conditions and grounds provided by law.

Considering the complexity and number of requests, we have the right to extend the one (1) month period by **an additional two (2)** months, informing you of this extension before the end of the first month and stating the reasons for the delay.

If your request is submitted electronically, we will also provide the response electronically, unless this is not possible (for example, due to the large volume of information) or if you have requested a different method of response.

We will provide this information free of charge, but if requests are manifestly **unfounded** or **excessive**, in particular due to their repetitive nature, we may charge a reasonable fee to cover administrative costs or refuse to act on **the** request.

14. HOW CAN YOU CONTACT US?

The **data controller** processing your personal data as described in this Privacy Policy is **MyBee Latvia SIA** (a limited liability company established and operating under the laws of the Republic of Latvia, legal entity code: 40203431136, registered office address: Zemitāna iela 9 k-1, LV-1012, Riga, Republic of Latvia).

In accordance with the requirements of the **GDPR**, we have appointed a **Data Protection Officer (DPO)**, with whom you can contact regarding any questions related to this Privacy Policy, as well as

any other matters concerning data processing and data subject rights. The contact for the Data Protection Officer is: **e-mail: dpo@mybee.group**.

You may also contact us by **telephone** at our general customer service number: **+371 28233888**.

15. DETAILED INFORMATION ABOUT THE PROCESSING OF YOUR PERSONAL DATA

The following tables are divided into convenient separate categories according to the purposes of the processing and describe in detail the data processing processes, provide detailed information about how we collect, why we collect, for what purposes we use, and how long we store your personal data.

15.1. CREATING AN ACCOUNT

When are your personal data processed?	If you wish to start using our Services, you must register and create a personal Account in the Website, as the Subscription Agreements are concluded only through the Accounts. If the client is a legal entity, registration and an Account on the Website are created on behalf of the client by an authorized employee of the client, after receiving confirmation from the client that the Subscription Agreement can be concluded. To ensure the proper provision of the Services and the operation of the Account, we must collect and process your personal data determined by us (a necessary standard) to recognize you as a Client and to be able to provide services remotely via computer / smartphone devices.
Data categories	Name, surname, mobile phone number, email address, password. Account data (email and phone number) confirmation records, Account creation date, Terms of Use and Privacy Policy acceptance/ acquaintance records, direct marketing consent records, IP address, and other technical records (logs).
Legal grounds for data processing	**GDPR Article 6(1)(b) – Execution of a contract:** • Creation of an Account and Terms of service.
Duration of data processing	If Client hasn't confirmed an email and/or phone number attempted registrations are automatically deleted after **1 month** from the attempt date.
	If the Account was terminated/deleted without entering Subscription Services – during the effective term of the Account and for a maximum period of **3 months after its expiry**.
	In all other cases, during the effective term of the Web App Account and for a maximum period of **5 years after its expiry**.
	Chapter 9 of the Privacy Policy lists the cases and conditions when your Personal data may be stored or otherwise processed for longer.
Data recipients	UAB „Citybee Solutions" - infrastructure service provider

15.2. ACCOUNT ADMINISTRATION

When are your personal data processed?	When you use your Account, we record information about your actions in your Account and process various personal data about you. We do this to ensure the implementation of the Terms of Use and/or Subscription Agreement and the smooth operation, integrity and security of the Account and our information systems. Also, data is collected and processed to identify a possible threat or abuse of the Services, fraud, or other illegal activity, to protect the Web App, information systems, and data from unauthorized changes, cyberattacks, unauthorized access, and other related risks.
Data categories	Personal data about connecting to the Account, data about the device's operating system, Account usage history, settings, parameters, and changes, various usage, and technical records (logs). Direct marketing consents and/or withdrawals, important messages reading records. Account information, records of acceptance of new Terms of use, and/or confirmation of familiarization with the Privacy Policy.
Legal basis for data processing	**GDPR Article 6(1)(b) – Execution of a contract:** • Account and Service execution and administration.
Data retention period	Various system and technical records – **3 months from the date of their creation.**
	If the Account was deleted without using any Subscription Services – during the effective term of the Account and for a maximum period of **3 months after its expiry.**
	After you have used the Services – during the entire Subscription Agreement validity and for **5 years after it ends**.
Data recipients	UAB „Citybee Solutions“ - infrastructure service provider

15.3. CONFIRMATION OF PERSONAL IDENTITY

When are your personal data processed?	If you intend to sign a Subscription Agreement and rent a Vehicle, we must confirm your identity and whether you have the right to drive a Vehicle, as well as collect supporting evidence. Without this confirmation step, we cannot provide you with our Subscription Services. If the customer is a legal entity, it is responsible for ensuring that persons who are granted the temporary right to drive and use the Vehicle have a valid driver's license during the use of the Vehicle. In cases where you are from a third country (i.e., not a citizen of the EEA), the driver's license you submitted does not have a personal identification number, or the driver's license or photo provided is inconclusive, before allowing you to use the Services, we will contact you and ask you to send an additional copy of your identification document and/or contact you via video call, during which we will ask you to show an additional identification.

	If you do not agree or cannot submit your face photo (selfie) and / or driver's license data through the Account for identity and driving license verification, you can contact us, and depending on the circumstances, we can offer other acceptable alternative data submission options.
Data categories	Face image (selfie), face image with driver's license in hand (selfie), photo of the first side of the driver's license. Name, surname, personal identification number or another identification number, date of birth, driver's license number, expiration date, photo of the Customer's face from the driver's license, state, and authority that issued the driver's license. Data for verifying the authenticity and validity of the driver's license, data for checking the correspondence between the face image and the photo on the driver's license, the date of uploading the driver's license to the Account, video call.
Additional categories of data, if it is necessary to check your identity and/or the accuracy and completeness of the data provided by the video call or by collecting additional document	Date and time when the video call took place. Personal code or another identification number (collected during the conversation and recorded in your Account). In some cases a copy of a passport or ID document. Comment with the reason why you did not pass the identity verification or document verification process during the video call.
Legal basis for data processing	**GDPR Article 6(1)(b) – Execution of a contract:** • Execution and administration of the Subscription Agreement; • Ensuring that the identity of the Clients is appropriately verified and the use of the identity of other persons is prevented. **GDPR Article 6(1)(c) – Legal obligation applicable to the Company:** • Ensuring that only persons with the right to drive can use the Company's Services (Article 20 and 51 of Road Traffic Law of 12 Republic of Latvia). **GDPR Article 9(2)(a) – Consent:** • Processing the face image (selfies).
Data retention period	If the Account was terminated/deleted without using any Subscription Services – during the effective term of the Account and for a maximum period of **3 months after its expiry**.
	After you have used the Services – during the entire Subscription Agreement validity and for **5 years after it ends**.
	The video call is **not recorded and stored**.
	Chapter 9 of the Privacy Policy lists the cases and conditions when your Personal data may be stored or otherwise processed for longer.

Data recipients	UAB „Citybee Solutions“ - infrastructure service provider; Driver's license and identity verification service providers.

15.4. CONCLUDING AN AGREEMENT WITH PRIVATE NATURAL PERSON CLIENTS

When are your personal data processed?	To use the Services, it is not enough to create an Account – you also have to conclude the Subscription Agreement with us. The Subscription Agreement with natural person Clients is concluded and signed only electronically via the Account after choosing a Vehicle model and specific subscription conditions, also by performing all verification and confirmation steps requested in the Account.
Data categories	To conclude the Subscription Agreement, we will process the following Personal data: all Personal data stated in Tables 15.1. - 15.3. Also, all information provided in the Subscription Agreement (e.g., payment method, pre-payment amount, monthly payments, duration of the Services etc.). Payment information such as payment card four last numbers, etc.
Legal grounds for data processing	**GDPR Article 6(1)(b) – Execution of a contract:** • Execution and administration of the Subscription Agreement and Services.
Duration of data processing	During the effective term of the Subscription Agreement and for a maximum period of **10 years after its expiry**.
	Chapter 9 of the Privacy Policy lists cases and conditions when your Personal data can also be stored or otherwise processed for longer.
Data recipients	UAB „Citybee Solutions“ - infrastructure service provider; UAB „Modus Mobility“ – IT service provider.

15.5. MYBEE TRANSPORT VEHICLE USE ADMINISTRATION

When are your personal data processed?	When you use the Services, i.e., Vehicle subscription, we collect various information about the use of the Services and your actions to ensure fulfilment of the terms of the Subscription Agreement and the smooth provision, integrity, and security of the Service. Also, all data generated and collected during the Services, including Personal data about your use of our Services, help us to carry out the traceability and accuracy of the Services provided and is also used to protect our interests if there are noticeable illegal actions that are considered as part of the Subscription Agreement violation. Every Vehicle has an electronic GPS monitoring system installed to register and transmit to us the Vehicle's location, the distance travelled by the Vehicle, speed, and other data related to the Vehicle usage. Mobility data is essential to us because, with its help, we determine Vehicle location and have accurate travel traceability to ensure our own and/or third parties’ legitimate interests (especially relevant in the case of

	leaving the country, theft, damage, and in traffic rules violations or criminal activity traceability cases). Suppose you connect your device to the Vehicle's devices (e.g., navigation, multimedia systems) while using the Vehicle. In that case, your device's data, such as your given name, device-stored contacts, and Bluetooth ID, will be stored in the Vehicle unless you remove them following the Vehicle manufacturer's instructions.
Data categories	Vehicle first pick up date and time, Vehicle use date and time, Vehicle locking/unlocking time (if it is done via Web App), Service start and Service end date and time. Vehicle GPS data associated with a specific Client, detailed GPS coordinates, date and time of use of the Vehicle, route, speed, travel distance, duration, Vehicle picked up and left places. The Service's price, the payment amount for the Services, the fact of issuing the invoice, the fact and amount of the debt, and the maximum amount owed by the Client for the Services provided. Data of the completed payment transactions (date, amount, last four digits of the payment card, etc.), the amount of the replacement car credit, and its usage history. Discounts, coupons and/or codes, participation in programs, their validity, and use.
Legal basis for data processing	**GDPR Article 6(1)(b) – Execution of a contract:** • Execution and administration of the Subscription Agreement; • Identify violations of the Subscription Agreement. **GDPR Article 6(1)(c) – Legal obligation applicable to the Company:** • Obligation to report your Personal data in case of an administrative and/or criminal offense. **GDPR Article 6(1)(f) – Legitimate interest of the Company and third parties:** • To ensure the protection of Vehicles and other assets of the Company, as well as safety of third parties and their assets.
Data retention period	GPS data - **12 months from the date of its creation**.
	After you have used the Services – during the entire Subscription Agreement validity and for **5 years** after it ends.
	Chapter 9 of the Privacy Policy lists the cases and conditions when your Personal data may be stored or otherwise processed for longer.
Data recipients	UAB „Citybee Solutions“ - software service provider; Telemetry service providers.

15.6. ACCOUNT BLOCKING AND/OR TERMINATION OF SUBSCRIPTION AGREEMENT

When are your data processed?	The Services provided by us are subject to the established Terms of Use and the General Part of the Subscription Agreement, which you agreed

	to before starting to use the Account and our Vehicle and concluding a Subscription Agreement with us. Therefore, we have the right to collect information related to the use of the Services, to respond to received information related to violations of the Terms of Use and Subscription Agreement, and to take active actions when gross violations of our rules are detected. Accordingly, when we detect violations of the Subscription Agreement or Terms of Use, we may block or suspend the use of the Account, according to the terms set by us. However, in cases where the violations are extremely serious (e.g., drunk driving, causing a major accident, and other violations indicated in the Subscription Agreement), then we have the right to terminate the Subscription Agreement with you and, in addition, add you to the list of blocked persons, so that you cannot use the Services and conclude a Subscription Agreement with us in the future.
Data categories	All data about the Client, available from the Account and the use of the Services as stated in all tables above. Reason for blocking or termination of the Subscription Agreement, basis, comment of the employee who performed the blocking or termination of the Subscription Agreement, duration of the blocking. Blocking list (Client name, date of birth, blocking date, and blocking term).
Legal basis for data processing	**GDPR Article 6(1)(b) – Execution of a contract:** • Execution of the Subscription Agreement; • Monitoring how the Client uses the Services and fulfils/does not fulfil the terms of the Subscription Agreement. **GDPR Article 6(1)(f) – Legitimate interest of the Company and third parties:** • Prohibit blocked Clients and/or those with whom the Subscription Agreement was terminated from creating a new Account or concluding a new Subscription Agreement.
Data retention period	After you have used the Services – during the entire Subscription Agreement validity and for **5 years** after it ends.
	In case of serious violations, Clients (minimum data) are stored in the blocking list for **10 years** after the Subscription Agreement's termination date.
Data recipients	UAB „Citybee Solutions“– software service provider; UAB „Modus Mobility“ – IT service provider.

15.7. ADMINISTRATION OF INQUIRIES, REQUESTS, COMPLAINTS, AND OTHER COMMUNICATIONS WITH YOU

When are your personal data processed?	If you contact us by phone and/or in writing (e-mail, via Website, social networks, or otherwise), we will save the fact of your application and the information provided, including Personal data, so that we can properly examine your application and answer your question, request or complaint.

Data categories	***When contacted by phone:*** first name, last name, mobile phone number, email, residential address, travel details, Vehicle details, and other information required to complete the Client verification. Also, all information that is become known during the call. Date and time of the call, call duration and call record. **By contacting e-mail by mail / or through the Website:** name, surname, mobile phone number, e-mail address, residential address. Travel data and other information required to complete the Client verification. Additional information related to the written request and correspondence history. In providing client service, additional and sensitive information may be used or disclosed to us: driver's license information, information about the incident, traffic incident, information about the passengers, detailed description of the specific accident and/or problem, detailed circumstances of the complaint or other request, complaint and/or documents proving the accident.
Additional categories of data if we need to contact you for important reasons	Your name, surname, mobile phone number, e-mail address, GPS data, other data from the Account or use of Services, the reason for contact need. Date and time of the call, call duration, and call recording. The electronic message/SMS message sent to you, the fact and date of delivery of the message, etc.
Legal basis for data processing	**GDPR Article 6(1)(b) – Execution of a contract:** • Subscription Agreement administration. **GDPR Article 6(1)(a) – Consent:** • to answer, consult, provide, and administer the Services when any person initiates the first conversation.
Data retention period	Complaints, claims, and written requests related to the execution of the Subscription Agreement, Services and/or which may be related to disputes - during the entire validity of the Subscription Agreement and for **5 years** after it ends. Call recordings are stored for **6 months from the moment of creation**. Chapter 9 of the Privacy Policy lists the cases and conditions when your Personal data may be stored or otherwise processed for longer.
Data recipients	UAB „Modus Mobility“ – IT service provider; Call management rental and other telecommunications service providers.

15.8. ADMINISTRATION OF FINES FOR TRAFFIC RULES AND PARKING VIOLATIONS

When are your personal data processed?	Taking into account the terms of the Subscription Agreement, the applicable legislation, and our rights and legitimate interests, we have the right and, in certain cases, the obligation to disclose information about you and your traffic violations (e.g., speeding, driving, etc.) to the competent authorities (e.g., the police). Also, disclose your data to municipalities and parking lot owners so that fines received are rewritten

	in your name. We act in this way following the requirements of the law, protecting our interests, so that you, as a possible violator of the relevant activity, can defend your rights and dispute the validity of the fine if you believe that the violation was recorded incorrectly.
Data categories	All data about the Client, available from the Account and the use of the Services; The fact of a parking violation or other traffic violation, written documents about inquiries and requests for information, data disclosed by the Client and the date of disclosure.
Legal basis for data processing	**GDPR Article 6(1)(c) – The legal obligation applicable to the Company:** • The obligation to report your data in case of an administrative and/or criminal offense. **GDPR Article 6(1)(b) - Contract performance:** • Identify the identity of the Client who has committed a traffic and/or other offence and have evidence to prove it.
Data retention period	After you have used the Services - during the entire Subscription Agreement validity and for **5 years** after it ends.
	Chapter 9 of the Privacy Policy lists the cases and conditions when your personal data may be stored or otherwise processed for longer.
Data recipients	Police, municipalities of the Republic of Latvia, other competent institutions.

15.9. ADMINISTRATION OF TRAFFIC INCIDENTS AND DAMAGES

When are your personal data processed?	If the car was damaged, the damage occurred due to your fault or another person's fault, or you or another person had a traffic accident with one of our cars, we process your personal data for the purpose of traffic accident and damage administration.
Data categories	All data about the Client, accessible from the Account and use of the Services, facts of damage related to the Company/Vehicle/third parties, driver's license data, all evidence and documents related to the damage, insurance cases and other related information. Information about other persons who were in and/or drove the Vehicle. Information about the amount of damage, the fact of payment, payment plans, the debt incurred, etc. ! The data processed may include data related to health conditions, such as information about drunk driving or similar data.
Legal basis for data processing	**GDPR 6(1)(b) – Performance of the contract:** • Damage management and administration. **GDPR 6(1)(f) – Legitimate interests of the Company and third parties:** • Enforcement of legal claims and/or administration of damage claims. ! If we become aware of data relating to health, we process it on the legal basis of Article 9(1)(f) of the GDPR.

Data retention period	After you have used the Services – during the entire Subscription Agreement validity and for **5 years** after it ends.
	Chapter 9 of the Privacy Policy lists the cases and conditions when your Personal data may be stored or otherwise processed for longer.
Data recipients	UAB „Citybee Solutions“ - infrastructure service provider and claims management system provider (EEA); Paus Konsults SIA - external debt management administrator (EEA); Also external claims management experts, brokers, insurance companies, other external debt management administrators, attorneys/legal professionals, courts, bailiffs (EEA, in exceptional cases outside the EEA).

15.10. DEBT ADMINISTRATION

When are your personal data processed?	In cases where You violate the Subscription Agreement and do not pay for the Services provided or have other overdue payments, we, in order to recover the debt, carry out internal debt administration, such as sending reminders, etc. However, if the debt cannot be collected through internal processes within a reasonable time frame, we have the right to contact debt collection service providers and/or judicial authorities and transfer your personal data to them for debt collection and/or initiation of legal proceedings, as well as to transfer the data to the debtors' data file manager.
Data categories	All data about the Client, accessible from the Account and use of the Services; Information about the debt(s), the amount of the debt, reminders and calls for payment by e-mail, repayment history, payment plan and debt closure/write-off date; *If the service of a debt collection company is used:* Client's name, surname, personal code or other personal code, residential address, e-mail address, telephone number, date of transfer of the debt to the collection company, debt, active actions of the debt collection company, repayment history and debt closure/write-off date. Data about the debtor from public registers and information systems.
Legal basis for data processing	**GDPR 6 (1)(b) – Performance of the contract:** • Ensuring the collection of fees for services provided; • Ensuring timely compensation for damages and fines. **GDPR 6(1)(f) - Legitimate interests of the Company and third parties:** • Debt collection management when the Company fails to recover debts through internal procedures; • Applying legal remedies to ensure that the Company's rights under the Subscription Agreement are respected.

Data retention period	After you have used the Services – during the entire Subscription Agreement validity and for **5 years** after it ends. Accounting data is stored for **10 years** from the date of its creation. Chapter 9 of the Privacy Policy lists the cases and conditions when your Personal data may be stored or otherwise processed for longer.
Data recipients	UAB "Modus Mobility" – IT service provider; UAB "Citybee Solutions" – software provider; Paus Konsults SIA **-** external debt management administrator (EEA); Also external claims management experts, brokers, insurance companies, other external debt management administrators, attorneys/legal professionals, courts, bailiffs, debtor data file managers (EEA, in exceptional cases outside the EEA).

15.11. EXECUTION OF TAX, ACCOUNTING, AND OTHER OBLIGATIONS PROVIDED BY LAW

When are your personal data processed?	To ensure the proper implementation of tax, accounting, and other legal obligations (i.e., correct writing and declaration of accounting documents to state institutions, implementation of money laundering prevention requirements, etc.), we create various accounting documents with your personal data and administer them.
Data categories	Name, surname, residential address, personal identification number, VAT payer code (when the person is registered as a VAT payer); data about the Services (description of the Services; price/amount paid), issued accounting documents and their requisites, and other accounting and tax data that the Company must collect, process and store following laws and other legal acts.
Legal basis for data processing	**Article 6(1)(c) GDPR – Legal obligations and requirements of legal acts:** **based on Article 28(5) of the Accounting Law:** • Accounting, taxes, and other state obligations; • Prevention of money laundering (as necessary); • Consumer protection.
Data retention period	Most often, the retention and deletion period is calculated from the date of creation of the accounting document - **10 years** from the creation of the document (e.g. VAT invoice). All Customer data related to the Account is stored **for 5 years** after termination of the Service Agreement (e.g., Customer personal data). Chapter 9 of the Privacy Policy lists the cases and conditions when your Personal data may be stored or otherwise processed for longer.
Data recipients	UAB "Modus Mobility" - IT service provider; UAB "Citybee Solutions" - software provider; Accounting and bookkeeping service providers, auditors, State institutions (EEA).

15.12. DIRECT MARKETING

When are your personal data processed?	We process your personal data to provide you with general and/or personalized marketing offers (including offers from our partners) and other information about our Services that may be relevant to you. We may send you offers in several ways: by e-mail, SMS, etc. (e.g., in your Account). You can easily opt out of receiving marketing information when creating an Account in your Account Settings or you can opt out at any time in your Account Settings (under the Offer Subscription section) or by clicking the opt-out link in the newsletters you receive. In certain cases, we may also organize marketing with the help of social networks.
Data categories	Name, surname, e-mail address, telephone number, customer identifier (internal customer number), country, city, age, customer type (private/business customer), service usage information such as frequency, continuity, last use, amount of money spent on the Services, etc. Information and history of direct marketing consents/withdrawals.
Legal basis for data processing	**GDPR Article 6(1)(a) – Consent:** • Receive marketing offers. **GDPR Article 6(1)(f) - Legitimate interest of the Company and third parties based on Article 9(2) of the Information Society Services Law:** • To send you general and personalized offers and information via email.
Data retention period	Personal data is processed as long as consent is valid, i.e., until consent is withdrawn but not longer than 3 years after consent given day.
	The history of consents you have provided when you use the Company's Services is stored for the entire duration of the Service Agreement and for **5 years** after its expiration. If the Account was terminated/deleted without using any Services – during the effective term of the Account and for a maximum period of **3 months** after its expiry.
Data recipients	UAB „Citybee Solutions“ – software provider; Twilio Ireland Limited (Sendgrid) – email sending service provider. This Data Processor operates in the USA, Standard Contractual Clauses here: https://www.twilio.com/en-us/legal/data-protection-addendum; Other email sending service providers are also available.

15.13. OPTIMIZATION OF MARKETING INSTRUMENTS

When are your personal data processed?	We use automated data analysis and decision-making, including profiling, to provide you with personalized content and recommendations, marketing offers tailored specifically to you and/or to provide you with our other possible benefits, and to enable us to expand the range of Services offered and improve the Services we provide. We use automatic means to group and analyse your data processed for the respective purpose and

	make insights and predictions about what content and/or messages may be relevant to you. The described actions do not have any legal or similarly significant effect on you, but they will allow us to understand your needs and interests better, to create and offer you more diverse Services that better meet your needs, to provide a better-quality experience using our Services, etc.
Data categories	Technical information related to the device used, such as browser type, device type, and model, processor, system language, memory, OS version, IP address, User agent, IDFA (identifier for advertisers), Android ID " devices); Google Advertiser ID, and other similar unique identifiers. Engagement information, i.e., information related to ad campaigns and final customer actions, such as clicks on ads, impressions of ads viewed, audiences or segments assigned to an ad campaign, type of ads, and web page or application where such ads were displayed, web pages, visited by the end user, URLs from the referring website, app downloads and installs, and other interactions, events, and customer actions within the app (such as car selected, clicks, engagement time, etc.). Another history of your browsing in your Account and/or Website.
Legal basis for data processing	**GDPR 6 (1)(a) – Consent:** • Execution of Consent obtained through the cookie tool on the Website. **GDPR Article 6(1)(f) - Legitimate interest of the Company and third parties:** • To implement automated devices to optimize marketing processes; • To categorise and divide clients into groups, test the marketing tools used, and organize the automated use of marketing tools for the most effective customer engagement.
Data retention period	Until Consent is revoked or the specified cookie retention periods.
	After you have used the Services – during the entire Subscription Agreement validity and for **5 years after it ends**. If the Account was terminated/deleted without using any MyBee Services – during the effective term of the Account and for a maximum period of **3 months after its expiry**.
	Data that is anonymized and cannot be linked to any specific Client and/or only statistical data is stored indefinitely for as long as it is needed to achieve the respective intended purpose.
Data recipients	UAB "Citybee Solutions" - software provider

15.14. ADMINISTRATION OF SOCIAL NETWORKS

When are your personal data processed?	We administer our profiles and accounts on various social networks, such as Instagram, Facebook, Linkedin. If you are interested in our Services and follow our profiles on social networks, participate in our published games, promotions, you share your photo with us or tag us in your photo or post etc., we collect and use your data, which we receive directly from you when you perform active actions on our profile. It should be noted that our accounts are integrated into social network platforms (e.g., Facebook, Instagram, Linkedin, etc.), so all

	social platform providers have all the opportunities to collect your other personal data. You can find detailed information about the data processing carried out by each social network platform and the purposes and scope of data use in the privacy policy of the respective social network. If you want to exercise your rights related to the data processed in social networks, it would be more efficient for you to contact the manager of the relevant social network directly.
Data categories	Name, surname, gender, country, photo, information about communication in the account ("like", "follow", "comment", "share", etc.), messages sent, information about messages (time of receiving the message, content of the message, messages attachments, correspondence history, etc.), comments, reactions to published posts, shares, information about participation in events and/or games organized by us. A photo sent/tagged to us and its public sharing.
Legal basis for data processing	**GDPR Article 6(1)(a) – Consent:** • To process your data when you voluntarily perform active actions on our social network accounts.
Data retention period	The provider of the respective social network determines the data retention periods. We recommend checking the privacy policy of the respective social network. Accordingly, we review the posts on our social networks that are no longer relevant and, if necessary, delete them.
Data recipients	Social media providers such as Facebook, Instagram, LinkedIn, etc.

15.15. ADMINISTRATION OF BUSINESS CUSTOMER ACCOUNTS

When are your personal data processed?	If the Subscription Agreement is concluded by a business client (company, institution, organization) (hereinafter referred to as the Business Client), we accordingly process the personal data of the employees and representatives of such business client, which are specified in this Privacy Policy (purposes listed in the tables above). Employees and representatives of business customers have all data subject rights outlined in Chapter 11 of this Privacy Policy. The Business Client must inform its employees or representatives about processing their personal data, as specified in the contract between the Business Client and the Company. If Business Clients act as data controllers of their employees, or representatives (i.e., when information is available to them through the Account and they use it for their own purposes), we are not responsible for this, and the provisions of this Privacy Policy do not apply to such processing operations.
Data categories	Company name, address, company registration code, VAT code, payment card data (card type, last four digits of card number, expiration date), Subscription Agreement.

	Name, surname, position, e-mail address, telephone number, and other information of the person responsible for the execution of the service contract. Name, surname, position, e-mail address, and telephone number of the employee who has been granted the right to use the Company's business account. When employees use the Services through Business Client accounts, all other data is collected and/or generated through the use of the Services and processed as specified for all other data processing purposes.
Legal basis for data processing	**GDPR Article 6(1)(b) - Execution of the contract:** • Conclusion and execution of the Subscription Agreement. **GDPR Article 6(1)(f) - Legitimate interest of the Company and third parties:** • To process employees' Personal data.
Data retention period	If the Account was terminated/deleted without using any MyBee Services – during the effective term of the Account and for a maximum period of **3 months after its expiry**.
	After you have used the Services – during the entire Subscription Agreement validity and for **5 years after it ends**.
	Chapter 9 of the Privacy Policy lists the cases and conditions when your Personal data may be stored or otherwise processed for longer.
Data recipients	All possible Data Recipients are listed in all other purposes of this Policy. We transfer personal data collected during the rental process (in particular from invoices, rental agreements, as well as monthly reports, traffic violation reports and accident reports) to your Company or third parties who will pay the invoice.

15.16. STATISTICS, ANALYTICS, CUSTOMER BEHAVIOR RESEARCH

When are your personal data processed?	In order to ensure the quality of the Services, monitor and evaluate the operation of the Services, analyze their use, improve and develop the Services, increase their security, accessibility and user experience, as well as develop and offer new or improved Services, we perform analytical and statistical data processing operations. When performing analytics and statistics, we process both aggregated and anonymized data, and in certain cases data related to a specific client, when this is necessary to achieve the above-mentioned purposes. When processing client-related data, the identification of the client is not sought for additional purposes that are not compatible with the improvement, security or operation of the Services, nor are automated decisions made.
Data categories	Vehicle reservations, location and time of their locking/unlocking, Vehicle information, Vehicle GPS data, route, speed, travel distance, duration, fuel and fuel card usage, other travel parameters, travel history, telemetry data, all other data generated during the Services. Analysis of your Account information such as age, country, city, and frequency of use of Services, your Account information.

Legal basis for data processing	**GDPR Article 6(1)(f) - Legitimate interests of the Company and third parties:** • To follow performance, it's results and analyze them; • To implement and use data analysis and processing modules and methods to create and increase value for the Client and the Company.
Data retention period	Created sets of statistical documents are stored for **no longer than 36 months after data generation** (some analytics do not require a long data retention period, so they can be deleted earlier).
Data recipients	Data analytics software providers (EEA and non-EEA)

WEBSITE ADMINISTRATION, SERVICE, IMPROVEMENT

When are your personal data processed?	When you visit and browse our Website, to collect statistical data and improve the quality of the Service and the experience of visitors, we process the data of the cookies used on the Website and analyse them using the analytical service Google Analytics, which allows you to record and analyse statistical data on the use of the website. More information about Google Analytics and the information collected by its tools can be found here: *https://support.google.com/analytics/answer/9019185?hl=en&ref_topic=2919631#zippy=%2Cin-this-article*.
Data categories	IP address, MAC address, date of visit, duration, pages visited, devices and programs used for Internet browsing, etc.
Legal basis for data processing	**GDPR Article 6(1)(a) – Consent:** • To manage your data when you have agreed that we will track your actions on the Website with the help of cookies.
Data retention period	Within the terms specified in the cookie policy and/or cookie tool.
Data recipients	Recipients of data specified in cookie settings; Website developer.

15.17. ORGANIZATION OF COMPETITIONS, EVENTS AND ADVERTISING CAMPAIGNS

When are your personal data processed?	When you participate in our various contests, games, events and advertising campaigns, we collect and process your personal data in order to include you in the selected contest activities. Also, when conducting public events and/or advertising campaigns in which you participate, we also additionally create various filmed and photographed materials, which we use to increase awareness of our activities. If you were captured during a public event, we may use your image (to a limited extent) for representational purposes of that event. If you participated in a photo session and/or filming organized by us, then we will use your image for advertising purposes and we will enter into an appropriate agreement with you regarding the use of the image.
Data categories	Name, surname, e-mail address, tel. number, post comments, post shares, information about being discussed in the network account and "following" in the social network account, reactions to the post, photo, message, time of receipt, message content, messages to messages, reply to reply, submission of reply to reply. time, event participation

	information, rating information, photos or videos - if they are for the competition as part of the conditions of participation. When the image can be seen in a photograph, the image and/or sound recording in the video material, the event, the event data, image usage agreement.
Legal basis for data processing	**GDPR Article 6(1)(a) – Consent:** • Monitoring the implementation of the conditions of tender participants and in case of winning contact with the winner. **GDPR Article 6(1)(b) - Execution of the contract:** • Conclusion and execution of the lottery (contest) contract; • Photo shoots and other advertising campaigns and sharing the results. **GDPR Article 6(1)(f) – Legitimate interest of the Company and third parties:** • To capture and use images and/or videos from events organized by us for representational purposes.
Data retention period	Contest participants' data is stored for **1 year from the date of announcement of the contest winner.** In case of public events and advertising campaigns, the created results are made public – **5 years from the day of the event or the day of giving consent or within another period, specified in the consent.** The created results are stored for campaign archiving purposes – **10 years**.
Data recipients	Social media platform providers, competition partners or organizers (in the EEA and outside the EEA where competitions take place on social media).

15.18. ENSURING LEGAL REQUIREMENTS AND INTERESTS

When are your personal data processed?	We process your personal data in order to implement our legal requirements and defend our legitimate interests (including fraud prevention), protect our property and interests, our Customers' and other persons' property and interests, collect evidence of violations and prevent misuse of the Vehicles and our Services. Accordingly, we reserve the right to use the services of various legal service providers and/or involve institutions in order to make claims against you and/or defend ourselves against legal claims brought against us.
Data categories	All data about the Client accessible from the Account and use of the Services; Provided documents and attachments, procedural documents, claims, court decisions, rulings, information about crimes and convictions.
Legal basis for data processing	**GDPR 6(1)(f) – Legitimate interests of the Company and third parties:** • To ensure defence against Customers, authorities and legal claims; • To initiate the defence of legitimate interests before authorities or in court.

Data retention period	Judicial proceedings: 3 (three) years from the date of entry into force of the court or authority decision or the date of a fully legally binding decision.
Data recipients	UAB "Modus Mobility" - IT service provider; Lawyers, bailiffs, courts, consumer protection authority and other institutions.

END OF PRIVACY POLICY.