CITYBEE PRIVACY POLICY (EN)

CityBee Eesti OÜ (hereinafter referred to as "**we**" **or "the Company**") values and protects the privacy and security of your personal data, therefore this Privacy Policy (hereinafter referred to as "the **Privacy Policy**") explains how we process your (hereinafter referred to as **"you"** or **"the Client**") personal data when you use (a) the CityBee mobile application (hereinafter referred to as "the **Mobile Application** or **Mobile App**"), (b) CityBee vehicles (hereinafter referred to as "the **Vehicles**"), and (c) CityBee's website e https://www.citybee.ee (the "**Website**"), and (d) communicate with us by phone, email, social media and/or other means.

The Privacy Policy provides you with the most important structured information about how we protect your personal data in accordance with the EU General Data Protection Regulation (EU) 2016/679 (hereinafter referred to as "**GDPR**") and the requirements of other legislation, i.e. you can find out how, to what extent, and for which purposes we process your data, whether we transfer your data to partners and service providers, when we delete your data, what rights you have and other things that may be important to you. **The most important information about the processing of your personal data is set out in the tables in section 16 of this Privacy Policy**.

If you use the Mobile App and/or the Website, we will assume that you have read and understood this Privacy Policy and the purposes, methods, and procedures for processing your personal data as set out herein. If you do not want your personal data to be processed as described in this Privacy Policy, please do not use the Mobile App and/or the Website and do not provide us with your personal data in any other way.

The Privacy Policy is a constantly changing document, and we may improve, change and update it from time to time, so please visit the Website or the Mobile App from time to time, where you will always find the most up-to-date version of the Privacy Policy.

The latest changes to the Privacy Policy have been made and are effective from the 14th of January 2025.

1. TERMS

For the purposes of this Privacy Policy, the following terms are used:

- **We, or** the **Company,** means – CityBee Eesti OÜ, osaühing, mis on loodud ja tegutseb tegutseb Eesti Vabariigi õiguse alusel, registrikood 14646800, registrijärgse asukoha aadress: Harju maakond, Tallinn, Kesklinna linnaosa, Narva mnt 31, 10120, which is the controller of your data.
- **Services** means all services offered and provided by the Company, including (i) the provision of rental (use), maintenance services, third party liability insurance, and materials and fuels necessary for the normal use of the Vehicles and the property therein, (ii) other services provided through the Mobile App and the Website.
- **Website** means the website accessible at https://www.citybee.ee.
- **Self-Service** means self-service on the Website, accessible at https://selfservice.citybee.ee/.
- **Mobile App** means the CityBee software for smartphones, tablets and/or other mobile devices, which is used for booking, unlocking, locking, and/or other actions of the Vehicles.
- **Account** means an electronic account created by a natural or legal person for personal use on the Mobile App.
- **Premium vehicles** High-value luxury and/or exclusive cars (such as Porsche).
- **Service Agreement** means the contract between you and the Company for the provision of the Services on the basis of the Terms of Service.
- **Terms** means the Company's Terms of Service available on the Mobile App and the Website.
- **Electronic Vehicle Management System** means an electronic system installed in the Vehicle that (i) records the location, route, coordinates, virtual speed, battery voltage and other data of the Vehicle as specified in the Contract and transmits such data to the Company, and (ii) enables blocking of the unlocking and/or start of the Vehicle.
- **EEA** means the European Economic Area, consisting of the countries of the European Union plus Liechtenstein, Iceland and Norway.

Other terms shall have the meanings ascribed to them and defined in the GDPR and the Service Agreement.

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

We only collect and process your personal data that is sufficient and necessary to achieve the stated purposes. **The purposes for which we process your personal data and the list of personal data we collect are detailed in the tables in Section 16 of this Privacy Policy.**

We may combine the personal data we receive from you through your use of the Mobile App, the Services and/or the Website with personal data we collect from other public or accessible sources (e.g., we may combine the personal data you provide with data obtained through the use of the Website's cookies or with data lawfully obtained from third parties).

3. WHAT ARE THE LEGAL GROUNDS FOR PROCESSING PERSONAL DATA?

We process your personal data referred to in this Privacy Policy on the following legal grounds:

- when entering into, performing, modifying and administering the Service Agreement (Article 6(1)(b) GDPR);
- to comply with our legal obligations and regulatory requirements (Article 6(1)(c) GDPR);
- for the pursuit of our legitimate interest and the legitimate interest of third parties (Article 6(1)(f) GDPR);
- in accordance with your consent (Article 6(1)(a) GDPR, Article 9(2)(a) GDPR).

One or more of the above legal bases may apply to the processing of the same personal data. The detailed **purposes and legal bases for processing your personal data are set out in the tables in Section 16 of this Privacy Policy.**

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

Your personal data is collected and processed for the purpose of entering into or performing the Services Agreement with you and/or to enable us to provide the Services promptly and appropriately and to respond to your queries, requests and complaints as a Client. If you do not provide your data, or if you provide it in error or refuse to continue to provide it, we will not be able to enter into and/or perform the Services Agreement, provide the Services and respond properly to your enquiries, requests, complaints and/or other requirements that require us to act. Accordingly, failure or refusal to continue to provide certain personal data will mean that the Services Agreement will not be concluded or will be terminated.

For more information about your rights, please refer to section 13 of the Privacy Policy.

5. FROM WHAT SOURCES DO WE GET PERSONAL DATA?

Almost all of your personal data is obtained directly from you by entering into a Services Agreement with us, using the Mobile App, the Services, the Website and/or other informed collection of personal data.

In addition, where permitted by law and where necessary for the performance of the Service Agreement and/or other purposes of processing your personal data, we collect or become aware of various information about you from the following sources:

- from public registers - driving licence validity;
- from the police and local authorities - information on road traffic rules and other traffic offences and accidents;
- from insurance companies and other official bodies or persons - information about traffic accidents, 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 - details of your financial obligations and performance of your obligations to the Company;
- from public registers - a range of publicly available information;
- from other official bodies (e.g. various police departments, tax authorities, various public service authorities etc.) - information on ongoing investigations.

6. DO WE SHARE PERSONAL DATA WITH OTHERS?

Yes, the Company discloses all or part of your personal data to the following recipients: various service providers, companies belonging to the same group as the Company, competent authorities and other data controllers who have a right to information in accordance with applicable law and/or our legitimate interests. Personal data may also be disclosed, with your consent, to the persons and/or companies you have indicated. Read more:

6.1. The Company has engaged various service providers (e.g. server and cloud rental, IT support, identity verification, payment collection, auditing, accounting, legal, tax advisory services, debt collection, analytics, direct marketing, Client service and other service providers). All service providers have entered into service and data processing agreements with us and are considered to be processors of your personal data and may only process your personal data in accordance with our instructions and in strict compliance with the purposes of the processing. All processors, like us, are obliged to ensure the security of your personal data in accordance with the applicable laws and the contracts they have with us.

6.2. In order to obtain the necessary services and to ensure the smooth 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 as the Company. Inter-group companies, like other service providers, are considered data processors and are subject to all the conditions and procedures applicable to data processors.

6.3. Where necessary and legally justified, we also provide your personal data to service providers who are separate data controllers, as well as to various authorities, organisations and other data controllers who have a right to receive the information in accordance with applicable law and/or our legitimate interests. For example:

- In the event of an accident and/or breakdown, your data will be passed on to insurance companies and, if necessary, to other parties involved in the accident;
- In the event of fines for traffic offences, we have the right, and in some cases the obligation, to disclose the data of the offender to the relevant authorities (e.g. the police);
- Upon formal request, we are obliged to pass on information about you to the competent authorities (e.g. law enforcement authorities, courts, other dispute resolution authorities) for the purposes of fraud, crime and crime prevention and other investigations;
- in the event of fines for parking offences, we have the right, and in some cases the obligation, to pass your data on to the owners of the car parks or to the designated collection companies that contact us on their behalf;
- If you do not fulfil your financial obligations under the Service Agreement and do not pay your debt within the time limit specified in the notice, we have the right to transfer your personal data to debt collection companies, bailiffs, courts to initiate debt recovery proceedings;
- Your personal data may also be transferred to other service providers who are independent data controllers and whose offers, promotions, game campaigns you have accepted to receive;
- Your personal data may be shared with the company whose details you have provided via the Mobile App for the purpose of billing us for the Services;
- Your personal data may be transferred to the operators of social networking platforms if you are active on our social media profiles (e.g. Facebook, LinkedIn).
- In cases where you wish to be invoiced on behalf of a company of your choice and where you provide the details of the company concerned via the Mobile App, we will be entitled to transmit your personal data and further information about your trip(s) to that company upon request.

7. HOW LONG DO WE KEEP PERSONAL DATA?

We process and store your personal data for no longer than the purpose(s) of the processing or as required by law. **Details of the possible purposes for which your personal data may be processed and the retention periods for personal data processed for those purposes are set out in Section 16 of this Privacy Policy**.

After the expiry of the data processing and storage period, we will erase or reliably and irreversibly depersonalise your personal data as soon as possible and within a reasonable and prudent period of time for such action.

Processing and/or storage of your personal data for longer than specified in this Privacy Policy may be carried out only if:

- the personal data is necessary for the proper administration of a debt or damage (e.g. you have not fulfilled your financial and/or property obligations or you have caused damage to the Company or other persons);
- to resolve a dispute or complaint in order to safeguard our legitimate interests or those of third parties;
- necessary for the Company to defend itself against actual or threatened claims, demands or actions to enforce its rights;
- there are reasonable grounds for suspecting irregularities or illegal activities that are or may be the subject of an investigation;
- to ensure the prohibition of the use of the Services in the event of termination of the Services Agreement for gross misconduct;
- data is necessary to ensure the security, integrity and resilience of information systems (e.g. in the event of suspicious activity on the Account, Mobile App, Website, etc.);
- other grounds provided for by law.

8. HOW DO WE ENSURE THE SECURITY OF PERSONAL DATA?

We process your personal data in a responsible and secure manner, in accordance with our internal rules on the processing of personal data and appropriate technical and organisational measures to ensure protection against unauthorised processing, accidental loss, destruction, damage, alteration, disclosure or any other unlawful processing. Accordingly, we follow the following basic principles for processing data:

- we collect personal data only for specified and legitimate purposes;
- we process personal data fairly and only for the primary purpose;
- we do not keep personal data for longer than the stated purposes or as required by law;
- we only entrust the processing of personal data to employees who have the right and official access to do so;
- we process personal data only with appropriate technical and organisational measures;
- We only disclose personal data to third parties where there is a legal basis;
- if applicable, inform the State Data Protection Inspectorate of recorded or suspected personal data breaches;
- We provide periodic data protection training for our employees;
- periodic internal and/or external IT security audits;
- change, adapt and continuously improve various processes to ensure that the collection, receipt, transmission, use, etc. of personal data is as secure as possible.

We regularly monitor our systems for possible breaches or attacks, but it is not possible to ensure the complete security of information transmitted over the internet or to prevent breaches, especially those that may occur due to your negligence or disclosure of data to others. In this regard, we note that you also bear the personal risks associated with the submission of personal data through the Internet connection, the Mobile Application and the Website, as well as the full risks associated with the voluntary disclosure of your Account Data to others and/or the careless and negligent processing of your personal data that you obtain directly from us.

9. HOW DO WE HANDLE DATA FROM BUSINESS ACCOUNTS?

If a business client (company, institution, organisation) (hereinafter referred to as the "**Business Client**") enters into a Services Agreement with us for the provision of the Services, we shall process the details of such Business Client, the personal data of the responsible persons provided to us, and the personal data of the employees attached to the Business Client's Account, as appropriate (the personal data may be obtained either directly from the Business Client or from the individuals themselves).

Business Clients' data is processed in the same ways and for the same purposes as any other user of the Account who uses the Services, and therefore all the purposes, categories of data, and other provisions of the processing of personal data described in this Privacy Policy apply. In addition, the Business Client is subject to the *General and Special Terms and Conditions of the Vehicle Rental and Service Agreement*, which may also set out additional terms and conditions for the processing of personal data.

The Business Client must always inform its employees and responsible persons about the processing of their personal data as specified in the agreement between the Business Client and the Company and provide a link to this Privacy Policy.

In the event that Business Clients act as data controllers of the personal data of their employees, representatives (i.e. when they have access to the information via the Mobile Application and use it to achieve their own purposes), we are not responsible for such processing and the provisions of this Privacy Policy do not apply to such processing operations.

10. DO WE TRANSFER PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA?

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

In such cases, we carefully follow the supervisory authorities' practices and guidelines on the transfer of personal data outside the EEA and carefully assess the conditions under which the data are transferred and may continue to be processed and stored after the transfer outside the EEA. Also, in order to ensure an adequate level of data security and to guarantee the lawfulness of the transfer, we sign, where possible, standard contractual clauses approved by the European Commission (Article 46(2)(c) of the GDPR) for data transfers outside the EEA, or otherwise ensure that they are carried out in accordance with the GDPR.

If you would like more information about how we ensure the security of your personal data when it is transferred outside the EEA, please contact us using the contact details set out in section 15 of our Privacy Policy.

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

Yes, in the course of providing the Services under the Services Agreement, we carry out fully or partially automated decision-making and/or profiling, such as registration confirmations, automated calls and text messages, as well as profiling of Clients based on age or other criteria for the use of the Services, in order to implement the Company's Service restrictions and/or other decisions related to the Services. You always have the right not to have the applicable decision based solely on automated processing, including profiling, if you believe that the decision is unfair or erroneous.
You can always contact us at the contact details provided in section 15 of the Privacy Policy and our staff will reassess whether the automated/profiling decision is correct based on the data available in your Account.

Also, the Company uses automated decision-making, including profiling, to enforce the terms of the Services Agreement (e.g. awarding Benefits) and/or to provide tailored direct marketing services (e.g. sending newsletters to interested Clients only). Accordingly, the Company may collect, analyse and process personal data through the use of specific algorithms and predictive models about your preferences, behaviour, criteria for using the Services, amounts spent and similar attributes. These activities do not have any legal or similar material effect on your use of the Services and are intended to improve your experience of using the Services. Please note that you can always object to profiling for these purposes by contacting us at the contact details set out in section 15 of this Privacy Policy.

12. DO WE FILM VIDEO AND/OR VEHICLES?

The Company and/or the owners of the relevant premises, sites and other areas shall carry out video filming of Client service premises, sites, etc. where the Vehicles are located and/or may be present. The contact details of the relevant Data Controller carrying out the filming should always be indicated in notices posted at the filming locations.

As part of its measures to protect persons and property, the Company carries out video surveillance only in Premium Class Vehicles, additionally informing Clients about this by means of an information sticker inside the Vehicle. These Vehicles are equipped with cameras which without sound, record in real time only the exterior view, and in the event of a traffic and/or other accident or other dangerous situation, the equipment records a short video clip (up to 30 seconds). The processing of personal data for video surveillance and recording of short video clips is based on the legitimate interest to ensure the safety and security of the Clients, the Premium Vehicle, and public traffic. Information from short video recordings may

be provided to Data Recipients where it is necessary for the investigation of unlawful acts and/or for the protection of the legitimate interests of the Company.

13. WHAT ARE YOUR RIGHTS?

If we process your personal data for the purposes set out in this Privacy Policy, or if you have reason to believe that we are processing your personal data, then you have the following rights as a data subject under the GDPR. You can exercise your rights by contacting us at the contact details set out in section 15 of this Privacy Policy.

13.1. Right to know - to know (be informed) about the processing of personal data:

In this Privacy Policy, in accordance with Article 15(1) of the GDPR, we have tried to provide you with relevant information about the processing of your personal data in as simple and detailed a manner as possible. You will find the most important information for you in Section 16 of the Privacy Policy, which details the purposes of processing personal data, categories of data, the lawful grounds for processing, the recipients of the data and the retention periods. We will also notify you of any changes to the Privacy Policy by means of a separate notice in the Mobile App.

13.2. Right of access to processed data - to obtain confirmation of whether your personal data is being processed, to request access to your personal data and to obtain a copy of it:

If you are our Client and have an active Account, then you can generate an up-to-date copy of your personal data yourself an unlimited number of times and at any time via the Self-Service website https://selfservice.citybee.ee. All you need to do is enter the address of the Self-Service website using a web browser (please note that you cannot download a copy of your data via the Mobile App) and complete the following steps: https://selfservice.citybee.ee - log in to your Account - complete the requested authentication steps - once logged in, click on your email address (at the top of the right-hand side of the window) - click on the "Get your data" link.

If you no longer have an active Account or if you are experiencing problems using the Self Service website, please contact us at dpo@citybee.ee and we will send you an email with information on how you can obtain a copy of your personal data.

13.3. Right to rectification - to request that inaccurate or incomplete personal data be rectified:

If the data you have provided (name, email address, telephone number) has changed, if your driving licence details have changed or if you believe that the information we are processing about you is inaccurate or incorrect, you have the right to change, revise or correct this information.

You can make some changes to your personal data in your Account via the Mobile App (e.g. upload a new driving licence, change your address, etc.). In other cases, you must contact us using the contact details set out in section 15 of this Privacy Policy.

13.4. Right to object to processing - to object to the processing of your personal data:

You have the right to object to the processing of your personal data for the purpose(s) set out by us under certain conditions set out in Article 21 of the GDPR. If you object to such processing of your personal data, we will terminate the processing complained of or re-examine whether our interest in processing your personal data does not override your interests and fundamental rights and freedoms.

If personal data is processed for direct marketing purposes, including profiling, you have the right to object to such processing at any time. Objecting to direct marketing means that we will no longer use your personal data for any advertising purposes.

13.5. The right to withdraw your consent - when we process data with your consent:

Where we process personal data on the basis of your consent, you have the right to withdraw your consent at any time and the processing based on your consent will cease. Withdrawal of consent does not affect the lawfulness of the processing prior to the withdrawal of consent.

You can conveniently manage and revoke certain consents in the following ways:

- you can unsubscribe at any time by clicking on the *"Unsubscribe from* newsletters*"* link in the email*;*

- newsletters, active push notifications in the Mobile App can be easily managed and changed in your Account Settings in the Mobile App (by *clicking on "My Profile" and then clicking on "Offer Subscriptions"*);
- by changing the settings on your device's operating system (by cancelling access to your device's information or applications, or by changing the cookie settings on your computer browser);
- by changing your cookie preferences in the Cookies Management Tool on the Website;

13.6. The right to restrict processing - to request the restriction of excessive or unlawful processing of personal data:

According to Article 18 of the GDPR, you have the right to restrict our ability to process your personal data in any of the above circumstances. If you restrict the processing of your personal data, we will no longer carry out any activities with your personal data other than the storage of personal data. However, the restriction of personal data may mean that we may not be able to provide the Services during the period of the restriction, which may result in the suspension or termination of the Services Agreement.

13.7. Right to erasure (right to be forgotten) - to request the erasure of personal data processed unlawfully or which are no longer necessary for the achievement of the purposes:

Under Article 17 of the GDPR. You have the right to request that we stop processing your personal data and delete it on any of the following grounds:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
- you have withdrawn the consent on which the processing was based and there is no other legal basis for processing the data;
- personal data are processed unlawfully;
- you have objected to the processing of your personal data on the basis of our legitimate interest and it is demonstrated that your interests are overridden in the specific case.

We will treat your request to delete all of your personal data as a request to also terminate the Services Agreement, which will be terminated in accordance with the procedure set out in the Terms. A request to delete only certain of your personal data may result in the suspension of the Services Agreement or the inability to provide all of the Services. Please note that deleting (uninstalling) the Mobile App will not terminate the Services Agreement, which will remain in effect until terminated in accordance with the Terms or until you request that we delete your data.

If you wish to delete all or part of your personal data and/or terminate the Services Agreement with us, we will no longer actively process your personal data, but your personal data will be stored in our systems and deleted after the time limits we set or as required by law. Only in the rare cases listed in section 7 of the Privacy Policy, your personal data may be processed after a request for deletion and/or termination of the Service Agreement or stored for longer than the retention periods.

13.8. The right to data portability - to receive your personal data in a computer-readable format and to transmit that data to another controller:

Where the processing is based on your consent (Article 6(1)(a) of the GDPR) or on a Service Agreement (Article 6(1)(b) of the GDPR) and is carried out by automated means, you have the right to receive the data that you have provided to us in a structured, commonly used, computer-readable format and/or to have that data transmitted to another data controller of your choice.

13.9. The right to lodge a complaint with the State Data Protection Inspectorate:

If you believe that we are processing your personal data in breach of data protection legislation, please always contact us directly in the first instance. We trust that, through good faith efforts, we will be able to resolve any doubts, answer questions, comply with requests and correct any mistakes, if any, we have made.

If you are not satisfied with the solution we offer or if you do not think that we will take the necessary steps to comply with your request, you always have the right to lodge a complaint. Our supervisory authority - the Lithuanian Data Protection Inspectorate (L. Sapiegos g. 17, LT-10312 Vilnius, by e-mail ada@ada.lt)

14. HOW CAN YOU CLAIM YOUR RIGHTS?

You can apply to exercise your rights in the following ways:

- **By contacting us at:** dpo@citybee.ee and submitting a free form application. Your request will only be accepted and processed if the email address from which you are applying matches the email address in your Account. As part of your request, we may send a follow-up message to the last contact in your Account (by SMS and email) requesting an active identity authentication step and/or requesting additional documents or data.
- **By phone:** +372 600 0160 (please note that we may not be able to enforce all your rights over the phone). When you contact us by phone, we will first verify your identity by asking for your Account information or other information that only you should know. As part of this verification, we may send a follow-up message (by SMS or email) to the last available contact in your Account, asking them to take an active action. If the verification procedure fails, we will be forced to declare that you are not a data subject and we will have to reject the request;
- **When you come to our Company's office** and fill in the application form, we will ask you to show your personal document (we do not keep a copy of the document).

If we have any doubts about your identity, we may ask you to provide us with additional documents or evidence before we take action, or we may ask you to submit your request in writing and/or signed with a qualified electronic signature only, or to come to our Company's registered office. For example, where you do not have an Account, you are unable to verify your identity by telephone and/or you no longer have an email address or telephone number listed in your Account.

Upon receipt of your request to exercise your right(s) and following the successful completion of the above identity verification procedure, we undertake to provide you, no later than 1 (one) month from the date of receipt of your request, with information on the action we have taken/not taken in response to your request. We remind you that your rights are not absolute and that we have the right to refuse your request in a reasoned written reply, under the conditions and on the grounds provided for by law.

If your request is made electronically, we will also respond to you electronically unless this is not possible (e.g. due to the extremely large volume of information) or you request a different response. We will provide the information free of charge, but if the requests are manifestly unfounded or disproportionate, in particular because of repetitive content, we may charge you a reasonable fee to cover our administrative costs, or we may refuse to act on your request.

15. HOW CAN YOU CONTACT US?

The data controller who processes your personal data specified in this Privacy Policy is - CityBee Eesti OÜ, legal entity code 14646800, address: Harju maakond, Tallinn, Kesklinna linnaosa, Narva mnt 31, 10120.

Data Protection Officer - In order to comply with the GDPR, we have appointed a Data Protection Officer who can be contacted on all matters relating to this Privacy Policy and any other data processing we carry out. **The Data Protection Officer's contact details are**: dpo@citybee.ee.

You can also contact us by phone by calling our general Client Service number - +372 600 0160.
You can also find a lot of relevant information in the Frequently Asked Questions (FAQ) section of our website.

16. DETAILED INFORMATION ABOUT THE PROCESSING OF YOUR PERSONAL DATA:

The following tables, which are conveniently categorised according to the purposes of the processing, describe in detail the data processing processes and provide detailed information on why we collect your personal data, what we use it for, what data we process, to whom we disclose it and how long we keep it.

16.1. CREATING AN ACCOUNT ON THE MOBILE APP FOR THE PURPOSE OF

When do we process your personal data?	If you wish to start using the CityBee Services, you must be at least 19 years old, register and create a personal Account on the Mobile App, as the Services are only available remotely via the Mobile App and only to Clients with Accounts. In order to ensure the proper provision of the Services and the functioning of your Account, we are required to collect and process your personal data as set out (standard) by us in order to identify you as a Client, to link your Account to other data we process about you, etc. Once you have completed the Account creation process, you can immediately see the functionality of the Mobile App, all Vehicles and their terms of use. It is not necessary to add a payment card and the necessary documents during the Account creation process, but failure to do so will prevent you from using the Vehicles. ! We do not process biometric data to recognise your face or fingerprint to unlock the Mobile App faster (this is a functionality of your device). ! We have the right, at any time during the term of the Contract, to ask you to update the Personal Data you have provided or the login details you have created. This is to manage possible breaches, identity theft and/or to update your personal data.
Data categories	Name, surname, age, mobile phone number, email address, home address; Account confirmation records (email and phone number), Account creation date, Terms of Use and Privacy Policy consent records, direct marketing consent records, PIN, IP address and other technical records.
Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • Establishing a Service Agreement.
Data retention period	If you have not completed the registration process and/or have not confirmed your email and phone number, the personal data you have provided will be deleted **3 months after** the date of the start of the registration attempt.
	If you do not use the Company's Services, for **the entire duration of the Services Agreement and for 3 months after its expiry.**
	after you have used the Company's Services - for **the entire duration of the Services Agreement and for 5 years after its expiry.**
	If you create an Account and do not log in to the Account for more than 3 consecutive years. The Company has the right to terminate the Service Agreement and to initiate the processes of erasure of personal data.
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	Citybee Solutions UAB - Mobile App Infrastructure Provider (EEA); Providers of server and cloud rental services (EEA and non-EEA).

16.2. FOR THE PURPOSES OF SUBMITTING THE NECESSARY DOCUMENTS

When is your personal data processed?	If you intend to rent a vehicle, it is necessary for us to make sure that you have the right to drive the car and to collect evidence to prove it. Also, if you are not the holder of a Lithuanian, Latvian or Estonian driving licence, please provide a copy of your identity card or passport so that we can verify your identity without any doubt, to make it more difficult for us to deal with possible cases of identity theft, and to have all the necessary data to manage claims, debts and legal proceedings. ! You can submit the requested documents remotely via the Mobile App, or if you do not wish to or cannot submit the documents via the Mobile App, you can come to our nearest office with the requested documents. If you do not provide the requested data, we will not be able to provide you with our Services in any of the prescribed ways. ! If you are from a third country (i.e. a non-EEA national), or if the documents or photographs you have provided are suspicious to us, we may contact you by video call before we allow you to use the Services, during which we will ask you to show your document(s) on the screen, dictate the requested data and/or perform other steps necessary for a more detailed verification of your documents or identity. ! Please note that a driving licence or identity document may be rejected by the system if it does not comply with the standards set by the Company, e.g. a temporary document is provided, the name does not match the data available in the Account, etc. In this case, please contact the Company for a manual assessment of the suitability of the documents provided.
Data categories	A copy of your driving licence (name, surname, identity number or other identification number, date of birth, licence number, expiry date, photo of your face from the driving licence, country and issuing authority); Verification of the authenticity and validity of the driving licence, verification of the facial image and photo match on the driving licence, and the date of upload of the driving licence to the Account.
Data categories **if you have a driving licence from a country other than Lithuania, Latvia or Estonia**	A copy of your passport or ID card (name, surname, personal identification number or other identification number, date of birth, document number, expiry date, photo of your face from the document, nationality, signature, country and issuing authority).
Data categories **if you need to verify the authenticity of the data provided by video call**	The date and time of the video call; Personal identification number or other requested data (collected during the interview and recorded in your Account). A comment from a member of staff with a reason if you didn't go through the identification or document verification process during the video call.

Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • Execution and administration of the Service Agreement; • Collecting copies of the necessary documents and carrying out identity checks to ensure that Clients have a valid driving licence and that the Client's identity is properly verified; **GDPR 6(1)(c) - Legal obligation for the Company:** • to ensure that the Company's Services are only available to persons who have the right to drive *(Road Traffic Act, § 202)* **GDPR 9(2)(a) - Consent:** • process face photos from document(s).
Data retention period	If you do not use the Company's Services, for **the entire duration of the Services Agreement and for 3 months after its expiry.**
	after you have used the Company's Services - for **the entire duration of the Services Agreement and for 5 years after its expiry.**
	A video call is not recorded and stored.
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	Citybee Solutions UAB - Mobile App Infrastructure Provider (EEA); Ondato UAB - Provider of document verification and assembly services (EEA); Transport Administration - Provider of driving licence verification services (EEA); Providers of server and cloud rental services (EEA and non-EEA).

16.3. FOR THE PURPOSES OF PROCESSING BIOMETRIC DATA

When is your personal data processed?	If you intend to rent a vehicle, we need to make sure that you have a valid driving licence and that you are the owner. Verification of identity is mandatory to prevent fraud and to prove the identity of the Client beyond doubt, which is of great importance in the event of an accident, administrative and/or criminal investigations, claims management and legal proceedings. To verify your identity, we scan your facial data from a real-time photograph (selfie) and compare it with the facial photo on your driving licence and/or additional identity document. In addition, real-time facial biometrics are used for periodic identity authentication. In the event of suspicious activity on your Account (i.e. we believe that your Account has been misappropriated, Account sharing, Account selling, etc.) or in accordance with our periodic verification procedures, we will ask you to authenticate yourself from time to time by taking an additional facial photograph (selfie), which will be matched with the data already in your Account. If you do not wish to provide your biometric data via the Mobile App, you have the option of visiting the nearest CityBee office with the above documents.
Data categories	Image of a face (selfie), image of a face with driving licence in hand (selfie); Biometric facial data (face map) for facial authentication based on unique facial features.
Data categories	Additional facial photo (selfie), date and time of authentication, authentication result (matched/not matched) with Account data.

additional identity authentication	
Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • Execution and administration of the Service Agreement; • to ensure that the identity of the Company's Clients is properly verified and to prevent the use of the identity of others. **GDPR 9(2)(a) - Consent:** • processing facial photos (selfies) and biometric facial data.
Data retention period	If you do not use the Company's Services, for **the entire duration of the Services Agreement and for 3 months after its expiry.**
	after you have used the Company's Services - for **the entire duration of the Services Agreement and for 5 years after its expiry.**
	Face photos (selfies) taken during additional authentication are not stored.
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	Citybee Solutions UAB - Mobile App Infrastructure Provider (EEA); Ondato UAB - Identity Verification Service Provider (EEA); Providers of server and cloud rental services (EEA and non-EEA).

16.4. FOR THE PURPOSES OF USING THE MOBILE APP

When is your personal data processed?	When you use the Mobile App, we record information about your activities on the Mobile App and the Account and process a variety of your personal data to ensure the performance of the terms of the Services Agreement, the smooth operation, integrity and security of the Mobile App and the information systems. Various data, including sensitive activity records, are collected and processed to identify potential threats of misuse of the Services, fraud or other illegal activity, and to protect the Mobile App, Client Accounts, information systems and data from unauthorised changes, cyber-attacks, unauthorised access, and other related risks. !Also, each time before you unlock the Vehicle, we need access to the location of your device to check that you are in the vicinity, so we will ask you to turn on the GPS of the device you are using to carry out this check. After this check, you can disable or keep the GPS data from your device for your convenience when using the Mobile App, e.g. to see the most accurate distance of the Vehicles from your current location (permissions are managed via your device settings).
Data categories	Mobile App login details, device operating system details, Mobile App version, unique device number (created by the Company), Account usage history, settings, settings and changes, miscellaneous usage records, technical records; Direct marketing consents and/or cancellations, records of reading important notifications in the Mobile App, records of accepting new Terms of Use and/or acknowledgement of the Privacy Policy; GPS coordinates of the device Start location, End location, Mobile app opening location.
Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • Execution and administration of the Service Agreement;

	• Checking the Client's GPS location to ensure proper unlocking of the Vehicle, checking for unauthorised transfer of the Vehicle, theft or any other unlawful act. **GDPR 6(1)(a) - Consent:** • Processing of GPS data for the convenience of the Service to the Client, in order to provide the Client with accurate distances from his location to the Vehicles.
Data retention period	Miscellaneous system and technical records - **3 months** from the date of creation.
	GPS data - **12 months** from the date of creation.
	If you do not use the Company's Services, for **the entire duration of the Services Agreement and for 3 months after its expiry.**
	after you have used the Company's Services - for **the entire duration of the Services Agreement and for 5 years after its expiry.**
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	Citybee Solutions UAB - Mobile App Infrastructure Provider (EEA); Providers of server and cloud rental services (EEA and non-EEA).

16.5. FOR THE PURPOSES OF USING VEHICLES

When is your personal data processed?	When you use the Vehicles, we collect various information about your use of the Services, your actions, and the parameters of the Vehicle in order to provide the Services, to fulfil the terms of the Service Agreement, and to ensure the smooth operation, integrity and security of the Service. All data generated and collected in the course of the Services, including data about your use of our Services and the Vehicle, is necessary for us to provide the Vehicle Rental Services in the first place. This data also helps us to ensure the traceability and accuracy of our Services and is used to protect our interests in the event of unauthorised acts that are deemed to be a breach of the Terms. ! We have the right to authorise some or all of the Vehicles, subject to age or other criteria, which are set out in more detail in the Terms and Conditions: https://citybee.ee/en/terms-of-use/. ! If you connect your device to the Vehicle's devices (e.g. navigation, multimedia systems) while using the Vehicle, your device data (e.g. the name you have been given, contacts and Bluetooth IDs that may be stored in the device) will be stored in the Vehicle unless you delete them in accordance with the instructions of the Vehicle manufacturer.
Data categories	Client's age (date of birth), date and time of reservation of the Vehicle, date and time of use of the Vehicle, time of locking/unlocking of the Vehicle, start of the Service and end of the Service, route, speed, distance, duration of the journey, fuel consumption and the use of the fuel card. GPS coordinate data of the Vehicle and other technical parameters of the Vehicle; Payment card details (name, surname, card type, first 6 digits of the card, last 4 digits of the card, expiry date; The type of purchase of the Service (single trip, package, subscription), the price of the Service, the fact and amount of payment for the Services,

	the invoice, the fact and amount of the debt, and details of other payment transactions (date, amount, etc.); Discounts, vouchers and/or codes, participation in programmes (e.g. refuelling), their validity and use.
Additional data categories when using Premium cars	Age (date of birth), number of trips made; Video footage of a traffic and/or other incident (up to 30 seconds in length), which may include images of you and/or other persons. ! The fact that the Vehicle is a Premium Vehicle and is being filmed is indicated on the Mobile App and inside the Vehicle.
Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • Execution and administration of the Service Agreement; **GDPR 6(1)(f) - Legitimate interest of the Company and third parties:** • filming to ensure the protection of Premium Vehicles and other Company assets, as well as the safety of third parties and their property, and to help reduce the number of speeding accidents.
Data retention period	after you have used the Company's Services - for **the entire duration of the Services Agreement and for 5 years after its expiry.**
	Video footage captured by camera in a Premium Vehicle (only footage of traffic and/or other incidents) is kept for **30 days from the date of creation**. If the video footage is used for internal and/or external investigations, it shall be kept until the date of completion of the relevant investigation.
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	Citybee Solutions UAB - Mobile App Infrastructure Provider (EEA); SEB bankas AB is a payment collection service provider (EEA); Xirgo Global UAB is a GPS system service provider (EEA); Lematisc UAB - Provider of vehicle tracking equipment (EEA).

16.6. FOR THE PURPOSES OF CHECKING THE VALIDITY OF YOUR DRIVING LICENCE AND/OR RENEWING YOUR DRIVING LICENCE

When is your personal data processed?	When you use the Vehicles, we have the right to periodically check the validity of your driving licence to ensure that your driving privileges have not been restricted. The driving licence check shall be carried out immediately upon attachment of the driving licence and shall be automatically checked before you attempt to use the Service, but not more frequently than every 7 days since the last check. We will also contact you (by email, SMS, active notifications on the Mobile App) if we notice that your driving licence is about to expire and inform you of the expiry of your driving licence, which you will be obliged to renew if you wish to continue using the Services. ! We have the right, at any time during the term of the Contract, to ask you to update your driving licence details by uploading a new copy of your driving licence. This is to manage possible breaches, identity theft and/or to update your personal data.
Data categories	Date and time of validation of the driving licence, results of validation (valid, invalid, suspended); A copy of the new driving licence, the name (if changed), the name of the person, the driving licence number, the expiry date, a photo of the Client's face from the driving licence, the country and the issuing authority of the driving licence and the date of adding the new copy of the driving licence to the Account.

Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • Use of the Services is restricted to persons with a driving licence. **GDPR 6(1)(c) - Legal obligation for the Company:** • to ensure that the Company's Services are only available to persons who have the right to drive *(Road Traffic Act, § 202).*
Data retention period	after you have used the Company's Services - for **the entire duration of the Services Agreement and for 5 years after its expiry.**
	Old copies of driving licences are deleted within 3 months from the date of uploading the new driving licence.
Data recipients	Citybee Solutions UAB - Mobile App Infrastructure Provider (EEA); Ondato UAB - Provider of document verification and assembly services (EEA); Transport Administration - Provider of the Driving Licence Validity Service (EEA).

16.7. FOR THE PURPOSE OF TRACKING MOBILITY VIA GPS COORDINATES (LOCAL DATA PROCESSING)

When is your personal data processed?	Each Vehicle is equipped with an Electronic Vehicle Management System combined with GPS, which allows you to select and reserve the Vehicle from anywhere and conveniently use and leave it in the permitted zone using only the Mobile App. This electronic system also records and transmits to us the location of the Vehicle, the distance travelled by the Vehicle, the speed of the Vehicle and other data relating to the Vehicle. Mobility data is of paramount importance to us as it allows us to organise the distribution of Vehicles, to locate them and to have an accurate trace of journeys in order to safeguard our own and/or third parties' legitimate interests (especially relevant in the case of travel price disputes, theft, damage and road traffic offences). ! Also, in exceptional cases where the Vehicle's electronic system records data that may endanger you, the Vehicle and other road users (e.g. extreme speed, unusual manoeuvring, etc.), we have the right to contact you (e.g. by phone call, automated call or text message) to inform you of an ongoing violation of the terms and conditions of the Service Agreement, in order to minimise the risk of damage to you and other road users.
Data categories	GPS data of the vehicle linked to a specific Client, GPS coordinates, date and time of use of the vehicle, route, speed, travel distance, duration, detailed GPS coordinates.
Additional data categories for automatic speeding calls	GPS data of the vehicle linked to a specific Client, GPS coordinates, date and time of use of the vehicle, route, speed, travel distance, duration; Date and time of the automatic call and/or SMS.
Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • Execution of a Service Agreement; • Identify the identity of the Client who has committed a traffic and/or other offence and have evidence to prove it; • Identify breaches of the Service Agreement. **GDPR 6(1)(c) - Legal obligation for the Company:** • the obligation to notify the Client's data in case of an administrative offence – *Penal Code.*

	GDPR 6 (1)(f) - Legitimate interest of the Company and third parties: • to ensure the security of the Vehicles and other assets of the Company, as well as the security of third parties and their property; • ensure road safety when using our services and vehicles; • reduce the number of speeding accidents.
Data retention period	GPS data - **12 months** from the date of creation.
	Automatic calls are not recorded or saved;
	Automatic call and SMS fact records - for **the duration of the Service Agreement and for 5 years after its expiry.**
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	Xirgo Global UAB is a GPS system service provider (EEA); Lematisc UAB - Provider of vehicle tracking equipment (EEA); TCG Telecom is a provider of call and SMS services (EEA).

16.8. FOR THE PURPOSE OF DETECTING DANGEROUS DRIVING

When is your personal data processed?	When we give you a Vehicle which is of high value and high risk, we have the right to check whether there are any breaches of the Terms and/or other risks to the Vehicle or to other persons or property on the road. Accordingly, we analyse and verify the data received from the Electronic Vehicle Management System installed in each Vehicle and subsequently take the actions provided for in the Rules (e.g. call you in real time to inform you about dangerous manoeuvres, warnings, initiate temporary suspension of your Account, impose a fine, etc). These actions shall have no effect on you as a Client if the terms and conditions set out in the Terms are being followed correctly. ! If a high-risk journey is identified, a member of staff can monitor the entire journey in real time and, if necessary, decide to contact the traffic police to inform them of potentially dangerous driving. For these purposes, we also carry out automated data analysis and decision-making, including profiling, i.e. we use automated tools to group and analyse various programmed allert signals from the data records we collect, derive trip scores, etc., in order to monitor, detect and stop unwanted activities on the Vehicles. In all cases, if you believe that we have misjudged the data and made an inappropriate decision, e.g. temporarily blocking your Account, imposing a fine or initiating termination of the Services Agreement. You have the opportunity to object to the decision by contacting us and filing a claim, in which case we will manually re-evaluate the totality of the data we hold.
Data categories	All data about the journey and the Vehicle are obtained from the electronic system in place; All data about the Client accessible from the Account and use of the Services; Journey assessment score, speeding score, other risk indicators; The fact that a call, SMS or speeding message was sent; The fine imposed, the circumstance/reason for the blocking or termination of the Contract, the grounds, the comment of the employee who carried

	out the blocking or termination of the Contract, the duration of the blocking.
Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • Execution of a Service Agreement; • monitor the Client's use of the Services and compliance/non-compliance with the terms of the Services Agreement and/or apply measures to restrict the Services. **GDPR 6(1)(f) - Legitimate interest of the Company and third parties:** • to carry out ratings and real-time trip monitoring of Client trips.
Data retention period	after you have used the Company's Services - for **the entire duration of the Services Agreement and for 5 years after its expiry.**
Data recipients	Citybee Solutions UAB - Mobile App Infrastructure Provider (EEA); Xirgo Global UAB is a GPS system service provider (EEA); Lematisc UAB - Provider of vehicle tracking equipment (EEA); TCG Telecom is a provider of call and SMS services (EEA).

16.9. FOR THE PURPOSE OF BLOCKING THE ACCOUNT AND/OR TERMINATING THE SERVICE AGREEMENT

When is your personal data processed?	Our Services are subject to the express Terms, which you have agreed to before using the Mobile App and entering into a Services Agreement with us (https://citybee.lt/lt/naudojimosi-taisykles/). We are therefore entitled to protect ourselves against attempts to commit fraud, to cause any type of damage to our property and/or other persons, and to try to minimise our financial and/or other liabilities. Accordingly, we have the right to collect information relating to the use of the Services, to respond to information we receive relating to breaches of the Service Agreement, and to take proactive action when we discover a gross violation of the Service Agreement as provided for in the Terms. When we identify breaches of the Service Agreement, we will generally take preventive action, i.e. sending warnings, imposing fines, and suspending the Account, in accordance with the time limits we set. However, in cases where the violation is particularly egregious (e.g. DUI, persistent speeding, causing a serious accident), then we have the right to terminate the Services Agreement with you and accordingly blacklist you from using the Services in future. For these purposes, we also carry out automated data analysis and decision-making, including profiling. Temporary blocking may be carried out by automatically blocking you because of suspicious activities recorded in your Account (e.g. frequent device changes, frequent changes to payment card details, significant speeding, etc.). However, in most cases, blocking is initiated by the Company's employees after assessing the totality of the available data, in accordance with the Company's processes. Termination of the Service Agreement due to a breach of the Terms and Conditions shall be carried out solely at the discretion of the Company's employee and no automated decisions are made. In all cases, if you believe that the suspension of your Account or the termination of the Service Agreement is unjustified, you have the opportunity to object to the decision by contacting us and filing a claim, in which case we will reassess the totality of the data available.
Data categories	All data about the Client accessible from the Account and use of the Services; The circumstance/reason for the fine, blocking or termination of the Contract, the basis, the comment of the employee who carried out the blocking or termination of the Contract, the duration of the blocking; Blacklist (Client's name, date of birth, blocking date and blocking period).

Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • monitor the Client's use of the Services and compliance/non-compliance with the terms of the Services Agreement and/or apply measures to restrict the Services; • Termination of a Service Agreement. **GDPR 6(1)(f) - Legitimate interest of the Company and third parties:** • Prohibit blocked Clients and/or those with whom the Services Agreement has been terminated from creating a new Account (inclusion on the Block List); • preventing fraud.
Data retention period	after you have used the Company's Services - for **the entire duration of the Services Agreement and for 5 years after its expiry.**
	In cases of serious breaches, the Client (minimum data) is stored in a blacklist **for 10 years** after the date of termination of the Service Agreement.
Data recipients	Citybee Solutions UAB - Mobile App Infrastructure Provider (EEA); Xirgo Global UAB is a GPS system service provider (EEA); Lematisc UAB - Provider of vehicle tracking equipment (EEA); TCG Telecom is a provider of call and SMS services (EEA); Police (EEA).

16.10. FOR THE PURPOSES OF ADMINISTERING ENQUIRIES, REQUESTS AND COMPLAINTS

When is your personal data processed?	If you contact us by phone and/or in writing (by email, mobile app, social media or otherwise), we will keep a record of the fact of your contact and the information you have provided to us, including your personal data, in order to properly process your request and respond to your question, request or complaint.
Data categories	**When contacted by call:** name, surname, mobile phone number, email address, residential address, travel details and other information required to verify the Client's identity. Date and time of the call, duration of the call and a recording of the call. **Contact by email / or via the Mobile App:** name, surname, mobile phone number, email address, residential address. Travel details and other information required to verify the Client's identity. Other information related to the written request and correspondence history; Additional and sensitive information may be used or disclosed in the course of this Client Service: driver's licence information, accident information, traffic incident information, passenger information, a detailed description of the accident and/or problem in question, details of the circumstances of the complaint or other request, documentation to substantiate the complaint and/or the accident or other incident.
Legal basis for processing	**GDPR 6(1)(a) - Consent:** • respond, advise, provide and administer the Services when any person initiates the first conversation.
Data retention period	Complaints, claims and written requests relating to the performance of the Service Agreement and/or which may be related to disputes - **throughout the duration of the Service Agreement and for a period of 5 years after its expiry.**
	Recordings of conversations are kept for **6 months** from the moment of creation.

	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	Citybee Solutions UAB - Mobile App Infrastructure Provider (EEE); Intercom is a communication system service provider. This Data Processor operates in the USA, Standard Contractual Clauses here: https://www.intercom.com/legal/data-processing-agreement TCG Telecom is a provider of call and SMS services (EEA); Twilio Ireland Limited (Sendgrid) is an email service provider. This Data Processor operates in the USA, Standard Contractual Clauses here:https://www.twilio.com/en-us/legal/data-protection-addendum

16.11. FOR THE PURPOSE OF COMMUNICATING WITH YOU

When is your personal data processed?	We have the right to contact you at any time in order to exercise our rights and obligations under the Service Agreement (e.g. if you have left the Vehicle unlocked, taken the keys with you, are speeding, may have left personal items in the Vehicle, etc.), and to provide you with important notices and information by email, telephone or on the Mobile App regarding any changes to the Service Terms. This important communication with you is not considered marketing and cannot be refused.
Data categories	Name, surname, mobile phone number, email address, home address, date and time of call, duration of call and call recording. A copy of the electronic message/SMS sent, the fact and date of delivery of the message, the fact and date of opening/reading of the message, the fact and date of opening of the link contained in the message.
Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • Managing the Service Agreement and providing important notifications.
Data retention period	Complaints, claims and written requests relating to the performance of the Service Agreement and/or which may be related to disputes - **throughout the duration of the Service Agreement and for a period of 5 years after its expiry.**
	Recordings of conversations are kept for **6 months** from the moment of creation.
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	Citybee Solutions UAB - Mobile App Infrastructure Provider (EEE); Intercom is a communication system service provider. This Data Processor operates in the USA, Standard Contractual Clauses here: https://www.intercom.com/legal/data-processing-agreement TCG Telecom is a provider of call and SMS services (EEA); Twilio Ireland Limited (Sendgrid) is an email service provider. This Data Processor operates in the USA, Standard Contractual Clauses here:https://www.twilio.com/en-us/legal/data-protection-addendum

16.12. FOR THE PURPOSES OF ADMINISTERING TRAFFIC RULES AND PARKING FINES

When is your personal data processed?	Subject to the terms of the Service Agreement, applicable law and our rights and legitimate interests, we have the right and, where appropriate, the obligation to disclose information about you and your Road Traffic Offences (e.g. speeding, drink driving) to the police on the basis of the Vehicle Data we hold. In most cases, we will pass your details on to the police, municipalities and parking lot owners, upon written request, so that the fines received can be reissued in your name and/or so that you can directly investigate the validity of the offences. We do this to comply with the law, to protect our interests and to enable you, as a potential infringer of the activity concerned, to defend your rights and to challenge the validity of the fine if you believe the infringement has been recorded in error.
Data categories	All data about the Client accessible from the Account and use of the Services; The fact of a traffic offence, written documentation of enquiries and requests for information, the data disclosed by the Client (name, surname, personal identification number or date of birth, place of residence, date of issue of the document granting the right to drive, number and the authority which issued the document), the date of disclosure; The fact of the parking violation, written documentation of enquiries and requests for information, the data disclosed by the Client (name, surname, personal identification number or date of birth, place of residence, date of issue of the document granting the right to drive, number and the authority issuing the document), the date of disclosure.
Legal basis for processing	**GDPR 6(1)(f) - Legitimate interests of the Company and third parties:** • we have the right to pass on information about breaches of parking regulations and road traffic rules to the competent authorities **GDPR 6(1)(c) - Legal obligation for the Company:** • obligation to report your details in the event of an administrative offence – *Penal Code.*
Data retention period	after you have used the Company's Services - for **the entire duration of the Services Agreement and for 5 years after its expiry.**
Data recipients	Police departments, municipalities of the Republic of Estonia; legal entities of parking lots (with whom we have concluded a Personal Data Processing or other type of Agreement).

16.13. FOR DEBT MANAGEMENT PURPOSES

When is your personal data processed?	In cases where you are in breach of the Service Agreement and have not paid for the Services or have other overdue payments, we carry out internal debt management, such as sending reminders, limiting the Services, in order to recover the debt. However, if the debt cannot be recovered through internal processes within a reasonable period of time, we have the right to contact debt collection service providers and/or judicial authorities and to transfer your personal data to them for the purpose of debt recovery and/or initiation of legal proceedings.
Data categories	All data about the Client accessible from the Account and use of the Services; Details of the debt(s), the amount of the debt, reminders and reminders to pay by email, repayment history, payment plan and date of closure/write-

	off; In the case of a debt collection company, the Client's name, surname, personal identification number or other personal identification number, date of birth, residential address, email address, telephone number, the basis, date and amount of the debt is provided to the debt collection company. If the debt needs to be taken to court, additional information may be sent to the debt collection company - for example, identity documents, proof of the debt or other information required by the court.
Legal basis for processing	**GDPR 6(1)(f) - Legitimate interests of the Company and third parties:** • Ensuring the collection of fees for services provided; • debt management through external service providers;
Data retention period	after you have used the Company's Services - for the entire duration of the Services Agreement and for 5 years after its expiry.
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	Citybee Solutions UAB - Provider of the mobile app infrastructure and claims management system (EEE); An external debt management administrator (EEE); Other external debt management administrators, lawyers, courts, bailiffs (in the EEA, exceptionally outside the EEA).

16.14. FOR CLAIMS MANAGEMENT PURPOSES

When is your personal data processed?	In most cases of damage to the Vehicle, we are do not carry out the claim determination and recovery process, provided that all the conditions of the fee paid to BeeChill are met (for more information, please refer to the Terms and Conditions). However, in cases where the terms of the fee paid to BeeChill do not apply, we have the right, in accordance with our legitimate interests, to administer and manage any damage caused by you to the Vehicles and/or our other property in order to reimburse us for any financial loss/expenses incurred as a result of the accident, your wilful misconduct, gross negligence or other factors. Also to administer traffic and/or other accidents in which you are not the perpetrator but only a participant or witness. The claims management process includes collecting information from recorded accidents, providing technical assistance, managing insurance processes, claims settlement processes and managing other claims from victims. In all cases, you will be informed of the claims/expenses identified and the amount of the claims/expenses incurred and you will be given the right to contest the decision and/or to clarify the circumstances etc. If the damages awarded are not paid within a reasonable period of time set by us, then debt management proceedings are initiated.
Data categories	All data about the Client accessible from the Account and use of the Services; The fact that BeeChill has paid the fee, information about breached BeeChill fee conditions; Information on the damage(s)/costs incurred, amounts of damage/costs, written claims, estimates, compensation certificates/invoices, fact of payment, payment plans, debt incurred, debt administration details, etc.; The facts of the damage relating to the Company/vehicle/third parties, driving licence details, all evidence, documents, testimonies relating to the

	damage. Insurance claims processing and all related information; Details of roadside assistance, costs incurred, invoices; Information about other people who were in and/or driving the vehicle; ! In some circumstances, we may also receive health-related data in this context, such as injuries or signs of alcohol or drug use.
Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • damage management and administration; **GDPR 6(1)(f) - Legitimate interests of the Company and third parties:** • enforcing legal claims and/or administering damage recovery **GDPR 9(2)(f) - processing is necessary for the establishment, exercise or defence of legal claims or for the exercise of judicial power by courts:** • Processing of health data received/obtained for the purpose of enforcing legal claims and/or administering damages.
Data retention period	after you have used the Company's Services - for **the entire duration of the Services Agreement and for 5 years after its expiry.**
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	Citybee Solutions UAB - Provider of the mobile app infrastructure and claims management system (EEE); An external debt management administrator (EEE); Also, external claims management experts, brokers, insurance companies, other external debt management administrators, solicitors/lawyers, courts, bailiffs (in the EEA, in exceptional cases outside the EEA).

16.15. FOR THE PURPOSES OF LEGAL REQUIREMENTS AND TO SAFEGUARD OUR INTERESTS

When is your personal data processed?	We process your personal data in order to enforce our legal claims and defend our legitimate interests (including fraud prevention), to protect the property and interests of ourselves, our Clients and others, to collect evidence of infringement and to prevent misuse of the Mobile App, the Website, the Vehicles and our Services. Accordingly, we reserve the right to use various legal service providers and/or involve the authorities in order to pursue claims against you and/or to defend ourselves against legal claims against us. ! In all cases where we suspect document fraud, identity theft, account theft and other illegal activities with our Vehicles, we contact the pre-trial investigation agencies (police, prosecutor's office).
Data categories	All data about the Client accessible from the Account and use of the Services; Documents and annexes submitted, pleadings, claims, court decisions, rulings, information on crimes and convictions.
Legal basis for	**GDPR 6(1)(f) - Legitimate interests of the Company and third parties:**

processing	• Defend against legal claims; • Initiate the defence of legitimate interests.
Data retention period	3 (three) years from the date of entry into force of the court or authority's decision, or the date on which the legally binding decision is fully implemented.
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	Lawyers/lawyers, bailiffs, courts, consumer protection authorities and other institutions (EEA, exceptionally outside the EEA).

16.16. FOR TAX, ACCOUNTING AND OTHER STATUTORY OBLIGATIONS

When is your personal data processed?	In order to ensure the proper implementation of tax, accounting and other legal obligations (i.e. the correct issuance and declaration of accounting documents to public authorities, the implementation of anti-money laundering requirements, etc.), we create and administer the relevant accounting documents with your personal data.
Data categories	Name, surname, residential address, email address, personal identification number (in rare cases), VAT identification number (where the person is VAT registered); Data about the Service (description of the Service, price/amount paid), accounting documents issued and their details, and other accounting and tax data that the Company is obliged to collect, process and store in accordance with laws and regulations.
Legal basis for processing	**GDPR 6(1)(c) - Legal duties and legal requirements:** • Accounting, tax and other public obligations; • prevention of money laundering (to the extent applicable); • protecting consumer rights. ***Additionally based on:*** • *Financial Accounting Law Taxation Act, § 58:* • *Accounting Act, § 12*
Data retention period	The retention and deletion period is usually calculated from the date of creation of the accounting document - **10 years after the creation of the document** (e.g. a VAT invoice).
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	External providers of accounting and bookkeeping services, auditors, Public Authorities (tax authorities) (EEA); Accounting system service providers (EEA and non-EEA).

16.17. FOR DIRECT MARKETING/MARKETING PURPOSES

When is your personal data processed?	We process your email and/or other contact details after we have been informed of your email and/or other contact details in order to provide you with general and/or personalised newsletters (including offers from our partners) surveys and other information about our Services that may be relevant to you. We may send you notifications, offers and information in a number of ways: by email, SMS, Mobile App messages (inactive and/or

	active), call. In order to provide you with personalised content, tailored marketing offers and/or other Benefits (i.e. discounts, coupons, etc.) and to enable us to expand the range of Services we offer and to improve the Services we provide, we carry out automated data analysis and decision making, including profiling, i.e. we use automated tools to aggregate and analyse data relating to your use of the Services and to make insights and predictions about what content, messages, Benefits may be relevant to you. We emphasize that when creating such personalized advertising campaigns, we only take into account your Service usage data (data is not collected through any other marketing optimization tools). Also, these personalised advertisements sent through our marketing channels will only reach you if we have your valid consent to provide marketing communications. Please note that you can always object to profiling for these purposes by contacting us at the contact details set out in section 15 of this Privacy Policy. ! You can easily object to the sending of offers and information notifications when you create your Account in the settings of the Mobile App, or you can easily unsubscribe from them at any time at a later date in the settings of the Mobile App (in the Offers subscription section) or in the newsletters sent to you by clicking on the unsubscribe link.
Data categories	Name, surname, email address and/or phone number, country, city, age, gender; Type of Client (private/business Client); Information about the use of the Service, such as frequency, continuity, last use, amount of money spent on the Services, etc. Information and history of direct marketing opt-ins/opt-outs.
Legal basis for processing	**GDPR 6(1)(a) - Consent:** • to receive our offers in the way(s) you choose; **GDPR 6 (1)(f) - Legitimate interest of the Company and third parties:** • Providing personalised newsletters and Benefits; • Legitimate interest in informing you about our goods and/or services; • send active messages in the Mobile app.
Duration of data processing and storage	**3 years** from the date of consent or provision of information, unless you opt out of receiving information about our Services earlier.
	The history of consents without your use of the Company's Services shall be retained **for the duration of the Services Agreement and for 3 months after its expiry.**
	The history of consents after you have used the Company's Services shall be kept for **the entire duration of the Services Agreement and for 5 years after its expiry.**
Data recipients	Clever tap is a Client lifecycle management and marketing service provider. This Data Processor operates in the USA, Standard Contractual Clauses here: https://clevertap.com/eu-us-data-privacy-framework-policy/ Twilio Ireland Limited (Sendgrid) is an email service provider. This Data Processor operates in the USA, Standard Contractual Clauses here:https://www.twilio.com/en-us/legal/data-protection-addendum

16.18. FOR THE PURPOSES OF MONITORING AND OPTIMISING MARKETING TOOLS

When is your personal data processed?	When you visit our Website or use our Mobile App, we have the ability to use various tracking tools (e.g. cookies) or other technologies to collect and store information about you, your device, settings, usage behaviour, etc. We use this information to improve and personalise your experience on the Website or Mobile App, and to provide you with relevant content and advertising on both our and third party websites. Certain tracking tools are mandatory and cannot be opted out of, otherwise certain functions would not function properly or we would not be able to identify potential system failures (e.g. essential cookies, essential tracking technologies), and all tracking tools designed to optimize marketing and increase dissemination are carried out with your consent. ! You can easily manage your consent through the Site's Cookie Settings - click on the chain icon at the bottom of the Site (on the left-hand side) and change your settings. You can manage the tracking tools in the mobile app via the menu bar, click on my profile and select Privacy settings and update your consents.
Data categories	Technical information related to the device you are using, such as browser type, device type and model, processor, system language, memory, OS version, IP address (usually depersonalised), User agent, IDFA (advertiser identifier), Android ID (on Android devices); Google advertiser ID, other similar unique identifiers. Engagement information, i.e. information related to ad campaigns and final Client actions, such as, Click-throughs on ads, ad impressions, audiences or segments targeted by the ad campaign, type of ads and the website or app where such ads were displayed, webpages visited by the end-user, URLs from the referring website, app downloads and installs, and other in-app interactions, events, and Client actions (e.g., car selected, trips booked, clicks, engagement times, etc.). The following personalised data is passed on to third parties for advertising purposes: the Client's Mobile Application ID generated by Google, the country in which the Mobile Application ID is opened, the date on which the Mobile Application was first launched, the date on which the registration was made, the date on which the first trip was made, information on whether or not a payment card was added, information on whether or not a driving licence was added, information on the payments made under the Mobile Application ID (amount, currency, the type of service paid for (type of service, extensions and suspensions of members), etc.).
Legal basis for processing	**GDPR 6(1)(a) - Consent:** • Enforcement of consent obtained through privacy settings on the mobile app at the time of first registration or later. • Exercising consent obtained through the cookie tool on the website. **GDPR 6(1)(f) - Legitimate interest of the Company and third parties:** • installing technological devices to optimise the functioning of the Website and the Mobile App;
Data retention period	The retention periods for cookies are specified in the Cookie Policy. Consent is valid until revoked.
	Consents given on the mobile app are valid for 3 years or until revoked.
	Analytical data that is anonymised and cannot be linked to any specific Client and/or statistical data only is stored indefinitely until it is needed to achieve the relevant objective.

Data recipients	Google Firebase and Analytics 4 - Analytics of the data used by the Website and Mobile App. This Data Processor operates in the USA, for more information see: https://support.google.com/analytics/answer/6004245?hl=en . Google Ads, buying and displaying advertising to users on Google and its platforms. This Data Processor operates in the USA, for more information see: https://support.google.com/google-ads/answer/2549116?hl=en . Meta Pixel/SDK - buying and displaying ads to users on the Meta (Facebook) platform. This Data Processor operates in the USA, for more information see: https://www.facebook.com/legal/EU_data_transfer_addendum.

16.19. FOR THE PURPOSES OF ADMINISTERING SOCIAL NETWORKS

When is your personal data processed?	We manage our profiles and accounts on various social networks such as: • *https://www.facebook.com/CityBeeEstonia,* • *https://www.instagram.com/citybeeestonia/,* • *https://www.linkedin.com/company/citybee-car-sharing etc* If you are interested in our Services and follow our profiles on social networks, participate in our games, promotions, share your photo with us or tag us in your photo, public post, etc., we collect and use your data, which we receive directly from you, when you are active in our profiles. Please note that our accounts are integrated into social networking platforms (e.g. Facebook, Instagram, Linkedin, etc.) and therefore all social platform providers have full access to collect your other personal data. You can find detailed information on the data processing, purposes and scope of data use by each social networking platform in the privacy policy of the respective social network. If you want to exercise your rights in relation to data processed by social networks, it is more efficient to contact the controller of the social network directly.
Data categories	Name, surname, photo, account communication information ("like", "follow", "comment", "share", etc.), messages sent, information about messages (time of receipt of the message, content of the message, attachments to the message, history of the correspondence, etc.), comments, reactions to the posts posted, shares, information about participation in events and/or games we organise. A photo sent to us/ tagged by us and its public sharing.
Legal basis for processing	**GDPR 6(1)(a) - Consent:** • To process personal data when you voluntarily take active steps on our social media accounts.
Data retention period	The provider of the social network concerned shall set the time limits for the retention of data. We recommend that you check the privacy policy of the social network concerned. We do not delete obsolete posts on our social networks unless we have a need to do so or a written request.
Data recipients	Social network providers such as Facebook, Instagram, Linkedin, etc.

16.20. FOR THE PURPOSES OF ADMINISTERING BUSINESS CLIENT ACCOUNTS

When is your personal data processed?	If a business client (company, institution, organisation) enters into a Services Agreement with us for the provision of Services, we will process the personal data of the responsible persons provided by such business client and the employees attached to the Business Client Account accordingly. The processing of the Business Client's data is subject to all the purposes set out in this Privacy Policy in addition to the purposes for processing personal data set out in the General and Special Conditions of the Vehicle Rental and Service Agreement. If you are an employee or responsible person of a Business Client, you are subject to all the purposes set out in this Privacy Policy and you have all the data subject rights set out in Section 13 of this Privacy Policy. If your company (i.e. the Business Client) processes your personal data for purposes other than those set out in this Privacy Policy, then more detailed information must be provided to you by your company. ! In cases where you wish to be invoiced on behalf of a company of your choice and where you provide the details of the company concerned via the Mobile App, we will be entitled to transmit your personal data and more information about your trip(s) to that company upon request.
Data categories	Company name, address, company registration number, VAT code, payment card details (card type, last four digits of the card number, expiry date), Service Agreement; The name, title, email address, telephone number and other details of the person responsible for the performance of the Service Agreement; The name, title, email address and telephone number of the employee authorised to use the Company's business account; When employees use the Services through business accounts, all other data is collected and/or generated through the use of the Services and processed as described for all other data processing purposes. Once you have provided your company details for invoicing, we may provide the following personal data about you to that company upon request: name, date of travel, travel information, price.
Legal basis for processing	**GDPR 6(1)(b) - Contract performance:** • Establishing and implementing a Service Agreement.
Data retention period	If you do not use the Company's Services, for **the entire duration of the Services Agreement and for 3 months after its expiry.**
	after you have used the Company's Services - for **the entire duration of the Services Agreement and for 5 years after its expiry.**
	Section 7 of the Privacy Policy lists the cases and conditions under which this personal data may be stored or otherwise processed for longer periods of time.
Data recipients	All potential recipients of Data are identified for all other purposes of this Policy.

16.21. FOR STATISTICAL, ANALYTICAL, CLIENT BEHAVIOURAL RESEARCH PURPOSES

When is your personal data processed?	We analyse a variety of statistical data in order to monitor, evaluate, analyse, improve and enhance the quality of the Services, the Mobile App, to offer new or better Services, to increase the availability of the Services, to improve the security of the Services, and to improve the Client experience with the Services. The data analysis activities do not have a legal or similarly significant effect on you.

	It is also important to note that in the course of our analytics and statistics, we strive to process non-personalised aggregated data and do not process your contact or other information that explicitly personalises you. That is to say, the analytical and statistical data does not identify a specific Client, is not linked to other data of an identified user, and is not combined into Client-specific data sets.
Data categories	Vehicle reservations, the place and time of locking/unlocking, Vehicle information, the start of the reservation, the date and time of use, the locations where the Vehicle was picked up and dropped off, the Vehicle's GPS data, the route, the speed, the distance, the duration of the journey, the use of the fuel and the fuel card, the use of fuel, the use of the fuel card, the other travel parameters, the history of the journey, the telemetry data, all other data generated during the course of the Services, which is created and used by us for our activities as statistics only, and is not associated with any specific Clients. Profile analysis, age, country, city, frequency of use of the Services, etc.
Legal basis for processing	**GDPR 6(1)(f) - Legitimate interests of the Company and third parties:** • tracking and analysing performance; • implement and use data analysis and processing modules and techniques to create and enhance value for the Client and the Company;
Data retention period	The statistical datasets generated are stored for a maximum of 36 months after data generation (some analytical datasets do not require a long retention period and can therefore be deleted sooner).
Data recipients	Providers of data analysis software systems (EEA and non-EEA).

16.22. FOR THE PURPOSES OF ADMINISTERING, MAINTAINING AND IMPROVING THE WEBSITE

When is your personal data processed?	When you visit and browse our Website, for the purposes of collecting statistical data and improving the quality of the Service and the visitor experience, we process and analyse the data from the cookies used on the Website using Google Analytics, an analytics service that allows us to record and analyse statistical data about the use of the Website. For more information about Google Analytics and the information collected by its tools, please visit: https://support.google.com/analytics/answer/9019185?hl=en&ref_topic=2919631#zippy=%2Cin-this-article. For more information about the cookies used on the Website, please see our Cookie Policy here: https://citybee.ee/en/cookie-policy/
Data categories	IP address, MAC address, date of visit, duration of visit, pages visited, devices and applications used for web browsing, etc.
Legal basis for processing	**GDPR 6(1)(a) - Consent:** • to process data where you have consented to us using cookies to track your actions on the Website.
Data retention period	See Cookie Policy.
Data recipients	Google Analytics 4 - Provider of website usage data analytics. This Data Processor operates in the USA, for more information see: https://support.google.com/analytics/answer/6004245?hl=en .

16.23. FOR THE PURPOSES OF ORGANISING COMPETITIONS, EVENTS AND PROMOTIONAL CAMPAIGNS

When is your personal data processed?	When you participate in our various competitions, games, events and promotional campaigns, we collect and process your personal data in order to include you in the chosen competition activities. In addition, when we run public events and/or promotional campaigns in which you participate, we also create a range of additional footage and photographic material that we use to raise awareness of our activities. If you have been photographed at a public event, we may use your image (to a limited extent) for representational purposes for that event. If you have taken part in a photo and/or film shoot organised by us, we will use your image (broadly) for promotional purposes and will enter into an agreement with you regarding the use of your image.
Data categories	Name, surname, email address, phone number, comments on the entry, shares on the entry, information about clicks on "like" and "follow" on the social network account, information about reactions to the entries, photo, message, time of receipt of the message, content of the message, attachments to the message, reply to the message, time of reply to the message, information about participation in events, information about the evaluation, photos or videos - if they are intended for the competition as a condition of entry. Image as seen in a photograph, image and/or audio in a video, event, date of the event. Image use agreement.
Legal basis for processing	**GDPR 6(1)(a) - Consent:** • tracking the implementation of the terms and conditions of the tenderers and contacting the winning bidder; • run photo shoots and other promotional campaigns and share the results. **GDPR 6(1)(f) - Legitimate interests of the Company and third parties:** • capture and use for representational purposes images and/or videos of events we organise.
Data retention period	The data of the tenderers will be kept for 1 year from the date of the announcement of the winner.
	In the case of public events and promotional campaigns, the results produced will be made public for a period of 5 years from the date of the event or the date of consent. The results generated are stored for campaign archiving purposes for 10 years.
Data recipients	Providers of social networking platforms, partners or organisers of competitions (in the EEA and outside the EEA when competitions take place on social networking sites).

END OF PRIVACY POLICY