Privacy Notice nextbike App

General information about the processing of your data

We are required by law to inform you about the processing of your personal data (hereinafter "data") when using our apps. We take the protection of your personal data very seriously. This data protection notice informs you about the details of the processing of your data and about your legal rights in this regard. For terms such as "personal data" or "processing", the legal definitions from Art. 4 GDPR are authoritative. We reserve the right to adapt the data protection declaration with effect for the future, in particular in the event of further development of the apps, the use of new technologies or changes to the legal basis or the corresponding case law. We recommend that you read the privacy policy from time to time and take a printout or copy for your records.

1. Controller

The controller responsible for processing personal data within the scope of application of this Privacy Policy is:

nextbike GmbH
c/o Mindspace coworking
Friedrichstraße 68
10117 Berlin
Deutschland

Contact: datenschutz@nextbike.de

2. Data Protection Officer

You can reach our data protection officer at dpo@tier.app or at the above postal address ("Attn: Data Protection Officer"). We expressly point out that when using the email address, the contents are not exclusively noted by our data protection officer. If you wish to exchange confidential information, please therefore first contact us directly via this email address.

3. Security

We have taken comprehensive technical and organizational measures to protect your personal data from unauthorized access, misuse, loss and other external interference. To this end, we regularly review our security measures and adapt them to the state of the Art.

4. Your rights

You have the following rights with respect to personal information concerning you which you may enforce against us:

- **Right to information**: According to Art. 15 GDPR, you can demand information on the personal data which we process.
- **Right to rectification**: Should the information in question not (no longer) be correct, you can demand rectification according to Art. 16 GDPR. Should your data be incomplete, you can demand that your data be completed.
- **Right to erasure**: According to Art. 17 GDPR, you can demand erasure of your personal data.

- **Right to restriction of processing**: According to Art. 18 GDPR, you have the right to demand restriction of your personal data.
- **Right to object**: According to Art. 21(1) GDPR, you have the right at all times to object to the processing of your personal data as performed on the basis Art. 6(1)(1) point e) or point f) for reasons relating to your particular situation. In this instance, we will not continue processing your data unless we can demonstrate mandatory grounds for processing that require protection and which are superior to your interests, rights, and freedoms, including if such processing is being undertaken to establish, exercise or defend legal claims (Art. 21(1) GDPR). According to Art. 21(2) GDPR, you are furthermore entitled to the right to object to the processing of personal data relating to your person for the purposes of direct marketing at any time; this also applies in the event of any profiling insofar as such is directly connected to such direct marketing. We refer you to the right to object in this Data Protection Policy with regards to the respective processing.
- **Right to withdraw your consent**: Insofar as you have given your consent to processing, you have the right to withdraw such according to Art. 7(3) GDPR.
- **Right to data portability**: You have the right to receive such personal data concerning you which you have provided to us in a structured, commonly used and machine-readable format ("data portability"), and the right to have these data transmitted to a further controller, provided the prerequisite under Art. 20(1) point a), b) GDPR has been fulfilled (Art. 20 GDPR).

You may enforce your rights by sending communication using the contact details named under "Controller", or the Data Protection Officer we have named.

If you are of the opinion that the processing of your personal data breaches data protection law, you also have the right to lodge a complaint with a data supervisory authority of your choice according to Art. 77 GDPR.

5. Use of our apps

Installing our apps

Our nextbike apps are made available on platforms provided by third party providers (iOS, Android and Huawei) for downloading onto your end device. In order to be able to download the respective apps, these platforms may require registration. nextbike has no influence whatsoever on the processing of the data collected, which may possibly arise in the course of registration on the respective platform.

Push notifications in our apps

Through our nextbike apps, we can use push notifications to inform you about certain technical updates or news about nextbike, even if the apps are not actively in use at the time. If this service is not desired, the function can be disabled via the device settings.

Location-based service in our apps

If you have registered in our app and use our service, we collect location data to offer you nextbikes in your area. In addition, we collect the return location of your nextbike so that the nextbike you returned can be found by other users. To use these services, you must also actively confirm access to your location via the operating system of the mobile device you are using. We do not record any movement profiles and only record the location when the app is actively used.

System permissions of our apps

In order to provide you with all the functions of our apps, our apps must access various interfaces on the mobile device you are using. In order to ensure these interfaces, you must allow them actively in some cases, depending on the operating system of your end device. You can adjust or withdraw these settings at any time in the system settings of your end device.

- **Location services:** In order for our apps to be able to determine your location, you must allow our app to access the location services on the mobile device you are using. You can activate or deactivate this setting at any time via the system settings of your end device.
- **Notifications:** In order to offer you our push service, you must activate the authorization to send push notifications via the mobile device you are using. You can activate or deactivate this setting at any time via the system settings of your end device.
- **Camera access:** To capture the QR code on our nextbikes via our apps and thus rent the nextbike, you must confirm access to your camera via our app. You can activate or reverse this setting at any time via the system settings of your end device.
- **Mobile data or network access:** In order to use our apps, an internet connection of your mobile device is necessary. To do this, you must activate the mobile data or network access of your end device. You can activate or deactivate this setting at any time via the system settings of your end device.

6. Registration and tariff options

During or after registration, we offer you options to decide on the collection and use of your data in certain areas. You can exercise your choices and options via your user account. As a business customer, you can also contact your contact persons.

Registration/login area of the websites and apps

If you want to use the password-protected area on our websites and in our apps, you generally have to register using the following information:

- Address
- E-mail address
- First/last name
- Phone Number
- Location / City / Postcode
- RFID chip number (optional)
- If applicable, specification of co-user/partner (optional)
- Means of payment
- Ticket number (optional)

When registering for the use of nextbike in different cities and countries, different data is requested that is required for the registration in the respective cities/countries. Furthermore, at the time of registration, your IP address and the date and time of registration are processed. We use the double opt-in process for registration on the websites and in our apps. After you have submitted the data required for registration, you will receive an SMS with a personalized PIN code to activate your customer account. Only after successful activation by entering the PIN code is access to the customer account created and registration successfully completed. For subsequent registrations (logins), the access data (user ID, password) selected by you during the first registration must be entered. If confirmation by entering the transmitted PIN code is not received within 24 hours, we will block the information transmitted to us and automatically delete it after one month at the latest. Otherwise, your data will be deleted as soon as they are no longer required to achieve the purpose of their processing. This is the case for the data collected during the registration process when the registration on the website or in the apps is cancelled or modified and your customer account is balanced.

The following functions are available in the login area of the websites and the apps:

You can...

- Check your nextbike account balance
- Edit your profile data (enter and change name, contact details, PIN code)

- Change payment methods
- Cancel your customer account
- View and manage tariff options
- Manage, change or cancel your newsletter subscription
- Link your user account with your customer accounts of selected partner companies
- Redeem vouchers

If you use the password-protected area of the websites or apps, e.g. to edit your profile data, we also process the personal data required to initiate or fulfill the contract, in particular address data and information on the method of payment. The legal basis for the processing is Art. 6 para. 1 (1) point b) GDPR. The provision of your data is necessary and mandatory for the conclusion or performance of the contract. If you do not provide your data, you can neither register nor use the login area, i.e. a contract conclusion and / or execution is not possible. The data will be deleted as soon as they are no longer required to achieve the purpose of their processing, or processing will be restricted if legal retention periods exist. Due to mandatory commercial and tax regulations, we are obliged to store your address, payment and order data for a period of ten years. 6 months after termination of the contract, we restrict the processing and reduce the processing to compliance with existing legal obligations.

Partner program

As part of the use of your customer account, we offer you the opportunity to benefit from customer advantages and special conditions, such as free rides, with our partner program. You can select the respective partner companies/associations within your user account on our websites or in our apps by confirming the associated fields. In order to enable you to benefit from the respective customer advantages and special conditions, we process the following data from you depending on the design of the customer account of the partner company:

- Code
- Customer number
- Subscription number

In addition, you can enter your e-mail addresses in the user settings, with which you are registered with the respective partner companies or have a customer account there. The legal basis for the processing is Art. 6 para. 1 point b) GDPR. The provision of your data is necessary for the performance of the contract, and you are contractually obliged to provide your data.

If you do not provide your data, it will not be possible to conclude and / or execute the contract in the form of enabling customer benefits and special conditions. Your personal customer data will not be passed on to the respective partner companies. The respective partner companies may receive anonymized statistics on the number of customers who have made use of a customer benefit or special conditions by providing their customer data.

Ticket subscription / season tickets

You also have the option to select different fare options and timecards on the websites or in our apps, manage your selected options and subscribe to our annual and monthly cards. Registration to receive timecards is done via our online form within your user account. We process the data you provide during registration, such as your first and last name, address, etc., to execute the contract. The provision of your data is required for the execution of the contract and you are contractually obliged to provide your data. If you do not provide your data, it will not be possible to conclude and / or execute the contract. The legal basis is Art. 6 para. 1 (1) point b) GDPR. We delete the data accruing in this context after the storage is no longer necessary or restrict the processing if legal retention obligations exist. Due to mandatory commercial and tax regulations, we are obliged to store your address, payment data and order data in

accordance with §§ 257 HGB, 147 Para. 1 point 4, Para. 3 AO for a period of ten years. Two years after termination of the contract, we restrict the processing and reduce the processing to compliance with existing legal obligations.

Coorperation in the course of joint responsibility

Nextbike processes personal data with partner companies in the course of a so-called "joint responsibility“ according to Art. 26 (2) sentence 2 GDPR. The reasons for the cooperation as joint controllers result from the respective contractual relationships and responsibilities of the controllers in the course of the operation of a bicycle rental system and may differ with respect to the different systems. The following is a list of the partners with whom nextbike cooperates as joint responsible parties, and in each case a further link to the information sheet in which the essential background to the responsibilities can be viewed.

Cooperations:

- Mobiel GmbH (Flowbie Siggi Bielefeld): https://www.nextbike.de/media/20221024_TIER mobiel_Informationen zur gemeinsamen Verantwortlichkeit.pdf
- Innsbrucker Verkehrsbetriebe und Stubaitalbahn GmbH (Stadtrad Innsbruck): https://www.nextbike.de/media/20221024_TIER_IVB_Informationen-zur-gemeinsamen-Verantwortlichkeit.pdf
- Radland GmbH: https://nextbike-live.pluspol-networks.de/niederoesterreich/wp-content/uploads/sites/80/2024/02/DatenschutzerklarungHP.02022024.pdf
- Rhein-Main-Verkehrsverbund, Rhein-Main-Verkehrsverbund GmbH, Alte Bleiche 5, 65719 Hofheim am Taunus („RMV“)
- Berliner Verkehrsbetriebe (BVG) AöR, Holzmarktstrasse 15-17, 10179 Berlin, Deutschland („Jelbi“)
- Rheinbahn AG, Lierenfelder Str. 42, 40231 Düsseldorf, Deutschland („redy“)
- Rhein-Sieg-Verkehrsgesellschaft mbH, Steinstraße 31, 53844 Troisdorf-Sieglar („RSVG“)
- Stadtwerke Bonn Verkehrs-GmbH, Sandkaule 2, 53111 Bonn („BONNmobil“)
- Telekom MobilitySolutions DeTeFleetServices GmbH, Friedrich-Ebert-Allee 140
- Großraum-Verkehr Hannover GmbH, Karmarschstr. 30/32, 30159 Hannover („GVH“)
- Sixt GmbH & Co. Autovermietung KG, Zugspitzstr. 1, 82049 Pullach („SIXT“)

Registration via "Konstanz-Login"

If you have a user account with Stadtwerke Konstanz (Stadtwerke Konstanz GmbH, Max-Stromeyer-Straße 21-29, 78467 Konstanz) ("Konstanz-Login"), you can use it to create a user account with us and log in to our website. If you create a user account using the Konstanz-Login, we will receive your name and e-mail address from the Konstanz-Login service. Your user account with us and your Konstanz-Login account are linked by exchanging pseudonymous user IDs. If you change your data in your K-onstanz login account, your data will be updated automatically. For subsequent logins via the K-onstanzLogin, we exchange authentication data with the Konstanz login service. Stadtwerke Konstanz is solely responsible for data processing in connection with the K-onstanzLogin. The data transfers are required in accordance with Art. 6 para. 1b GDPR for your desired use of the K-onstanzLogin for registration and login and are therefore necessary for the provision of the services.

7. Collection and processing of location data

Collecting in the course of the rental process

For the purpose of faster traceability and billing, we locate the location (coordinate-based) of the respective bicycles within our business areas when renting and returning each bicycle. We do not track the distance traveled during the time the bicycle is borrowed. Insofar as we use the location data (GPS data) for billing purposes, the legal basis for the processing is Art. 6 para. 1 lit. b) GDPR. Otherwise, we base the processing of location data on the legal basis of Art. 6 (1) (f) GDPR, as we pursue the purpose of improving the service for our customers by being able to distribute the bicycles evenly in the city area. In addition, the GPS tracking serves the prevention and detectability of criminal offenses in connection with the use of the bicycles. After the purpose has been achieved (e. g. after the bicycle has been returned), the GPS data is blocked for further processing or deleted, unless we are entitled to further storage and processing required in the respective context on the basis of a consent granted by you, a contractual agreement, a legal authorization or on the basis of legitimate interests (e. g. storage for the enforcement of claims). Due to mandatory commercial and tax regulations, we are obliged to store GPS data that serve as a basis for accounting in accordance with §§ 257 HGB, 147 para. 1 No. 4, para. 3 AO for a period of ten years.

You may object to the processing. Your right to object exists for reasons arising from your particular situation. You can send us your objection via the contact details mentioned in the section "Controller".

Push notification: Location query

When you register as a new customer on our websites or in our apps, a (push) message usually opens asking for the use of your current location. In the event that you allow location access, we process this information for the analysis of the use of our websites and apps and to make our web offer more attractive as well as to provide you with additional service. The legal basis for the processing is Art. 6 para. 1 p. 1 lit. f) GDPR. We store this data for a maximum of 2 years after the page is accessed. Your data will not be passed on to third parties.

You can object to the processing. Your right to object is on grounds relating to your particular situation. You can send us your objection via the contact details mentioned in the section "Controller".

8. Payment / Payment provider

Payment Service Provider (PSP)/ Payment service provider / Credit check - Credit assessment via Abilita

Within the framework of payment processing, e.g. SEPA direct debit, we reserve the right to forward the bank details you have provided to external companies for the purpose of a credit check. For this purpose, we use the services of the online platform "Abilita" of Abilita GmbH (Prüfeninger Straße 20, 93049 Regensburg, Germany; hereinafter: Abili-ta) under the domain www.debitcheck.de to compare creditworthiness and economic information. The bank details (IBAN/BIC) you provide when creating a user account or depositing a means of payment within the user account are processed by us primarily for the purpose of processing payments. The legal basis in this case is Art. 6 para. 1 p. 1 lit. b) DSGVO. The provision of your payment data is necessary and obligatory for the conclusion or execution of the contract. If the payment data is not provided, it will not be possible to conclude and/or execute the contract by SEPA Direct Debit.

In order to carry out the creditworthiness query and for the purposes of fraud prevention and the avoidance of default risks, the bank connection data (IBAN/BIC) provided by you will be forwarded to "Abilita" and subjected to a check there. "Abilita" then checks the transmitted data with the help of

available information from credit agencies, retail and mail-order trade databases, public debtor lists and registers of telecommunications companies and compares them with databases of the following recipients:

- **CRIF Bürgel GmbH**, Leopoldstraße 244, 80807 München
- **infoscore Consumer Data GmbH**, Rheinstraße 99, 76532 Baden-Baden
- **SCHUFA HOLDING AG**, Kormoranweg 5, 65201 Wiesbaden

With the help of the return debit prevention pool (RPP) used here, the validity of the bank account, the existence of known return debits and the existence of a block on the bank account are then checked. In the process, a mathemati-cal-statistical procedure is used to determine or predict the payment behaviour. From this, after completion of the creditworthiness check via the online platform used by "Abilita", both the positive or negative prognosis of the credit risk in the context of soft, medium or hard negative features is transmitted to us as well as a score value which ena-bles us to make a decision on the establishment, implementation or termination of the contractual relationship with you as our customer. The determined score or probability values also allow conclusions to be drawn about the pay-ment behaviour to be expected in the future. If the result of the creditworthiness check is negative, i.e. a poor credit-worthiness or a low score value is determined, this may lead to restrictions in the payment methods provided by us and we may only be able to offer you a payment via selected, restricted payment methods.

The legal basis for processing by Abilita is Art. 6 para. 1 p. 1 lit. f) DSGVO. Our legitimate interests lie in the preven-tion of abuse and fraud, automated decision-making in relation to the determination of payment behaviour and the avoidance of default risks in accordance with Art. 22 (1) DSGVO. Further information on data protection at "Abilita" is available at https://www.debitcheck.de/datenschutz/ and https://abilita.de/datenschutz. We delete the data accruing in this context after the storage is no longer necessary or restrict the processing if there are statutory retention obli-gations. Due to mandatory commercial and tax regulations, we are obliged to retain your address, payment and or-der data for a period of up to ten years. Two years after termination of the contract, we restrict processing and re-duce processing to compliance with existing legal obligations.

You can object to the processing. You have the right to object on grounds relating to your particular situation. You can send us your objection via the contact details mentioned in the section "Person responsible".

PayPal

On our websites and in our apps, we offer you payment via PayPal. The provider of this payment service is PayPal (Europe) S.à.r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg (hereinafter: "PayPal"). If you select payment via "PayPal", the payment data you enter will be transmitted to "PayPal". The processing of your data at "PayPal" is based on Art. 6 para. 1 sentence. 1 point b) GDPR (processing for the performance of a contract). The provision of your payment data is necessary and mandatory for the conclusion or performance of the contract. If the data is not provided, a contract conclusion and / or execution with the payment method "Paypal" is not possible. The data required for payment processing are transmitted securely via the "SSL" procedure and processed exclusively for payment processing. We delete the data accruing in this context after the storage is no longer necessary or restrict the processing if legal storage obligations exist. Due to mandatory commercial and tax regulations, we are obliged to store your address, payment and order data for a period of up to ten years. Two years after termination of the contract, we restrict the processing and reduce the processing to compliance with existing legal obligations. Further information on data protection and the storage period at "PayPal" can be found at https://www.paypal.com/de/webapps/mpp/ua/privacy-full.

Credit card payments

For the purpose of payment processing, the customer provides the payment data required for the credit card payment to the credit institution commissioned with the payment. nextbike subsequently only stores an ID created by the payment service provider as well as a token in order to process future payments.

Payment service providers used by us are:

- Worldpay (Worldpay, The Walbrook building, 25 Walbrook, London EC4n8AF)
- Adyen (Adyen N.V., Simon Carmiggeltstraat 6-50, 1011 DJ Amsterdam)

The processing is carried out on the basis of Art. 6 para. 1 s. 1 point b) GDPR. The provision of your payment data is necessary and mandatory for the conclusion or execution of the contract. If the payment data is not provided, a conclusion of the contract and / or the execution by means of a credit card payment is impossible. The data required for payment processing are transmitted securely via the "SSL" procedure and processed exclusively for payment processing. We delete the data accruing in this context after the storage is no longer necessary, or restrict the processing if there are legal obligations to retain data. Due to mandatory commercial and tax regulations, we are obliged to store your address, payment and order data for a period of up to ten years. Two years after termination of the contract, we restrict processing and reduce processing to compliance with existing legal obligations.

Google Pay and Apple Pay

On our websites and apps, we offer you the option to pay with Google Pay or Apple Pay. This takes place via the payment provider Adyen (Adyen N.V., Simon Carmiggeltstraat 6-50, 1011 DJ Amsterdam). For the purpose of payment processing, the customer deposits the required payment data with Google Pay or Apple Pay. nextbike then only stores an ID created by the payment service provider and a token to process future payments.
The processing is carried out on the basis of Art. 6 para. 1 s. 1 point b) GDPR. The provision of your payment data is necessary and mandatory for the conclusion or execution of the contract. If the payment data is not provided, a conclusion of the contract and / or the execution by means of Google Pay or Apple Pay is impossible. The data required for payment processing are transmitted securely via the "SSL" procedure and processed exclusively for payment processing. We delete the data accruing in this context after the storage is no longer necessary or restrict the processing if there are legal obligations to retain data. Due to mandatory commercial and tax regulations, we are obliged to store your address, payment and order data for a period of up to ten years. Two years after termination of the contract, we restrict processing and reduce processing to compliance with existing legal obligations.
You can find more information about data protection at Adyen at:
https://www.adyen.com/de_DE/richtlinien-und-haftungsausschluss/privacy-policy.

Klarna Pay Now

You can choose the payment method Klarna Pay Now via the provider Adyen (Adyen N.V., Simon Carmiggeltstraat 6-50, 1011 DJ Amsterdam).
For the purpose of payment processing, the customer deposits the required payment data with Klarna Pay Now. nextbike then only stores an ID created by the payment service provider and a token to process future payments.
Since Klarna (Klarna Bank AB (publ), Sveavägen 46, 11134 Stockholm, Schweden) carries the risk of failure or, the risk for a return debit note your personal data is transferred to Klarna for them to carry out a credit check. This data includes a so-called unique account identifier, which is a name or number that is used to identify a customer. The date of registration, the last account change, your payment history, the payment option, the number and the total amount of money of successful purhcases, the date of the

first and last payment is transferred. You can find more information about Klarnas privacy at: https://www.klarna.com/de/datenschutz/#.
The processing is carried out on the basis of Art. 6 para. 1 s. 1 point b) GDPR. The provision of your payment data is necessary and mandatory for the conclusion or execution of the contract. If the payment data is not provided, a conclusion of the contract and / or the execution by means of Klarna Pay Now is impossible. The data required for payment processing are transmitted securely via the "SSL" procedure and processed exclusively for payment processing. We delete the data accruing in this context after the storage is no longer necessary or restrict the processing if there are legal obligations to retain data. Due to mandatory commercial and tax regulations, we are obliged to store your address, payment and order data for a period of up to ten years. Two years after termination of the contract, we restrict processing and reduce processing to compliance with existing legal obligations.

You can find more information about data protection at Adyen at: https://www.adyen.com/de_DE/richtlinien-und-haftungsausschluss/privacy-policy.

Cash payments via “viacash”

We offer the possibility of cash payment “viacash” via the payment service provider viafintech (Budapester Straße 50, 10787 Berlin).
As a nextbike customer, you have the option of making a deposit in the branches and/or ATMs of the viacash-partner companies (e.g Retailers, especially supermarkets, kiosks etc.) by presenting an individually generated number or barcode (“payment slip”) for the respectice transaction. You will receive this payment slip via SMS, for which your mobile phonenumber will be transferred to viafintech.
With every payment or payout slip request nextbike will transfer the specific transaction date for every customer to viafintech, which allows the customer to be uniquely assigned to a particular transaction (so called Customer ID). This date is transmitted pseudonymized, e.g alphanumeric.
The processing is carried out on the basis of Art. 6 para. 1 s. 1 point b) GDPR. The provision of your payment data is necessary and mandatory for the conclusion or execution of the contract. If the payment data is not provided, a conclusion of the contract and / or the execution by means of viacash is impossible.

Payment by mobile phone bill

On our websites and apps, we offer you the option to pay via mobile phone bill. This is done via the payment servce provider Dimoco (DIMOCO Carrier Billing GmbH, Campus 21, Europaring F15/302, 2345 Brunn am Gebirge/Wien). With choosing this payment method, your data, such as your mobile phone number, the user-ID (depending on your mobile phone provider) and your IP-address, will be transferred to Dimoco.

The processing is carried out on the basis of Art. 6 para. 1 s. 1 point b) GDPR. The provision of your payment data is necessary and mandatory for the conclusion or execution of the contract. If the payment data is not provided, a conclusion of the contract and / or the execution by means of apple pay is impossible. The data required for payment processing are transmitted securely via the "SSL" procedure and processed exclusively for payment processing. We delete the data accruing in this context after the storage is no longer necessary or restrict the processing if there are legal obligations to retain data. Due to mandatory commercial and tax regulations, we are obliged to store your address, payment and order data for a period of up to ten years. Two years after termination of the contract, we restrict processing and reduce processing to compliance with existing legal obligations.

You can find more information about data protection at: https://dimoco.eu/privacy-policy/

Purposes of enforcement or rights/address enquiry

In the event of failure to pay, we reserve the right to forward the data disclosed upon ordering/booking to a solicitor for the purposes of address enquiry and/or enforcement of rights. The legal basis for this processing is Art. 6(1)(1) point f) GDPR. We have a legitimate interest in preventing fraud and avoiding default risks. Furthermore, we will forward your data, where necessary, in order to protect our rights and the rights of our affiliated companies, our cooperation partners, our employees, and/or those of the users of our websites or our apps, and to the extent that processing is necessary. We will never sell or lease your data to third parties. The legal basis for processing is Art. 6(1)(1) point f) GDPR. We have a legitimate interest in this processing for the purposes of enforcing rights. We erase the data collected as soon as storage is no longer necessary, or alternatively we restrict processing in the event that there exist legal retention periods.

You may object to this processing. You have a right to object where there exists grounds related to your particular situation. You can communicate your objection to us using the contact details provided under the section “Controller”.

9. E-Mail-Marketing

Newsletter

You have the possibility to subscribe to our e-mail newsletter under "Account Settings - Profile", with which we will inform you regularly about the following contents:

- System News;
- Price changes / limited time offers;
- Promotions of our company.

To receive the newsletter, you must provide a valid e-mail address. We process the e-mail address for the purpose of sending our e-mail newsletter and as long as you have subscribed to the newsletter. We use an external e-mail marketing service to send the newsletter. You can find more information about these service providers in the section "Email marketing services".

The legal basis for the processing is Art. 6 para. 1 s. 1 point a) GDPR.

You can revoke your consent to the processing of your e-mail address for the receipt of the newsletter at any time, either by clicking directly on the unsubscribe link in the newsletter or by sending us a message via the contact details provided under "Responsible party". This does not affect the lawfulness of the processing that took place on the basis of the consent until the time of your revocation.

In order to document your newsletter registration and to prevent misuse of your personal data, registration for our e-mail newsletter takes place in the form of the so-called double opt-in procedure. After entering the data marked as mandatory, we will send you an e-mail to the e-mail address you provided, in which we ask you to explicitly confirm your subscription to the newsletter by clicking on a confirmation link. In doing so, we process your IP address, the date and time of your subscription to the newsletter and the time of your confirmation. In this way, we ensure that you really want to receive our e-mail newsletter. We are legally obliged to prove your consent to the processing of your personal data in connection with the registration for the newsletter (Art. 7 (1) GDPR). Due to this legal obligation, the data processing is based on Art. 6 para. 1 s. 1 point c) GDPR.

You are not obliged to provide your personal data during the registration process. However, if you do not provide the required personal data, we may not be able to process your subscription at all or in full. If no confirmation of the newsletter subscription is received within 24 hours, we will block the

information transmitted to us and automatically delete it after one month at the latest. After your confirmation, your data will be processed as long as you have subscribed to the newsletter.

In the event of unsubscription by exercising the revocation of the declaration of consent, we process your data, in particular your e-mail address, to ensure that you do not receive any further newsletters from us. For this purpose, we add your e-mail address to a so-called "block list", which makes it possible that you do not receive any further newsletters from us. The legal basis for the data processing is Art. 6 para. 1 s. 1 point c) GDPR in order to comply with our verification obligations, otherwise Art. 6 para. 1 s. 1 point f) GDPR. Our legitimate interests in this case are to comply with our legal obligations to reliably no longer send you newsletters.

You can object to the processing. Your right to object exists for reasons arising from your particular situation. You can send us your objection via the contact details listed in the section "Responsible party".

In addition, we process the aforementioned data for the establishment, exercise or defense of legal claims. The legal basis for the processing is Art. 6 para. 1 point c) GDPR and Art. 6 para. 1 point f) GDPR. In these cases, we have a legitimate interest in asserting or defending claims.

You may object to the processing. Your right to object exists for reasons arising from your particular situation. You can send us your objection via the contact details listed in the "Responsible party" section.

We also statistically evaluate newsletter opening rates, the number of clicks on included links and the reading duration, measure the reach of our newsletters and adapt the offers and information sent to your personal interests. For this purpose, the usage behavior on our websites as well as within the newsletters sent by us is evaluated on the basis of end device-specific information (e.g. e-mail client used and software settings). For this analysis, the e-mails sent contain so-called web beacons or tracking pixels, which are single-pixel image files that are also embedded on our website.

For the purpose of measuring reach, we measure the number of visitors who have reached our websites by clicking on links and who perform certain actions there, such as redeeming coupons and purchasing products via the online store. Depending on the reading behavior, we also form target groups to which we send newsletter content tailored to the identified user interest. In order to be able to adapt our newsletter even better to your interests, we assign your e-mail address or your user profile to other user profiles within our database.

The legal basis for the processing is Art. 6 para. 1 s. 1 point a) GDPR. We delete your data when you terminate the newslet-ter subscription.

Revocation of your consent is possible at any time, either by sending a message to us (cf. the contact details in the section "Responsible party" or by directly using the unsubscribe link contained in the newsletter. This does not affect the lawfulness of the processing that took place on the basis of the consent until the time of your revocation.

Email marketing service

We use the email marketing service "Braze" of the provider Braze, Inc.,330 W 34th St 18 th floor, New York, NY 10001, USA. Braze also processes your data in the USA. There is an adequacy decision of the EU Commission for the data transfer to the USA. If you have registered for the newsletter, the data provided during registration and the data processed during the use of our newsletter service will be processed on the servers of Braze. Braze acts as our processor and is contractually limited in its authority to use your personal data for purposes other than providing services to us in accordance with the applicable data processing agreement.

The legal basis for the processing is Art. 6 para. 1 p. 1 point f) GDPR. Our legitimate interests in using an external email marketing service lie in the optimization and more targeted control and monitoring of our newsletter content. For more information on data protection, please refer to the privacy policy of Braze: https://www.braze.com/company/legal/privacy.

You can object to the processing. Your right to object exists for reasons arising from your particular situation. You can send us your objection via the contact details listed in the "Person responsible" section.

10. Use of third-party tools

In order to provide and continuously improve our services, we rely on the services of the following third-party providers, through which personal data may also be processed.

Zendesk

We use the customer relationship management (CRM) service "Zendesk" to process customer requests. The tool is operated by Zendesk Inc, 989 Market Street #300, San Francisco, CA 94102, USA. Zendesk is used to handle inquiries via email, phone, or the contact forms on our apps and websites. We have concluded the required data protection agreement with the company Zendesk in accordance with Art. 28 GDPR. According to this agreement, Zendesk undertakes to ensure the necessary protection of your data and to process it exclusively on our behalf in accordance with the applicable data protection regulations.

When processing customer requests, Zendesk processes personal data collected in the course of the contractual relationship, such as telephone number, name, e-mail address, payment information, loan or address data.

The processing of your data takes place on EU servers offered by Zendesk. This is the content of the described agreement according to Art. 28 GDPR. For more information on Zendesk's compliance with data protection, please visit https://www.zendesk.de/company/privacy-and-data-protection/.

The legal basis of the processing is Art. 6 para. 1 point b GDPR. The personal data will be kept for as long as it is necessary to fulfil the purpose of the processing. The data will be deleted as soon as they are no longer necessary to achieve the purpose.

Cloudflare

For information security purposes, our apps use various services of the provider Cloudflare (Cloudeflare Inc., 101 Townsend St., San Francisco, CA 94107, United States). The following data may be processed in the process:

- Operating system used
- Host name of the accessing end device
- IP address
- Date and time of the server request
- Access status
- Amount of data transferred
- Time zone difference from Greenwich Mean Time (GMT)

We have concluded an order processing agreement with cloudflare in accordance with Art. 28 GDPR, after which processing of the data only takes place via servers located in the EU. The legal basis for the processing is Art. 6 para. 1 s. 1 point f) GDPR. Our legitimate interests lie in ensuring the functionality as well as the integrity and security of the apps.

For more information on data protection and the storage period at "Cloudflare", please visit: https://www.cloudflare.com/de-de/privacypolicy/ (section 7 "additional safeguards").

You may object to the processing. Your right to object exists for reasons arising from your particular situation. You can send us your objection via the contact details mentioned in the section "Responsible provider".

Braze push notifications

Via our nextbike app, we inform you with a push message service about individual offers, discount codes and news. You actively agree to this service at the start of app use or deactivate it. If you no longer want this service at a later time, you can deactivate this function at any time via your device settings.

To be able to send push messages, we use a service of the company Braze, Inc.,330 W 34th St 18 th floor, New York, NY 10001, USA. With the company Braze, we have concluded the required data protection agreement in accordance with Art. 28 GDPR. According to this agreement, Braze undertakes to ensure the necessary protection of your data and to process it exclusively on our behalf in accordance with the applicable data protection regulations.

Braze processes the following data to provide the service or to send our push messages:

- Date and time of the request
- End device information
- IP address
- Location data
- Browser type
- System information

If you have agreed to the use of push messages, this user data is statistically processed and evaluated in order to continuously improve our offers via push messages and to tailor them to your interests. The legal basis for the processing of your data for the purpose of registration, login or user management is Art. 6 para. 1 point a GDPR.

For more information about Braze's compliance with data protection, please visit https://www.braze.com/company/legal/privacy.

CleverReach

We use CleverReach (CleverReach GmbH & Co. KG, Schafjückenweg 2, 26180 Rastede, Deutschland) to send you E-Mails with necessary information about our services, prices, changes to our terms and conditions or changes the contractual relationship in general. We have concluded an order processing agreement with CleverReach in accordance with Art. 28 GDPR. Insofar as the information is relevant to the contractual relationship the legal basis is Art. 6 para. 1 lit. b) GDPR. Otherwise, the legal basis is your and our legitimate interest according to Art. 6 para. 1 lit. f) GDPR. You can find more information about privacy at: https://www.cleverreach.com/en/privacy-policy/

easyfeedback

Für das Erfassen der Kundenzufriedenheit nutzen wir easyfeedback (easyfeedback GmbH, Ernst-Abbe-Straße, 56070 Koblenz) zur Erstellung von Umfragen. Sie können freiwillig an einer Umfrage über easyfeedback teil. Es werden Ihre Antworten und der Gerätetyp, mit dem Sie an der Umfrage teilnehmen von easyfeedback gespeichert. Die weiere Erhebung von personenbezogenen Daten variieren bei jeder neuen Umfrage. Die eingegebenen Daten werden nur für den Zweck der Unfrage genutzt. Rechtsgrundlage dafür ist Art. 6 Abs. 1 lit. f) DSGVO. Mit easyfeedback haben wir einen Auftragsverarbeitungdvertrag gemäß Art. 28 DSGVO geschlossen. Weitere Informationen zur Einhaltung des Datenschutzes finden Sie unter: https://easy-feedback.de/privacy/datenschutz/.

Usercentrics

For our Apps we use the Software Usercentrics (Usecentrics GmbH, Sendlinger Straße 7, D- 80331 München) to collects, administer and store our customers consent.
For that personal data of our customers/registered Users and App Users is being processed. This personal data includes Login settings and user data such as their consent data (consent ID, Consent Number, consent Time, implicid or explicid consent, opt-in or opt-out, banner language, customer setting, template version) and devive data (http agent and http referer).
We have concluded an order processing agreement with Usercentrics in accordance with Art. 28 GDPR. According to this agreement Usercentrics is committed to ensure the necessary protection of your data and only process this data in accordance with the applicable data protection regulations on our orders. All data is being processebd on servers in the EU/EEA.
The legal basis for the processing is Art. 6 para. 1 s. 1 point c) GDPR in conjunction with. Art. 7 (1) GDPR, insofar as the processing serves to fulfill the legally standardized obligations to provide evidence for the granting of consent.

Google Analytics 4.0

In order to be able to optimally adapt our websites and apps to user interests, we use "Google Analytics 4.0", a web analysis service from "Google" (Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland and Google, LLC 1600 Amphitheatre Parkway Mountain View, CA 94043, USA). The "Google Analytics 4" analysis service uses technologies such as "cookies", "tracking pixels", "device fingerprinting" and programming interfaces to track specific user behavior on websites and in apps. Information stored on users' devices is also processed in the process. With the help of tracking pixels embedded in websites and cookies stored on users' end devices, Google processes the information generated about the use of our website by users' end devices and access data across all end devices for the purpose of statistical analysis - e.g., that a website or several specific web pages have been accessed or that a newsletter registration has taken place.

To analyze usage behavior, we use an application programming interface, the Firebase Software Development Kit (SDK), provided by Google to access end-device information such as the advertising ID (IDFA from Apple and GAID from Google) of the end device used and to enable statistical analysis of the use of the app. Google assigns a randomly generated user ID to which the respective usage behavior is assigned.

Using machine learning methods, Google automatically records user behavior and other events during interaction with our website/app. In addition, a cross-platform analysis of user behavior takes place on websites and apps that use Google Analytics 4 technologies. This makes it possible to record, measure and compare user behavior in different environments. For example, the user's scroll events are recorded automatically to enable a better understanding of how websites and apps are used. Different user IDs from different cookies or end device resources are used for this purpose. We are then provided with anonymized statistics on the use of the various platforms, compiled according to selected criteria.

With the help of "Google Analytics 4", target groups are automatically created for certain cookies or mobile advertising IDs, which are later used for renewed individualized advertising targeting. Target group criteria that can be considered are, for example: Users who have viewed products but not added them to a shopping cart or added them to a shopping cart but not completed the purchase, users who have purchased certain items. In this case, a target group includes at least 100 users. With the help of the "Google Ads" tool, interest-based advertisements can then be displayed in search results. In this way, users of websites can be recognized on other websites within the Google advertising network (in Google search or on "YouTube", so-called "Google Ads" or on other websites) and presented with tailored advertisements based on the defined target group criteria.

For these purposes, it can also be determined whether different end devices belong to you or your household.

Access data includes, in particular, the IP address, browser information, the website previously visited and the date and time of the server request. "Google Analytics 4" automatically shortens the IP address by the last octet in order to make it more difficult to relate it to a person. According to Google, the IP addresses are shortened within member states of the European Union. Due to the "Google Analytics" tool used, the user's browser automatically establishes a direct connection with Google's server. If users are registered with a Google service, Google can assign the visit to the user account and create and evaluate user profiles across applications.

Storage period: The storage period is 14 months.

Third-country transfer: Consent for Google Analytics also includes consent to the possible transfer of data to the USA. The USA is classified by the European Court of Justice as a country without an adequate level of data protection and without appropriate guarantees according to EU standards. In particular, there is a risk that your personal data may be processed by U.S. authorities for control and monitoring purposes, possibly without the possibility of a legal remedy to prevent access to data or to establish the illegality of the access. In addition, it cannot be guaranteed that your data subject rights can be fully implemented and supervisory authorities in the USA will take appropriate remedial action. The use of Google Analytics requires the third country transfer. If you do not wish to consent to the third country transfer, you must deselect Google Analytics.

The legal basis for the processing is your consent according to Art. 6 para. 1 s. 1 point a) GDPR. "Google" also processes the data in part in the USA. So-called "standard contractual clauses" have been concluded with Google to ensure compliance with an appropriate level of data protection. Upon request, we will provide you with a copy of the standard contractual clauses. Your data in connection with "Google Analytics 4.0" will be deleted after fourteen months at the latest. Further information on data protection at "Google" can be found at: http://www.google.de/intl/de/policies/privacy.

Revocation of your consents to the processing [and third-party transfer] is possible at any time by pushing back the slider in the "Advanced Settings" of the Consent Tool for the respective third-party provider. The lawfulness of the processing remains unaffected until you exercise the revocation.

Google Firebase

Our apps used the following Firebase services provided by Google Ireland Limited, Gordon House, Barrow Street, Dub-lin 4, Ireland ("Google", parent company: Google LLC , USA) to analyze app bugs and fix problems:

- Firebase Crashlytics

When the app crashes, an anonymized crash report is sent to Google in real time. This contains information related to your use of our app on the device state, device type, operating system, app version, time of the crash as well as an ID assigned by Firebase and location data at the time of the crash.

The legal basis for the use of Firebase services is Art. 6 para. 1 s. 1 point a GDPR, our legitimate interest is to provide our app and our services as error-free as possible, to analyze and eliminate any sources of errors and to optimize them accordingly.

Revocation of your consents to the processing [and third-party transfer] is possible at any time by pushing back the slider in the "Advanced Settings" of the Consent Tool for the respective third-party provider. The lawfulness of the processing remains unaffected until you exercise the revocation.

- Firebase Cloud Messaging

To communicate with our users within the app, we use Google's Firebase Cloud Messaging (FCM) messaging capabilities. To enable us to send topic-specific messages to individual recipients or user groups, we create message requests that are processed by Firebase Cloud Messaging to generate message types and send them to the recipients. For this purpose, we use an application programming interface, a Firebase Software Development Kit (SDK), provided by Google to access end device information such as the advertising ID (IDFA from Apple and GAID from Google) of the end device used. Firebase Cloud Messaging generates a message ID after a message request is created or received, which is sent to the recipient's end device via a transport layer. As part of the usage analysis, Google also processes end device information of the recipient, language settings as well as opening and click rates of the respective message.

Storage period: The storage period at Google is 6 months.

Legal basis for the use of Firebase services is Art. 6 para. 1 s. 1 point f GDPR. Our legitimate interest is to provide relevant services to customers, e.g. communicating the status of bike rentals or locations. "Google" also processes some of the data in the USA. So-called "standard contractual clauses" have been concluded with Google to ensure compliance with an appropriate level of data protection. We will provide you with a copy of the standard contractual clauses on request.

You may object to the processing. Your right to object exists for reasons arising from your particular situation. You can send us your objection via the contact details mentioned in the section "Responsible provider".

- Firebase Analytics

We use Google's external analytics and validation features, Firebase Analytics and Firebase Remote Configuration, to optimally tailor the app to users' interests. We use a programming interface, the Firebase Software Development Kit (SDK), provided by Google to access end-device information such as the advertising ID (Apple's IDFA and Google's GAID) of the end device used and to enable statistical analysis of the use of the app and segmentation of user interests. With the help of the Firebase SDK, we can define various events (e.g., average app usage, average sessions per user, button presses) in order to track and understand the behavior of app users across devices and thus optimize and improve the app's functionalities accordingly.

Revocation of your consents to processing [and third party transfer] is possible at any time by pushing back the slider in the "Advanced Settings" of the Consent Tool for the respective third party provider. The lawfulness of the processing remains unaffected until you exercise the revocation.

For more information about the Firebase services, see the Google LLC privacy notice at: https://firebase.google.com/support/privacy#examples_of_end-user_personal_data_processed_by_firebase and http://www.google.de/intl/de/policies/privacy

Huawai Mobile Service & AppGallery Service (only for Huawei devices)

For the provision of our app in the HUWAI AppGallary and the optimal use of the app on Huwai end devices, we use the following services:

Service: AppGallery Service

Provider: Aspiegel SE, First Floor, Simmonscourt House, Simmonscourt Road, Dublin 4, D04 W9H6, Ireland. Registration number 561134 ("Aspiegel").

Purpose: To provide the nextbike app in the Huawei AppGallery. Aspiegel is responsible for building the digital infrastructure and managing the daily operations of all Huawei Mobile Services.

Transfered data: Huawei ID, IP address, browser and device information, system information.

Legal basis is Art. 6 para. 1 p. 1 lit. f GDPR, our legitimate interest is the best possible offer and use of our services also for Huawei end customers.

You can find more information at https://consumer.huawei.com/minisite/cloudservice/hiapp/privacy-statement.htm?code=DE&branchid=2&language=en_GB

Service: HMS Core Map SDK

Provider: Huawei Software Technologies Co, Ltd.

Purpose: To analyze the required statistics on API calls and improve services based on the collected device and app information, and to provide the location display function for developer apps based on the collected location information.

Transferred Data: Device information, location, system information

Legal basis is Art. 6 para. 1 p. 1 lit. f GDPR, our legitimate interest is the best possible offer and use of our services also for Huawei end customers.

You can find more information at https://developer.huawei.com/consumer/en/doc/development/HMSCore-Guides/sdk-data-security-0000001061442563

Service: HMS Core Scan SDK

Provider: Huawei Software Technologies Co, Ltd.

Purpose: To equip app with functions such as barcode creation and scanning.

Transfarred data: Text and image information, app information, system information.

Legal basis is Art. 6 para. 1 p. 1 lit. f GDPR, our legitimate interest is the best possible offer and use of our services also for Huawei end customers.

You can find more information at https://developer.huawei.com/consumer/en/doc/development/HMSCore-Guides/sdk-data-security-0000001050043971

Translated with www.DeepL.com/Translator (free version) You may object to the processing. Your right to object is for reasons arising from your particular situation. You can send us your objection via the contact details listed in the "Responsible Provider" section.