

General information

1. Privacy

We, Canyon Bicycles GmbH (hereinafter referred to as "CANYON"), appreciate your interest in our app and our services. The protection of your personal data is important to us. In this privacy statement, we explain how we process your personal data, for what purposes and on what legal basis this is done and what rights you can assert in this context.

Our privacy notice for the use of our mobile app and services does not apply to your activities on the social networking sites or other providers that you may access through the links in our app. Please check the websites of these providers for their privacy policies.

Since changes in the law or changes in our internal processes may make it necessary to adapt this privacy policy, we ask you to read this privacy policy regularly.

2. Scope of application, responsible person and data protection officer

The provider within the meaning of the Telecommunications and Media Data Protection Act (hereinafter: TTDSG) and controller within the meaning of the EU General Data Protection Regulation (hereinafter: GDPR) and other national data protection laws of the member states as well as other data protection regulations is:

Canyon Bicycles GmbH

Karl-Tesche-Straße 12 56073 Koblenz Germany Phone: +49 (0) 261 9490 3000 E-mail: Please use our contact form at <https://www.canyon.com/de-de/contact/>.

This Privacy Policy applies to our mobile app and the services offered.

If you have any questions about data protection or this privacy policy, please contact our data protection officer:

Dr. Karsten Kinast, LL.M. KINAST Rechtsanwaltsgesellschaft mbH Hohenzollernring 54 D-50672 Köln Tel.: +49 (0)221 222 183 0 E-Mail: mail@kinast.eu Website: <http://www.kinast.eu>

3. Principles of data processing

Personal data is any information relating to an identified or identifiable natural person. This includes, for example, information such as your name, age, address, telephone number, date of birth and e-mail address, but also pseudonymous data such as your customer number or IP address. Information that we cannot relate to you (or only with disproportionate effort) is not personal data.

We process personal data (e.g. by collecting, querying, using, storing or transmitting) only if there is a legal basis for doing so. The processed personal data will be deleted as soon as the purpose of the processing has been achieved and there are no longer any legally prescribed retention obligations to be fulfilled.

In the following, we will inform you about the specific data processing processes, the scope and purpose of the data processing, the legal basis for the processing and the respective storage period.

I. General processing operations when using the App

1. Provision and use of the app

a. Type and scope of data processing

When you download our app, the required information will be transmitted to the respective app store, i.e. in particular the username, email address and customer number of your app store account, the time of download, the payment information and the unique device identification number. In addition, the respective app store collects various data from you independently. We have no influence on this data processing and we are not responsible for this data processing. We only process the data to the extent necessary to download the mobile app on your mobile device.

When you use our app, we collect personal data that your device either automatically transmits to our server or that is read by your device. When you use our app, we collect the following data in particular, which is technically necessary to display our app to you and to ensure its stability and security:

- IP address of the requesting device
- Learn more about the device you're using (brand, model name, operating system, app version, language)
- Date and time of installation or access
- Name and URL of the page/file accessed

We use the Microsoft Azure cloud computing platform (Microsoft Corp., 1 Microsoft Way Redmond, WA 98052 United States) as the backend service for the app, which provides APIs ("Application Programming Interfaces") that we need to display content to the user. All data collected in the course of using this app is processed on its servers. Processing on other servers only takes place within the scope explained in this declaration.

In the course of use, personal data may be transferred to countries outside the EU / EEA, in particular to the USA. The USA is classified by the European Court of Justice as a country with an insufficient level of data protection according to EU standards. Due to the lack of an adequacy decision and without adequate safeguards, there is a particular risk that your data will be processed by US authorities for control and monitoring purposes, possibly without any legal remedy. In order to be able to guarantee adequate protection of your personal data in the event of the transfer of personal data to such so-called third countries, we have entered into so-called EU-US standard contractual clauses with Microsoft. In addition, where possible, we are in contact with Microsoft to ensure the protection of your personal data by taking additional measures that may be necessary.

In addition, we process the following additional information, among others, for the purpose of error detection or correction or for marketing purposes:

- Access status (for example, whether you were able to access the app or received an error message).
- Information about the use of the app's features

b. Legal basis

The legal basis for the aforementioned data processing for the purpose of reading out the information stored on your device is § 25 para. 2 no. 2 TTDSG. The subsequent processing of your personal data is carried out on the basis of our legitimate interest in accordance with Art. 6 (1) (f) GDPR. The processing of the aforementioned data is necessary for the provision of an app and thus serves to safeguard a legitimate interest of our company.

c. Duration of storage

As soon as the aforementioned data is no longer needed to display the app, it will be deleted. The collection of data for the provision of the app and the (temporary) storage of the data in log files is necessary for the operation of the app. Further storage may take place in individual cases if this is required by law.

2. Cookies and similar technologies

a. Type and scope of data processing

When using the app, so-called **cookies and similar technologies (hereinafter referred to as "cookies")** are also used. Cookies can be used to store, enrich, read and manage information on the user's device.

A distinction can be made between essential cookies and optional cookies.

Essential cookies are necessary for the functioning of the App and our Service: The technical structure of the mobile app requires the use of technologies, in particular cookies. Without these technologies, our app and service cannot be used (completely correctly) or certain support features could not be activated. You cannot refuse these cookies if you want to use our app and service.

Optional cookies with your consent: We only set some cookies with your consent, which you can select via the consent checkbox on your first visit to our mobile app. The functions are only activated if you give your consent and serve in particular to analyse and improve the use of our mobile app and service, to make it easier for you to use it via different browsers or devices, to recognise you when you visit or to deliver advertising (possibly also to target advertising to your interests, measure the effectiveness of advertising or to show you interest-based advertising).

Detailed information about the individual cookies we use, as well as the option to give or revoke consent individually, can be found in our consent checkbox. You can change your settings at any time within the app under the My Canyon menu.

b. Legal basis

The use of essential cookies, which are necessary for the provision or use of the app and our service, is based on § 25 para. 2 no. 2 TTDSG. The subsequent processing of personal data is carried out on the basis of Art. 6 (1) (f) GDPR. The processing is necessary for the provision or use of the App and our Service and thus serves to safeguard our legitimate interests.

The use of optional cookies and the subsequent processing of personal data is carried out exclusively on the basis of the corresponding consent of the users in accordance with § 25 (1) sentence 1 TTDSG or Art. 1 sentence 1 TTDSG or Art. 6 (1) (a) GDPR. These consents can be revoked at any time with effect for the future.

c. Notes on the iOS operating system

In addition, you have various options in the iOS operating system to restrict advertising and tracking to a large extent, which is essentially done via the so-called "Advertising Identifier" (IDFA). This is a unique, but non-personalized, and non-persistent identification number for a specific device provided by iOS. The data collected through the IDFA is not linked to any other device-related information. We use the IDFA to provide you with personalized advertising, if necessary, and to evaluate your usage.

If you call up the "Privacy" option in the iOS settings, you can largely deactivate the advertising analysis under "Tracking". If you activate the "Allow apps to request tracking" function, you will be asked whether you agree to advertising measures when you use our app for the first time. You can turn ads on or off. In addition, you can select the option "Apple Advertising" under "Privacy" and deactivate the "personalized advertising". In the "Analytics & Enhancements" option, you can also disable the "Share iPhone Analytics" and "Enhance Siri & Dictation" features, which means that no static information about your iOS usage is transmitted to Apple. Please note that you may not be able to use all the features of our app if you restrict the use of IDFA.

3. App permissions

In order to provide some features of our app, it is necessary for the app to be able to access certain services and data of your mobile device/smartphone. Disabling permissions can prevent you from using certain features of the app.

The permissions can be managed via the operating system of your mobile device/smartphone, i.e. activated and deactivated. Depending on the operating system, the permissions are also automatically requested when the app is opened for the first time, but can be

activated/deactivated again at any time. If you are using a mobile device/smartphone with iOS, you can view the permissions under Settings -> CANYON and adjust them accordingly. On Android, you can find the permissions under Settings -> Apps -> CANYON.

Usually, you can enable/disable the following permissions on the device page:

- **Notifications:** The permission to send push messages is used, for example, to show you notifications about orders or other status events or actions, even if you haven't just opened the app. The notifications can be made through sounds, messages and/or icon displays.
- **Camera access:** With the camera access authorization, you can take a profile photo or scan a CANYON QR code on your bike.
- **Location:** If you have agreed to share your location, we may show you the location of your phone in relation to the location of your bike and your distance from your bike.

II. Individual processing operations when using our services

1. Registration / User Account My Canyon

a. Type and scope of data processing

As part of our app and also via our website, we offer you the opportunity to register for our service by providing your personal data. With the processed data, we create an individual user account for you, with which you can use our services.

The following overview shows you in detail what personal data we process when you register:

- Forenames
- Surname
- E-mail Address
- Password
- Date of birth (optional)

After registering, you can optionally enter the following data categories:

- Residential address
- Postal code
- Residence
- Mobile number
- Country you're signing up for
- Message settings
- Body height and step height

To make sure that you have actually registered, we will send you an e-mail with a confirmation link to your e-mail address after entering your data. Only when you click on the link, your account will be activated.

We use the service provider "Loqate GBG" (GB Group PLC, The Foundation, Herons Way, Chester Business Park, Chester, CH4 9GB, United Kingdom) to verify your address, email address and telephone number so that no false data enters our system.

In the course of processing, your data may therefore end up in the United Kingdom and thus outside the EU or the European Economic Area (EEA). The EU Commission has determined that an adequate level of protection comparable to the GDPR is guaranteed in the United Kingdom. Data transfers to the United Kingdom are therefore permissible under Article 45 GDPR. In order to legitimize the data processing, we have concluded a corresponding data processing agreement with the service provider. For more information about the processing of your data by an external service provider, please see point V. of this Privacy Policy.

b. Legal basis

The processing of the aforementioned personal data serves the performance of a contract or the implementation of pre-contractual measures between you and CANYON in accordance with Art. 6 (1) (b) GDPR. In addition, the measures may serve to prevent breaches of contract or violations of the law on the basis of our legitimate interest in accordance with Art. 6 (1) (f) GDPR.

c. Termination of registration / deletion of user account

As a user, you have the option of deleting your registration at any time. You can also change the data stored about you at any time via the settings of your user account. However, if the processed data is necessary for the processing/termination of a contract, premature deletion of the data is not possible.

d. Duration of storage

As soon as the processed data is no longer required for the performance of the contract, it will generally be deleted.

However, even after the contractual relationship with you has ended, it may be necessary to continue to store certain personal data in order to comply with legal obligations. In particular, due to statutory retention obligations (in particular tax and commercial regulations), we continue to store certain order, customer and contract data for up to 10 years after the termination of the contractual relationship with you. In this case, however, your data will only be stored and used within the framework of the applicable retention periods.

2. User Login

a. Type and scope of data processing

When you use our app for the first time, you will be asked to log in via your Canyon user account. For this purpose, we use the single sign-on solution of the identity provider "Salesforce" (salesforce.com Germany GmbH, Erike-Mann-Str. 31, 80636 Munich, Germany) for one-time user authentication. For authentication, after entering your username and

password, a so-called token is created, which compares your information once with the information from our user directory to validate your identity.

b. Legal basis

Art. 6 para. 1 lit. f) GDPR serves as the legal basis for the aforementioned data processing. The processing is necessary for the purposes of user authentication and identification and thus serves to safeguard our legitimate interests.

c. Duration of storage

Once the aforementioned data is no longer needed for user authentication, it will be deleted. This usually happens when you unsubscribe.

3. Registration and user login via social logins

a. Type and scope of data processing

We offer you the option of registering for our service via login plugins from **Facebook, Google and Apple**. An additional registration in our app is therefore not necessary. For this purpose, we use the single sign-on solution of the identity provider "Salesforce" (salesforce.com Germany GmbH, Erike-Mann-Str. 31, 80636 Munich) for one-time user authentication. If you make use of this option, you will be redirected to the provider's registration page, subject to your consent, where you can register with your user data. This will link your profile to the provider and our service.

If you log in via Facebook (Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA), we automatically receive the following information from the provider: first name, last name and e-mail address.

If you log in via **Google** (Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA), this connects your Google profile to our service. Through the connection, we automatically receive the following information from "Google": name, Google ID, profile URL and email address.

If you log in using your **Apple** ID (Apple Inc., 701 One Apple Park Way, Cupertino, 95014 CA, USA), we automatically receive the following information from "Apple": name, email address.

From a technical point of view, the respective provider integrates a corresponding button (so-called social plug-in) into our app. On our registration or login page you will find the buttons of the respective providers of the social networks supported by our website.

By clicking on the respective button, a new window opens in which you can log in with your access data for the social network. After successful registration, the social network will inform

you which data (name and e-mail address) will be transmitted to us for authentication as part of the registration or login process. If you have consented to this data transfer, the fields required by us for registration will be filled with the transmitted data.

The information we receive from the providers is necessary for the provision of our customer area and the conclusion of a contract in order to be able to identify you if you decide to use a social login. Via the login, we also transmit information about the user to the provider (e.g. the fact that you use our service, status messages, etc.). There is no connection between the customer account created with us and your account with the corresponding social network beyond the authentication process.

In order to be able to carry out the authentication process for registration and login, your IP address will be transmitted to the respective provider of the social network/provider after clicking on the corresponding button. To prevent the data from being transmitted to the providers in the USA without the user's knowledge, we have used passive buttons in our app. We have no influence on the purpose and scope of the data collection and the further processing of the data by the respective provider of the social network. For more information, please read the privacy policy of the respective provider.

In the course of use, personal data may be transferred to countries outside the EU / EEA, in particular to the USA. In order to be able to guarantee adequate protection of your personal data in the event of the transfer of personal data to such so-called third countries, we have concluded so-called EU-US standard contractual clauses with the providers. The USA is classified by the European Court of Justice as a country with an insufficient level of data protection according to EU standards. Due to the lack of an adequacy decision and without adequate safeguards, there is a particular risk that your data will be processed by US authorities for control and surveillance purposes, possibly without a legal right to it. In addition, where possible, we are in contact with the providers to ensure the protection of your personal data through additional measures that may be necessary.

b. Legal basis

The legal basis for the use of the social plugin and for the subsequent reading of the data processed in this way is your consent in accordance with § 25 para. 1 sentence 1 TTDSG. 1 sentence 1 TTDSG. You can revoke this consent at any time with effect for the future by sending an e-mail to privacy@canyon.com. The subsequent processing of your personal data for authentication purposes is carried out on the basis of your express consent in accordance with Art. 6 (1) (a) GDPR. You can revoke this consent at any time, preferably by sending an e-mail to privacy@canyon.com with effect for the future.

c. Duration of storage

Once the aforementioned data is no longer needed for user authentication, it will be deleted. This usually happens when you unsubscribe.

4. Push notifications for program changes

a. Type and scope of data processing

The app informs you with push messages on your device. With this feature, you will be notified as soon as there is a change in your program.

When using the push service, a device token from Apple or a registration ID from Google is assigned. These are encrypted, anonymized device IDs that are changed regularly. Their use serves exclusively to provide the push services. It is not possible for us to draw conclusions about the individual user.

You can enable/disable push notifications at any time as follows: Android: Settings -> Apps -> CANYON -> Notifications -> "Block All"; iOS: Settings -> Notifications -> CANYON -> Allow notifications -> Off.

We use the tool "Google Firebase" (Google Ireland Ltd., Google Building Gordon House, 4 Barrow Street, Dublin D04 E5W5, Ireland) to deliver push messages. Since Google Firebase only works with the assigned device IDs, no personal data is transmitted to Google.

b. Legal basis

In accordance with Art. 6 (1) (b) GDPR, the processing of the aforementioned personal data serves the performance of a contract between you and CANYON or the implementation of pre-contractual measures.

c. Duration of storage

As soon as the data is no longer needed for the provision of the service, it will be deleted.

5. Insurance

a. Type and scope of data processing

During the ordering process, you can insure your CANYON bike with the provider "Qover SA/NV", Rue du Commerce, 31 1000 Brussels, Belgium. If you wish to take out an insurance contract for your bike, CANYON will transmit the following data collected during the ordering process to Qover SA/NV:

- Last name, first name
- Date of birth
- Title
- Mailing address
- E-mail Address
- Landline phone number

- Number des Mobile Phones
- Value of a bicycle
- Type of bike
- Bicycle serial number
- Selected insurance option
- If applicable, the complaints
- the dates of the conclusion of the contract (date of conclusion of the insurance contract, date of commencement of the contract, date of end of the contract, status of the contract)

If you choose to insure your CANYON bike and click on the corresponding button, the app will redirect you to a web-based form from Qover. Qover collects all the data you enter in this form. After you have taken out insurance, Qover will send us the details of the insurance (insurance number and type of insurance). Qover SA/NV is an independent controller for the processing of the shared data, provided that the contract has been concluded solely for the purpose of insurance administration.

Both controllers could use the shared data to validate the billing process and payment flows. Both controllers could create retargeting/marketing campaigns to promote the insurance product.

b. Legal basis

The processing of the personal data submitted and its transmission to Qover serves the purpose of fulfilling the insurance contract between you and Qover or carrying out pre-contractual measures in accordance with Art. 6 (1) (b) GDPR.

c. Duration of storage

The data will be stored by both CANYON and Qover for as long as necessary for the performance of the insurance contract and then deleted. However, even after the contract with you has ended, it may be necessary to continue to store some of your personal data in order to comply with legal obligations. In particular, due to statutory retention obligations (in particular tax and commercial regulations), we and Qover will continue to store certain order, customer and contract data for up to 10 years after the termination of the contract with you. If the type of customer communication is also tax-relevant customer communication, it will also only be deleted after 10 years. In this case, however, your data will be stored and used exclusively for these purposes (fulfilment of retention obligations).

6. Accessing the camera and creating a profile picture

a. Type and scope of data processing

You can give the app access to your camera. If you give the app this permission, you can take your own pictures and save them as a profile picture, for example. Access to your camera is

also required to scan a CANYON QR code on your bike. If you decide to share your bike with family members or other people you want to give access to your bike to, we will show the profile picture in the shared invitation and in the app (as the owner of the bike).

Since we use the cloud computing platform Microsoft Azure (Microsoft Corp., 1 Microsoft Way Redmond, WA 98052 United States) as the backend service for the app, your image will be stored on their servers.

When used, personal data may be transferred to countries outside the EU/EEA, in particular to the USA. The USA is classified by the European Court of Justice as a country with an insufficient level of data protection according to EU standards. Due to the lack of an adequacy decision and without adequate safeguards, there is a particular risk that your data will be processed by US authorities for control and monitoring purposes, possibly without any legal remedy. In order to be able to guarantee adequate protection of your personal data in the event of the transfer of personal data to such so-called third countries, we have entered into so-called EU-US standard contractual clauses with Microsoft. In addition, where possible, we are in contact with Microsoft to ensure the protection of your personal data by taking additional measures that may be necessary.

b. Legal basis

The processing of your personal data is carried out exclusively on the basis of your explicit consent in accordance with Art. 6 (1) (a) GDPR, which you have given in the App. You can revoke this consent at any time with effect for the future by deactivating camera access on iOS under Settings -> CANYON -> Camera or on Android under Settings -> Apps -> CANYON. You can revoke your consent to the storage of your profile picture at any time with effect for the future by deleting your profile picture in your My Canyon profile.

c. Duration of storage

If you have withdrawn your consent, we will delete your data, unless there is a legal obligation to keep the data.

7. Location determination for bicycles

a. Type and scope of data processing

If you agree to location sharing, we can show you the location of your bike. By clicking on the "Connect" button, you activate the localization of your bike. The app asks for the location of the phone, which is determined by GPS.

To locate your bike, we work with a developer of connected bike systems. The bike sensor that is integrated into your bike can - if activated by your consent - send data continuously. You can choose to grant full or essential access. When fully accessed, the bike sensor

communicates the GPS location every 30 seconds while the bike is in motion. If you allow essential access, the location data will only be transmitted when the bike is moved. In addition, the sensor shares details about the bike such as battery level, odometer, and range. The shared GPS positions can be converted into a route.

We may also process and analyze the data collected in this way to gain insights into product performance and usage.

If you agree to location sharing under your app permissions, we can also show you your location in relation to the location of your bike and thus your distance to your bike.

b. Legal basis

The processing of your personal data is carried out exclusively on the basis of your explicit consent in accordance with Art. 6 para. 1 lit. a) GDPR that you have issued in the app. You can revoke this consent at any time with effect for the future by deactivating the "Theft Protection" in the app. This puts the device into a deep sleep mode so that no new location data is processed. If you want to completely deactivate the sensor and deregister your bike from this service, please contact CANYON via the following link: <https://www.canyon.com/de-de/contact/>.

c. Duration of storage

If you have withdrawn your consent, we will delete your personal data, unless there is a legal obligation to retain the data. We only keep the telemetry data, which consists of geolocation and technical data. It is ensured that there is no possibility of (re)establishing a personal reference.

8. Delivery and tracking

a. Type and scope of data processing

You can't order in the app, but you can view details about your order. In order to display your shipping status in the app, we process the data provided during delivery (name, delivery address). We do not offer tracking in the app itself, but we do display a link to the delivery service. If you click on the link, you will be redirected to the website of the delivery service. The respective delivery service is responsible for data processing in the context of delivery and delivery (either DHL Paket GmbH, Sträßchensweg 10, 53113, Bonn or United Parcel Service Deutschland S.à r.l. & Co. OHG, Görlitzer Straße 1, 41460 Neuss).

b. Legal basis

The processing of the personal data provided and its transmission serves the performance of the contract between you and CANYON in accordance with Art. 6 para. 1 lit. b) GDPR, insofar as this is necessary to check the delivery status of the ordered goods.

c. Duration of storage

As soon as your data is no longer required for the fulfilment of the contract for delivery, it will be deleted, provided that the deletion does not conflict with statutory retention periods. We delete the data for the purpose of delivery notification and coordination if you have revoked your consent or the purpose has ceased to exist and the deletion does not conflict with any statutory retention obligations.

9. Purchasing and payment processing

a. Type and scope of data processing

When you purchase products or services through our app, we process the data required for this. These include:

- Order Information: Items purchased, order number, date and time of order
- Customer data: name, address, e-mail address
- Payment Information: Depends on the payment method you choose (e.g., credit card information, PayPal or other payment processor information).
- Payment service providers: We use third-party payment service providers to process payments. Depending on the provider you choose, your payment details will be transmitted directly to them. Please note the privacy policies of the respective payment providers.
- Logistics company: We only pass on your order data if it is necessary for delivery.

b. Legal basis

The processing of your data is carried out for the performance of the contract in accordance with Art. 6 (1) (b) GDPR.

c. Storage period

We store your order and payment data in accordance with the statutory retention obligations. Invoice-relevant data is stored for up to 10 years in accordance with tax and commercial regulations.

10. Telephone customer service

a. Contact by Phone

You can contact us by phone to clarify your concern. In doing so, we process the personal data that you provide to us during the interview. To process customer enquiries, we use the ticket system of Natterbox, a customer service platform of Natterbox Ltd, No.1 Croydon, Croydon, London, CR0 0XT, UK.

b. Legal basis

The legal basis for the associated storage of information on your device and its subsequent reading is § 25 para. 2 no. 2 TTDSG. The subsequent processing of your personal data serves the effective processing of our customer inquiries and is therefore based on our legitimate interest in accordance with Art. 6 para. 1 lit. f) GDPR. If your contact request is aimed at concluding a contract, the legal basis is Art. 6 para. 1 lit. b) GDPR.

For your own protection of your personal data, we ask you to refrain in particular from providing us with special categories of personal data within the meaning of Art. 9 para. 1 GDPR (for example: health data).

The processing regularly takes place in the United Kingdom and thus outside the EU or the European Economic Area (EEA). The EU Commission has found that a sufficient level of protection comparable to the GDPR is guaranteed in the United Kingdom. Data transfers to the United Kingdom are therefore permissible under Article 45 GDPR. In order to legitimize the data processing, we have concluded a corresponding data processing agreement with the service provider.

c. Duration of storage

The data provided and the message history with our Service Desk will be stored for queries and follow-up contacts and deleted in accordance with data protection regulations after the purpose of storage has ceased to exist, unless there are statutory retention periods to the contrary.

Further information on data processing by Natterbox can be found in Natterbox's privacy policy at: <https://www.natterbox.com/privacy-policy/>.

11. Canyon Assist

a. Contact via our chatbot

You have the opportunity to ask various questions via our chat "Canyon Assist". To process your questions more efficiently, we use the AI-powered service ChatGPT from OpenAI, 3180 18th Street, San Francisco, CA 94110, USA.

When using Canyon Assist, interaction with the system may process certain information, including, for example, name, address, customer number, entered texts, communication data or other relevant information.

We have concluded a data processing agreement with OpenAI in accordance with Art. 28 GDPR to ensure the security of your personal data.

There may not currently be adequate safeguards in place for data transfers to the United States. The protection of personal data is limited by the fact that, under US law, security authorities can access data transferred from the EU to the USA and use it without restriction to what is strictly necessary. As a data subject without US citizenship, you cannot take legal action against such use. However, we have entered into standard contractual clauses with the service provider to ensure the security of your personal data.

b. Legal basis

The use of the chat for general communication is based on our legitimate interest (Art. 6 para. 1 lit. f GDPR) to provide efficient customer service.

Processing for profiling or personalized content is carried out exclusively on the basis of your consent (Art. 6 para. 1 lit. a GDPR).

c. Duration of storage

As soon as the processed data is no longer necessary, it is generally deleted.

In order to comply with legal obligations, we may store data for longer. In particular, due to legal retention obligations (in particular tax and commercial regulations), we continue to store certain order, customer and contract data for up to 6 years after the termination of the contractual relationship with you. In this case, however, your data will only be stored and used within the framework of the applicable retention periods.

12. MyCanyon

a. Customization

With **MyCanyon**, you can put together your own bike according to your wishes. Our partner **Quest, QUEST COMPOSITE TECHNOLOGY (TAIWAN) LIMITED**, No. 310, Rongchun St., Fengyuan Dist., Taichung City 420004, Taiwan (R.O.C.), will help us put together the right frame, your name sticker and the right components for you.

When you **use MyCanyon**, the following personal data may be transferred to Quest:

- Customer
- Order number
- Address number
- Name
- Street
- House number
- Postal code
- City
- Land
- State

We have entered into a data processing agreement with Quest in accordance with Art. 28 GDPR to ensure the security of your personal data.

b. Legal basis

The processing of your data serves the performance of a contract or the implementation of pre-contractual measures between you and Canyon in accordance with Art. 6 (1) (b) GDPR.

c. Duration of storage

Your data will be stored by both Canyon and Quest for as long as it is necessary for the performance of the contract and will then be deleted. However, in some cases, we may still need to retain certain information to comply with legal obligations.

In particular, order, customer and contract data are stored for up to 10 years after the end of the contract due to legal retention obligations (e.g. tax and commercial regulations). If it is tax-relevant customer communication, it is also deleted after 10 years. During this time, however, your data will be stored and used exclusively for these purposes.

How we protect your personal data

We do everything we can to keep your data secure. To do this, we use technical, administrative and physical security measures.

To protect your data during transmission, we use SSL (Secure Sockets Layer) encryption. We also adhere to PCI-compliant security standards when it comes to credit card payments.

Despite these measures, no data transmission over the Internet can be completely secure. There is always a risk that third parties will access transmissions or stored data without authorization. That's why you should make sure to keep your password safe and always log out after using a shared computer.

13. Newsletter

a. Type and scope of data processing

Based on your consent, we will inform you about current offers, news about our service and other news and for this purpose we will use your name and contact details that you provided to us during registration.

In connection with sending the newsletter, we use the "Salesforce Marketing Cloud", a tool of Salesforce.com, Inc. (One Market Street, San Francisco, CA 94105 USA), with which we have concluded a contract processing agreement in accordance with Art. 28 GDPR in order to ensure the security of your personal data.

There may not currently be adequate safeguards in place for data transfers to the United States. The protection of personal data is limited by the fact that, under US law, security authorities can access data transferred from the EU to the USA and use it without restriction to what is strictly necessary. As a data subject without US citizenship, you cannot take legal action against such use. However, we have entered into standard contractual clauses with the service provider to ensure the security of your personal data.

As part of the newsletter dispatch, it is also possible for us to send you surveys or give you the opportunity to participate in competitions. Participation in these actions is voluntary.

b. Legal basis

The processing of your personal data for the purpose of sending the newsletter is carried out on the basis of your consent, which you have given during the registration process, in accordance with Art. 6 para. 1 lit. a) GDPR. You can revoke your consent at any time and unsubscribe from the newsletter at any time by clicking on the corresponding unsubscribe link within our newsletter.

c. Duration of storage

Your personal data will be processed and stored for as long as you have subscribed to the newsletter, i.e. until you revoke your consent. If you unsubscribe from the newsletter, your data will be deleted. After unsubscribing from the newsletter by opting out, the opt-out will be saved so that you will no longer receive the newsletter.

14. Feedback-Formulate

a. Type and scope of data processing

To give us feedback on our app, you can leave us a message in our feedback form. We process the following data that can be assigned to your account: the probability that you would recommend our app to a friend (from 1-10) and your individual message telling us what you want for the app.

b. Legal basis

Art. 6 para. 1 lit. f) GDPR serves as the legal basis for the aforementioned data processing. The processing of the aforementioned data is necessary so that we can continuously develop our app in accordance with the needs of the users and thus serves to safeguard a legitimate interest of our company.

c. Duration of storage

The data will be stored for as long as it is necessary to achieve the purpose and will be deleted when this is no longer the case.

15. CANYON offers on social media

a. Type and scope of data processing

CANYON itself cannot present individual offers on networks such as Facebook, Instagram, Snapchat, LinkedIn or Google. Only the respective operator has this option. In order for us to be able to address our customers with individual offers, we use your pseudonymized or hashed data (e-mail address, telephone number, IDFA, Google Play Service ID) - if you have consented - to assign you to one or more target groups at the respective network operator. The hashed data is only used once and it is not possible for us to identify you or your device individually.

b. Legal basis

The processing of your personal data is carried out on the basis of your consent in accordance with Art. 6 para. 1 lit. a) GDPR, which you can revoke at any time with effect for the future.

c. Duration of storage

The personal data will be stored until the purpose for which it was collected has been achieved or no longer exists, and then deleted.

The personal data will also be deleted once you have withdrawn your consent.

16. Market Research/Surveys

a. Type and scope of data processing

For the purpose of quality assurance and to improve our services and products, we conduct personalized market and opinion research, in which you can participate on a voluntary basis. In doing so, we process the personal data collected from you as part of the measures.

b. Legal basis

The processing of your personal data is carried out on the basis of your consent in accordance with Art. 6 para. 1 lit. a) GDPR. Your consent can be revoked at any time with effect for the future.

c. Duration of storage

The personal data will be stored until the purpose for which it was collected has been achieved or no longer exists, and then deleted.

The personal data will also be deleted once you have withdrawn your consent.

17. Tracking and analytics tools

We use tracking and analysis tools to ensure the ongoing optimization and needs-based design of our app. With the help of tracking measures, it is also possible for us to statistically record the use of our app by users and to further develop our online offer for you with the help of the knowledge gained.

16.1 Google Analytics 4

a. Type and scope of data processing

We use Google Analytics 4, a web analytics service provided by Google LLC (for users within the EU: Google Ireland Limited, Gordon House Barrow St, Dublin 4, Ireland; outside the EU: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA), in our app for the purpose of reach measurement, personalized online advertising and remarketing. Google Analytics 4 uses the so-called IDFA, (Identity for Advertisers) or AAID (Android Advertising ID). An IDFA or AAID is a unique, random identifier assigned to each device.

By default, the following personal data is collected and processed, among others: gender, interests, age group of users, continent, subcontinent, country, region, city from which the user activity originates; device category (mobile, tablet), brand name and device model of the users; the platform on which the app was run, such as web, iOS, or Android; Operating system; the language set in the device's operating system; Operating system.

We create and assign a user ID to registered users. This allows us to analyze how you interact with our app across different platforms and devices. All data associated with the same ID is merged into a single user path in Google Analytics 4. This allows us to filter out unnecessary data and get a holistic view of your interactions.

When using Google Analytics, personal data may be transferred to countries outside the EU/EEA, in particular to the USA. The USA is classified by the European Court of Justice as a country with an insufficient level of data protection according to EU standards. Due to the lack of an adequacy decision and without adequate safeguards, there is a particular risk that your data will be processed by US authorities for control and monitoring purposes, possibly without any legal remedy. In order to be able to guarantee adequate protection of your personal data in the event of the transfer of personal data to such so-called third countries, we have concluded so-called EU-US standard contractual clauses with Google. In addition, we are in constant contact with Google to ensure the protection of your personal data by taking any additional measures that may be necessary.

The IP anonymization automatically activated in Google Analytics 4 means that your IP address will be shortened by Google within member states of the European Union or in other contracting states of the Agreement on the European Economic Area in order to ensure anonymized collection of IP addresses (so-called IP masking).

You can find more information about data processing and data protection by Google Analytics at: <http://tools.google.com/dlpage/gaoptout> or under <https://policies.google.com/> (general information on Google Analytics and data protection).

b. Legal basis

The legal basis for the use of this service for the associated storage of information on your device and its subsequent reading is your explicit consent in accordance with § 25 para. 1 sentence 1 TTDSG. 1 sentence 1 TTDSG. You can revoke this consent at any time within the app under the menu item My Canyon and change your settings. The subsequent processing of your personal data is carried out on the basis of your explicit consent in accordance with Art. 6 para. 1 lit. a) GDPR. You can revoke this consent at any time within the app under the menu item My Canyon and change your settings.

c. Duration of storage

The IDFA / AAID has no specific validity. The personal data collected with the IDFA / AAID will be stored for 50 months and then deleted if there is no other legal obligation to retain it.

16.2. Salesforce Data Cloud

a. Type and scope of data processing

We use Salesforce Data Cloud, a platform from Salesforce (Salesforce, Inc., 415 Mission St, 3rd Floor, San Francisco, CA 94105, USA) to integrate data from different sources and create a unified customer profile. In doing so, we comply with the data protection regulations of the European Union, in particular the General Data Protection Regulation (GDPR).

Salesforce processes personal data in accordance with the principles of the GDPR: lawfulness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity. This means that we only collect and process necessary data for specified and legitimate purposes.

We rely on Salesforce's security infrastructure, which includes robust technical and organizational measures, including encryption, access controls, and regular security audits.

When transferring personal data outside the EU, we ensure that appropriate safeguards are in place. These include EU standard contractual clauses or other recognised safeguards.

b. Legal basis

The legal basis for the use of this service for the associated storage of information on your device and its subsequent reading is your explicit consent in accordance with § 25 para. 1 sentence 1 TTDSG. 1 sentence 1 TTDSG. You can revoke this consent at any time within the app under the menu item My Canyon and change your settings. The subsequent processing of your personal data is carried out on the basis of your explicit consent in accordance with

Art. 6 para. 1 lit. a) GDPR. You can revoke this consent at any time within the app under the menu item My Canyon and change your settings.

c. Duration of storage

The personal data will be stored until the purpose for which it was collected has been achieved or no longer exists, and then deleted.

The personal data will also be deleted once you have withdrawn your consent.

18. Transfer to third parties

a. Type and scope of data processing

In addition, we pass on your personal customer data (name, address) to third parties if this is necessary to enable these third parties to contact you and so that these third parties can assert claims directly against you in the event of claims against CANYON that are not obviously unfounded, e.g. due to parking violations in the private sector.

We also transmit your personal customer data (name, address) to authorities, courts and other public bodies, external consultants or other authorized third parties, insofar as this is permissible under applicable law, e.g. if the processing is necessary to protect CANYON's legitimate interests. This can be the case, for example, if you commit an administrative offense.

b. Legal basis

The data processing is carried out on the basis of legal requirements in accordance with Art. 6 para. 1 lit. c) GDPR or our legitimate interests pursuant to Art. 6 para. 1 lit. f) GDPR.

c. Duration of storage

The personal data will be stored until the purpose for which it was collected has been achieved or no longer exists, and then deleted. In addition, the relevant retention periods of national laws apply.

III. Transfer to service providers, third countries or international organisations

We use service providers to provide services and process your data in connection with our services. The service providers process the data exclusively within the framework of our instructions and have been obliged to comply with the applicable data protection regulations. All service providers have been carefully selected and only have access to your data to the extent and for the period of time necessary for the provision of the services or for the period in which you have consented to the processing and use of the data.

If personal data is transferred to third countries or international organisations or, in certain cases, access to personal data from third countries is made possible, e.g. for maintenance work or technical support, this is done on the basis of appropriate safeguards within the meaning of Art. 44 et seq. GDPR.

If no adequacy decision has been issued by the European Commission in accordance with Art. 45 GDPR for the third country in question, we regularly base the data transfer on the so-called EU standard contractual clauses adopted by the European Commission, which we have concluded with the recipients of the data, as well as - where necessary - on additional technical and organizational measures to ensure a sufficient level of data protection. In addition, in certain individual cases, transfers of personal data may take place on the basis of the exceptions under Art. 49 GDPR.

IV. Are you obliged to provide your personal data - and what happens if you don't provide it?

The provision of personal data is always on a voluntary basis. However, the processing of certain personal data is necessary for the use of individual services. Without this data, it is generally not possible for us to offer the respective service or provide individual services.

V. Your Privacy Rights

You have the option to assert your rights as a data subject under the GDPR in the app itself by submitting a request. A ticket is then automatically created in customer service. The GDPR gives you the following rights as a data subject to the processing of personal data:

- In accordance with Article 15 GDPR, you can request information about your personal data processed by us. In particular, you may request information about the purposes of processing, the categories of personal data, the categories of recipients to whom your data has been or will be disclosed, the planned storage period, the existence of a right to rectification, erasure, restriction of processing or objection, the existence of a right to lodge, the source of your data if it has not been collected by us, via a transfer to third countries or international organisations and on the existence of automated decision-making, including profiling.
- In accordance with Art. 16 GDPR, you can immediately request the correction of inaccurate personal data or the completion of your personal data stored by us.
- In accordance with Art. 17 GDPR, you can request the deletion of your personal data stored by us, unless the processing is necessary for the exercise of the right to freedom of expression and information, for compliance with a legal obligation, for reasons of public interest or for the establishment, exercise or defence of legal claims.

- According to Article 18 GDPR, you can request the restriction of the processing of your personal data if the accuracy of the data is disputed by you, the processing is unlawful or we no longer need the data and you refuse to delete it because you need it to establish, exercise or defend legal claims. You also have the right under Article 18 GDPR if you have objected to the processing in accordance with Article 21 GDPR.
- Within the framework of the requirements of Art. 20 GDPR, you can request to receive your personal data that you have provided to us in a structured, commonly used and machine-readable format, or you can request the transfer to another controller.
- In accordance with Art. 7 para. 3 GDPR, you can revoke your consent at any time. As a result, we may no longer continue the data processing based on this consent for the future.
- According to Article 77 GDPR, you have the right to lodge a complaint with a supervisory authority. As a rule, you can contact the supervisory authority of your habitual residence, your place of work or our company headquarters .

Right to object

If the processing of your personal data is based on legitimate interests pursuant to Art. 6 para. 1 lit. f) GDPR, you have the right to object to the processing of your personal data in accordance with Art. 21 GDPR, provided that there are reasons for doing so that arise from your particular situation or the objection is directed against direct marketing. In the case of direct marketing, you have a general right to object, which we exercise without specifying a specific situation.

To exercise your rights, please contact the Data Controller or our Data Protection Officer as indicated in point I.2 above.

VI. Data security and security measures

We are committed to protecting your privacy and keeping your personal information confidential. In order to prevent manipulation, loss or misuse of your data stored by us, we take extensive technical and organizational security measures, which are regularly reviewed and adapted to technical progress. This includes, among other things, the use of recognized encryption methods (SSL or TLS). However, we would like to point out that due to the structure of the Internet, it is possible that the rules of data protection and the aforementioned security measures may not be respected by other persons or institutions that are not within our area of responsibility. In particular, unencrypted data transmitted - e.g. if this is done by e-mail - can be viewed by third parties. We have no technical influence on this. It is the responsibility of the user to protect the data provided by him against misuse by means of encryption or otherwise.

Status: March 2025

