Privacy policy - Use of the TRP / CMD app

Version: 1.0 | Status: 27.02.2025

The protection of your personal data is a top priority for us. This privacy policy explains how we process your data when you use our TRP / CMD app, always in compliance with data protection regulations, in particular the EU General Data Protection Regulation (GDPR).

§ 1 - Scope of application and person responsible

This privacy policy provides information about the processing of personal data in connection with the use of the TRP / CMD app (hereinafter "app").

The controller pursuant to Art. 4 No. 7 GDPR is:
TEKTRO Europe GmbH
August-Bebel-Straße 10
67454 Hassloch
Germany

Represented by the managing director Thomas Lattke.

Data Protection Officer pursuant to § 13 GDPR:
You can contact the data protection officer at info@tektro.eu (subject: To the data protection officer) or by post to the company address with the addition "Data protection officer".

§ 2 - Sources and categories of personal data

We process personal data that we receive as part of the provision and use of the TRP / CMD App ("App"). We also process personal data that we receive within the group of companies or from third parties (e.. cloud providers, technical service providers, analysis tools) in a permissible manner. Insofar as this is necessary for the app functions or to ensure security, we also process personal data from publicly accessible sources (e.. app store information, press reports, online databases), provided that the legal requirements for this are met.

Relevant categories of personal data are

- Contact details: E-mail address (required to create and manage the user account)
- Device and access data: Device type, operating system version, IP address, app and device identification features (e.g. ID) if applicable
- Usage data: Settings, switching operations, firmware information, charging cycles, ABS mode data and other operating parameters of the TRP components connected to the app
- Communication data: Content of communication with our support (e.. e-mail traffic or in-app requests)
- Crash and error reports: Data that is transmitted to our service providers (e.. Sentry.io) in the event of crashes or error messages

§ 3 - Purposes and legal bases of data processing

The provision of personal data is necessary for the proper functioning of the app so that a clear assignment and administration of the user account as well as technical communication with the TRP components can take place. Without this data, essential services of the app cannot be provided.

- Implementation of pre-contractual measures and fulfillment of the contract (Art. 6 para. 1 lit. b GDPR): We process personal data in order to provide the app functions and manage user accounts. This includes in particular
    - Registration and authentication of user accounts
    - Carrying out app updates and firmware updates for the TRP components
    - The processing of usage data and technical data of the TRP components to provide or improve the app functions.

  Without the provision of this data, it is not possible to use the app or individual functions.
- Consent (Art. 6 para. 1 lit. a GDPR): If you have given us consent to process your personal data for specific purposes, the data processing is based on this consent. A typical example is consent to the use of analysis tools (e.. Google Analytics), provided that an opt-in procedure has been implemented. You can withdraw your consent at any time with effect for the future. This does not affect the processing that took place prior to the withdrawal.
- Legitimate interests (Art. 6 para. 1 lit. f GDPR): We process personal data insofar as this is necessary to protect our legitimate interests or the legitimate interests of third parties. This includes, among other things:
    - The analysis and further development of TRP components (e.. evaluation of usage and switching processes)
    - Ensuring IT security as well as troubleshooting and rectifying errors in the app (e.g. by means of crash and error reports)
    - Assertion and defence of legal claims, internal administrative purposes and other organizational measures

  We always take your interests and fundamental rights into account in order to ensure an appropriate balance between our interests and your rights.
- Legal obligations (Art. 6 para. 1 lit. c GDPR): We are subject to various legal requirements (e.. retention obligations under commercial and tax law). In this context, we only process your personal data to the extent necessary to fulfill these obligations.
- Changes of purpose: Where legally permissible, we also process your personal data for purposes other than those originally intended. This is done in accordance with Art. 13 para. 3 GDPR. This is the case, for example, if the new purposes are compatible with the original purposes, e.g. when introducing new services or continuing to use your data for new services that are closely related to the original service provision. This further processing always takes place within the framework of the applicable legal requirements.
- Training measures: We process your personal data for internal training purposes for our employees and external processors, provided you have consented to this or there is a legitimate interest on our part. These measures serve the continuous improvement of our service quality. You can withdraw your consent at any time with effect for the future. If no express consent has been given, your personal data will be used for training purposes exclusively in anonymized form, which does not allow any conclusions to be drawn about your person.
- No processing for marketing purposes: We do not currently use your personal data for advertising purposes such as direct advertising, newsletters or other marketing measures. Should this change in the future, we would inform you of this separately in advance and obtain your consent accordingly.

§ 4 - Data collection methods

The collection of personal data within the TRP / CMD App ("App") takes place in various ways, whereby a distinction can be made between direct and indirect data collection:

- Direct survey:

- Registration and user account: When creating a user account in the app, an e-mail address is requested. This information is required to clearly assign the account and to be able to use it to reset the access data. After entering your e-mail address for registration, we may send you a confirmation e-mail via our own SMTP server. Your account will only be finally activated after you click on the corresponding activation link (double opt-in). This ensures that you are the owner of the e-mail address provided and that you agree to the creation of an account.
- Support requests and communication: In the event of contact, for example via support functions provided in the app or by email, the transmitted data (e.g. content data, contact data, device data) is recorded directly.

– Indirect survey:
  - Technical usage data: When using the app and connecting to TRP components (e.. gears, brakes, ABS), certain usage and diagnostic data is automatically logged. This includes shifting operations, battery charging cycles, firmware versions, ABS mode and error or crash data (crash reports).
  - Analysis tools: If analysis tools (e.. Google Analytics) are implemented in the app, usage statistics and interactions are collected if consent or another legal basis exists for this.
  - Data from third parties: In individual cases, information from third-party providers (e.. cloud service providers, analysis tools) may also be added, for example to ensure the functionality of the app, create error reports or provide updates.

The data collected is used to enable the app functions, process technical support requests, implement security measures and continuously improve the app and the associated TRP components.

§ 5 - Concrete processing

As part of providing the app, we process your personal data for the following purposes:

– Provision of the app functions:
  - User account and registration: A user account is required to use the TRP / CMD app. A valid e-mail address is required for this. This is used to clearly assign your account and to enable a password reset. If necessary, a double opt-in procedure is used, in which you receive a confirmation email and your account is only activated after clicking on the activation link.
  - Regular account verification: If there is an Internet connection, the validity of the user account is checked from time to time to ensure that the registered e-mail address is still active.
  - Connecting TRP components: TRP shifters, brakes or ABS units can be connected via the app. Device-specific data (e.. firmware version, current settings, charging cycles) is read out and transmitted so that the corresponding app functions can be used. Depending on the product (e.. electronic shifting, TRP ABS), individual settings can only be accessed via the app.

– Analysis and optimization:
  - Usage data of the TRP components: In order to enable diagnoses, make product improvements and optimize future developments, we collect detailed usage information on the connected TRP components. This includes in particular Settings for sprocket packs (cassettes) and shifting modes (e.. manual or automatic); number of shifting operations and gears used; battery charging cycles for electronic shifting; ABS modes used (if a TRP ABS system is coupled).

As a rule, this data is stored on our servers and evaluated in anonymized or aggregated form in order to draw conclusions about general usage habits and improve product quality.
    - Error and crash reports: Crash data is processed by service providers in order to identify sources of errors and increase the stability of the app. Technical device data and other metadata can be transmitted for this purpose.
- Support and maintenance
    - Support requests: For support requests, contact details, communication content and relevant device and app information are processed to enable efficient problem solving.
    - Firmware updates and maintenance: The app offers options for installing firmware updates on TRP components. Version data and update packages are processed for this purpose.
- Documentation and archiving:
  To fulfill legal obligations, we document the progress of support requests (e.g. in the event of defects or error messages) and the associated communication. This data is archived in accordance with the relevant retention obligations and deleted or anonymized after expiry of the statutory periods, unless there is a legitimate interest in longer storage.

Automated decision-making and profiling
Automated decision-making or profiling does not take place within the scope of our services or when purchasing products.

§ 6 - Recipients of the data

We only pass on personal data if this is permitted under German or European data protection law. Our external service providers may only process your data under special conditions and in accordance with our instructions. If we use service providers as processors, they will only have access to your data to the extent and for the period required to provide the respective service.

Internal receiver
Employees who are entrusted with the development, maintenance and support of the app.

External receivers
Your personal data may be passed on to the following categories of recipients as part of the TRP / CMD app, insofar as this is necessary for the provision of the app functions, the fulfillment of the contract or due to legal obligations and is permitted under German or European data protection law:

- Authorities and other third parties: e.g. police, public prosecutor's office in the event of a legal obligation
- Companies within the group of companies: e.g. for administrative purposes
- Partner companies: e.g. companies that provide specialized services (such as app development, firmware updates or external analysis services) or suppliers that are involved in the functionality and maintenance of the app.
- Debt collection legal service provider: for the enforcement of legal claims or representation in the event of a dispute.
- Marketing and analysis service providers: to optimize and analyze the app functions (if consent has been given or there is a legitimate interest in data processing).
- Technical service providers: e.g. cloud and hosting providers, IT support companies that maintain our systems or process error and crash reports.
- External employees (freelance processors): If necessary, we use external freelance employees who provide certain repair, support or administration services on our behalf and

are given access to personal data for this purpose. Appropriate data processing contracts are concluded with these external employees to ensure the protection of your data.

In the following, we name the individual external service providers to whom personal data is transmitted and explain which categories of data are processed and for what purpose:

1. Sentry
   - Recipient: Functional Software, Inc., 45 Fremont Street, 8th Floor, San Francisco, CA 94105
   - Processed data: Crash and error reports (crash reports), possibly technical device data.
   - Purpose of processing: Error analysis, stability improvement and troubleshooting.
   - Legal basis for data transfer: The data transfer takes place on the basis of EU standard contractual clauses in accordance with Art. 46 para. 2 lit. c GDPR.
   - Reference to risks: The level of data protection in the USA is not comparable to that in the EU. There is a risk that US authorities may be able to access your data without you having effective legal remedies.
2. Google Analytics (Google Ireland Limited / Google LLC)
   - Recipient: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.
   - Processed data: In particular, Google Analytics processes usage statistics (e.. length of stay, interactions within the app), device information and location-based metadata. IP addresses of users from the EU are anonymized before each storage and are not logged.
   - Purpose of processing: The analysis of user behavior serves to optimize and further develop the app functions.
   - Hosting and data processing in the EU: Google Ireland Limited ensures that data from end devices located in the EU (according to IP address) is collected via EU-based domains and servers before being forwarded to other Analytics servers. IP addresses are not stored permanently in Google Analytics and are anonymized before any storage.
   - Note on potential data transfer to the USA: Although Google Analytics can be hosted in the EU, a transfer of data to Google LLC (USA) is not completely excluded (e.g. for technical support services or internal administrative purposes). In the USA, there is no level of data protection equivalent to EU law. In this respect, it cannot be ruled out that US authorities may access the data without there being any effective legal remedies against this. Any data transfer that takes place is based on EU standard contractual clauses in accordance with Art. 46 para. 2 lit. c GDPR.
3. Supabase
   - Recipient: Supabase, Inc, 970 Toa Payoh North, Singapore.
   - Processed data: E-mail addresses (user accounts), usage and diagnostic data (e.. switching operations, firmware information), database backups.
   - Purpose of processing: Supabase provides a cloud database platform to store and manage the data generated in the TRP / CMD app (accounts, product usage data).
   - Hosting in the EU: According to its own information, Supabase operates servers and infrastructure in Europe for customers from the European Economic Area (EEA), meaning that data processing generally takes place within the EU.
   - Legal basis: Either Art. 6 para. 1 lit. b GDPR (fulfillment of contract, if data processing is necessary for the use of the app) or Art. 6 para. 1 lit. f GDPR (legitimate interest in secure and efficient data management). Alternatively: Art. 6 para. 1 lit. a GDPR (consent), if corresponding functions or declarations of consent are available.
   - Potential transfer to third countries: In the event that support or maintenance services are provided from outside the EEA, data may be transferred to third countries (e.. USA). Any data transfer is carried out on the basis of EU standard contractual clauses in accordance with Art. 46 para. 2 lit. c GDPR.
4. Amazon Web Services (AWS)

- Recipient: Amazon Web Services, Inc, 410 Terry Avenue North, Seattle WA 98109, United States.
- Processed data: Depending on the technical implementation, all data processed by the app via Supabase can be hosted on AWS. This includes account data (email addresses), usage and diagnostic data of the TRP components as well as backups.
- Hosting in the EU: The servers are located in the AWS data center "Europe (Ireland)" (eu-west-1). This is a location within the European Economic Area (EEA).
- Purpose of processing: AWS provides the underlying cloud infrastructure for Supabase and enables the hosting and technical operation of the app data.
- Legal basis for data transfer: The processing is based either on Art. 6 para. 1 lit. b GDPR (fulfillment of contract) or Art. 6 para. 1 lit. f GDPR (legitimate interest in a secure, globally available and efficient cloud environment).
- Security and data protection measures: According to AWS, comprehensive technical, organizational and contractual measures are taken to protect personal data. These include encryption at rest, encryption in transit and the control and logging of access authorizations (e.. AWS Identity and Access Management, CloudTrail). AWS only processes customer data in accordance with the documented instructions of its customers and has internationally recognized certifications, such as ISO 27017/27018, 27701.
- Data transfer to third countries: If access to data by AWS employees or subcontractors outside the EEA is necessary (e.. in the context of maintenance and support requests), this may lead to a transfer of personal data to third countries. In such cases, a suitable legal basis, in particular a Data Processing Addendum offered by AWS including standard contractual clauses pursuant to Art. 46 GDPR, will be used. However, an equivalent level of data protection as in the EU cannot always be guaranteed in these third countries.

5. Unlockd
   - Recipient: Unlock'd, Veldkant 33A, 2550 Kontich, Belgium.
   - Processed data: Usage data, support and development data, contact data if applicable.
   - Purpose of processing: Development and maintenance of the app, provision of updates and customer support.
   - Legal basis: Order processing pursuant to Art. 28 GDPR.
6. TRP Cycling
   - Recipient: TRP Cycling, 688 W Amidan Dr. Bldx 4X-1, Ogden, Utah 84404, USA.
   - Processed data: Device data, contact data if applicable.
   - Purpose of processing: To carry out specific repair and support services, product development.
   - Legal basis for data transfer: The data transfer takes place on the basis of EU standard contractual clauses in accordance with Art. 46 para. 2 lit. c GDPR.
   - Reference to risks: The level of data protection in the USA is not comparable to that in the EU. There is a risk that US authorities may be able to access your data without you having effective legal remedies.
7. TEKTRO Technology Corporation (parent company in Taiwan)
   - Recipient: Tektro Technology Corp. NO. 338, SEC. 2, CHANG SHUI RD, PU YEN HSIANG, CHANG HUA HSIEN, Taiwan.
   - Processed data: Support tickets, device data, contact details and purchase details (e.g. order information, shipping addresses).
   - Purpose of processing: product improvement, analysis of software and hardware problems, research and development.
   - Legal basis for data transmission: We have taken technical and organizational measures to ensure the protection of your data. This data will only be transmitted if it is necessary to fulfill the above-mentioned purposes.
   - Reference to risks: There is no adequacy decision by the EU Commission in Taiwan. It cannot be guaranteed that a level of data protection comparable to that in the EU exists. There is a

risk that government agencies may be able to access your data without you having effective legal remedies.

Data transfer to third countries
Other personal data will only be transferred to third countries (outside the EU/EEA) if there is an adequacy decision by the European Commission for the third country in question or on the basis of suitable guarantees (e.g. EU standard contractual clauses, binding internal data protection regulations). In certain cases, your express consent may also serve as the basis for data transfer.

Data processing contracts
Appropriate contracts for order processing have been concluded with all external service providers who process personal data on our behalf in order to guarantee the protection of your data. In the case of independent service providers, such as shipping companies, data is passed on on the basis of the applicable data protection laws.

§ 7 - Duration of data storage

We only store your personal data for as long as is necessary for the purposes stated in this privacy policy. The data will be deleted as soon as the purpose has been fulfilled and there is no longer a legal obligation to continue storing it. If your customer account is deleted, all personal data will be deleted unless there is a legal obligation to retain it (e.g. commercial and tax law requirements in accordance with the German Commercial Code (HGB) and Tax Code (AO)) or a legitimate interest, such as the assertion or defense of legal claims.

- Automatic deletion: If there has been no contact with you within three years, we will automatically delete your personal data, unless legal obligations or legitimate interests prevent this.
- Criteria for determining the storage period: The storage period depends on the statutory retention periods and the respective purpose of the data processing. These include, in particular, the legal requirements for document retention in accordance with the German Commercial Code (HGB) and the German Tax Code (AO). In addition, we store data for as long as is necessary for the enforcement, exercise or defense of legal claims.

When your user account is deleted, all personal data in the active system will be removed immediately. Please note, however, that for technical reasons our service provider (e.. Supabase) may have data backups in which your account and usage data will remain stored for up to 7 days before final deletion also takes place there. During this backup phase, your data is no longer actively available and is stored exclusively for the purpose of data backup.

§ Section 8 - Rights of data subjects

Under the legal requirements, you have the following data protection rights:

- Right to information (Art. 15 GDPR): You can request information about the personal data processed by us and further information such as processing purposes and recipients.
- Right to rectification (Art. 16 GDPR): You have the right to demand the immediate correction of incorrect or incomplete personal data.
- Right to erasure (Art. 17 GDPR): You can request the erasure of your personal data, in particular if the data is no longer required for the original purposes or if you have withdrawn your consent.
- Right to restriction of processing (Art. 18 GDPR): Under certain circumstances, e.g. if you dispute the accuracy of the data, you can request the restriction of data processing.

- Right to data portability (Art. 20 GDPR): You may request that your personal data be provided in a structured, commonly used and machine-readable format or transmitted to another controller.
- Right to object (Art. 21 GDPR): You can object to the processing of your personal data at any time, in particular if the processing is based on legitimate interest.
- Right to lodge a complaint with the supervisory authority (Art. 77 GDPR): You have the right to lodge a complaint with a data protection supervisory authority if you believe that the processing of your data violates the GDPR.

You can contact our data protection officer to exercise your rights. The contact details can be found in section "§ 1 - Scope and controller". Alternatively, you can also contact the competent data protection supervisory authority:

The State Commissioner for Data Protection and Freedom of Information Rhineland-Palatinate, Hintere Bleiche 34, 55116 Mainz.

§ 9 - Safety measures

We use extensive technical and organizational measures to ensure the security of the personal data processed in the TRP / CMD app. These include in particular

- Encryption of the database: Data stored in the Supabase database is encrypted in accordance with the provider's specifications in order to prevent unauthorized access.
- Access management: The authorizations for database management are restricted to a clearly defined group of people. Every access request is logged and checked regularly.
- Encryption of connection data: Data transfers between the app and server are encrypted to protect the data stream from unauthorized access.
- Proprietary authentication: Proprietary authentication technology is used for the connection between the app and TRP components (e.. electronic circuits, ABS). If this is not successful, the connection is terminated to prevent misuse.

These measures are regularly reviewed and adapted to the current state of the art in order to maintain a high level of protection for the processed personal data.

§ 10 - Consent and revocation

Insofar as certain processing of your personal data (e.. the use of Google Analytics) is based on your consent (Art. 6 para. 1 lit. a GDPR), you have the right to withdraw this consent at any time with effect for the future. This does not affect the lawfulness of the processing carried out until the withdrawal.

If you have given your consent to the use of analysis tools as part of the initial setup of the app (opt-in) or via the app settings, you can revoke this consent at any time by opting out. We do not transmit any directly personal data (e.. plain text email addresses) as part of the analysis, and IP addresses are anonymized before they are stored.

§ 11 - Provision in the app store

The TRP / CMD app is published via a Tektro account in the common app stores (e.. Apple App Store, Google Play Store). Depending on the store provider, further data protection regulations may apply, over which we have no influence.

§ 12 Changes to the privacy policy

We reserve the right to amend this privacy policy if this becomes necessary due to legal, technical or business developments. The current version is available in the app itself. In the event of significant changes, users will be informed within the app or by other suitable means.