Data Processing Agreement
Trackboxx

By opening a customer account on Trackboxx.com, you enter into the following agreement on the processing of personal data, in addition to the agreement governing the use of Trackboxx services (Main Agreement), with

Trackboxx
Christian Pust
Dorfstr. 12
22956 Grönwohld

hereinafter referred to as the “Contractor”, “Processor” or “Trackboxx”.

This Data Processing Agreement may not be terminated separately and applies for the duration of the use of the Trackboxx services (Main Agreement).

1. General provisions

In providing the services under the Main Agreement, the Contractor processes personal data made available by the Client for the provision of those services. In respect of these data (Client Data), the Client acts as the controller within the meaning of data protection law (Article 4(7) GDPR).

On the basis of the General Data Protection Regulation (GDPR), this Agreement specifies the rights and obligations of the contracting parties in connection with the processing of Client Data for the provision of the services under the Main Agreement.

Where this Agreement uses the term “data processing” or “processing” (of data), the definition of “processing” in Article 4(2) GDPR applies.

2. Subject matter of the processing

a. The scope and duration of the processing are determined by the Main Agreement governing the Client’s use of the Trackboxx services.

b. The Contractor shall process data solely on behalf of and in accordance with the instructions of the Client, and solely in the manner, to the extent and for the purpose specified in Annex 1 to this Agreement. The processing relates exclusively to the types of personal data and categories of data subjects specified therein.

c. The duration of the processing corresponds to the term of the Main Agreement.

3. Rights and obligations of the Client

a. If the Client uses Trackboxx services in the name of or on behalf of a third party, the Client shall ensure, and shall be responsible for ensuring, that it is fully authorised to act in the name of and on behalf of that third party and that it obliges the third party, in accordance with this Agreement, to fulfil all obligations of the Client arising from the processing relationship, including in particular all obligations of the Client under this Agreement. In this case, the Client further confirms that it holds all rights, consents and authorisations that may be required for data processing in accordance with this Agreement. Any prohibitions, restrictions or consent requirements concerning the use of the Contractor’s services for third parties, as well as the consequences of any related breach of contract, remain unaffected.

b. The Client is the controller pursuant to Article 4(7) GDPR. Under Clause 4(d), the Contractor is obliged to inform the Client without undue delay if, in its opinion, the subject matter of the engagement and/or an instruction involves unlawful data processing.

c. As controller, the Client is responsible for upholding the rights of data subjects. The Contractor shall inform the Client without undue delay if data subjects exercise their rights against the Contractor in connection with this processing of data on behalf of the Client. The Client shall then take over communication with the data subject concerned, unless it has already done so.

d. The Client has the right to issue supplementary instructions to the Contractor at any time concerning the nature, scope and procedure of data processing. Instructions must be in text form (e.g. email).

e. The Client shall inform the Contractor without undue delay if it identifies errors or irregularities in connection with the Contractor’s processing of personal data.

f. Where there is an obligation to inform third parties under Article 33 GDPR, Article 34 GDPR or any other statutory notification obligation applicable to the Client, the Client is responsible for compliance with that obligation.

g. The Client shall ensure that it does not transmit, through the Trackboxx services, any data that directly identify visitors to its websites (e.g. names, email addresses, telephone numbers or postal addresses). This applies in particular to freely definable event properties and to parameters in the URLs accessed. The transmission of order numbers as part of e-commerce tracking remains unaffected.

4. General obligations of the Contractor

a. The Contractor shall process personal data exclusively within the framework of the agreements entered into (Main Agreement) and/or in compliance with any supplementary instructions issued by the Client.

b. The only exceptions are mandatory provisions of European Union or Member State law (e.g. in the event of investigations by law enforcement authorities) that may require the Contractor to process data otherwise. In such a case, the Contractor shall inform the Client of those legal requirements before processing begins, unless the relevant law prohibits such information on important grounds of public interest.

c. The contractually agreed service shall be provided exclusively in a Member State of the European Union or in a state party to the Agreement on the European Economic Area. Any relocation of the service or of any part of the work to a third country requires the Client's prior consent and may take place only if the specific requirements of Articles 44 et seq. GDPR are met in order to ensure an adequate level of protection.

d. The Contractor shall inform the Client without undue delay if, in its opinion, an instruction issued by the Client infringes statutory provisions. The Contractor is entitled to suspend implementation of the instruction concerned until it is confirmed or amended by the Client. If the Contractor can demonstrate that processing in accordance with the Client's instructions may result in liability for the Contractor under Article 82 GDPR, the Contractor may suspend further processing to that extent until liability has been clarified between the parties.

e. The Contractor has bound all persons who process Client Data to confidentiality regarding the processing of Client Data. Its own employees have been bound directly, and employees of the Contractor's subcontractors have been bound through a respective agreement with each subcontractor.

f. In accordance with Article 32 GDPR, the Processor shall take all appropriate technical and organisational measures necessary to ensure a level of security appropriate to the risk to Client Data. The IT infrastructure of a sub-processor (see Clause 5) is used to provide the services. Further information is provided in Annexes 2 and 3.

5. Engagement of sub-processors

a. The Client hereby gives general authorisation for the Contractor to engage further sub-processors. A list of the subcontractors used is attached as Annex 3. Upon conclusion of this Agreement, the Client's consent to the use of the subcontractors shall be deemed to have been given.

b. The Processor has entered into a corresponding data processing agreement with the sub-processors, contractually imposing on each service provider the same data protection obligations as those imposed on the Contractor under this Agreement.

c. The Contractor shall inform the Client in good time before any intended changes concerning the addition or replacement of sub-processors, thereby giving the controller the opportunity to object to such changes. If the Client objects on an important data protection ground and the parties cannot reach agreement, the Client is entitled to terminate the Main Agreement with effect from the time of the change. In the event of a change, the Contractor shall update the list of subcontractors and provide it to the Client without being requested to do so.

d. The Contractor shall contractually impose on each further processor the same data protection obligations as those imposed on the Contractor under this Agreement.

e. Before each engagement and regularly throughout the engagement, the Contractor shall verify that the further processors have taken appropriate technical and organisational measures and that those measures are implemented in such a way that Client Data are processed in accordance with this Agreement. The Contractor shall document the results of these checks.

6. Duties of the Contractor to cooperate

a. To the extent reasonably practicable, the Contractor shall assist the Client by technical and organisational measures in fulfilling its obligation to respond to requests by data subjects to exercise their rights.

b. In particular, the Contractor shall:

- inform the Client without undue delay if a data subject contacts the Contractor directly with a request to exercise their rights in respect of Client Data;
- upon request, provide the Client with all information available to the Contractor concerning the processing of Client Data that the Client needs to respond to a data subject's request and that the Client does not itself hold.

7. Other duties of the Contractor to provide assistance

a. The Contractor shall notify the Client of any breach of the security of Client Data, in particular incidents leading to the destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, Client Data, without undue delay after becoming aware of such a breach.

Where possible, the notification shall include a description of:

- the nature of the breach of the security of Client Data, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- the likely consequences of the breach of the security of Client Data;
- the measures taken or proposed by the Contractor to address the breach of the security of Client Data and, where appropriate, measures to mitigate its possible adverse effects.

b. Taking into account the nature of the processing and the information available to it, the Contractor shall assist the Client in ensuring compliance with the obligations set out in Articles 32 to 36 GDPR. This concerns in particular the security of processing (Article 32 GDPR), notification of personal data breaches to the supervisory authority and communication to data subjects (Articles 33 and 34 GDPR), a data protection impact assessment (Article 35 GDPR), and prior consultation with the supervisory authority (Article 36 GDPR).

8. Deletion and return of data

Following termination of the Main Agreement, Client Data shall be handled as follows, at the Client's choice:

- **Immediate deletion:** The Client may request the complete and irreversible deletion of all Client Data. Deletion shall then take place without undue delay.
- **Retention followed by deletion:** Otherwise, Client Data shall remain stored for 90 days after the end of the Agreement and shall then be automatically, completely and irreversibly deleted. Until then, the Client may retrieve its data using the export functions in the customer account (CSV, PDF).

Copies in backups shall be deleted as part of the regular backup rotation. Upon request, the Contractor shall confirm completion of deletion in text form. The obligations under this Agreement shall continue to apply until final deletion. Data shall not be deleted to the extent that Union or Member State law requires the Contractor to continue storing Client Data.

Irrespective of the above, the pseudonymous hash values referred to in Annex 1 shall be automatically deleted after no more than 24 hours.

9. Evidence and audits

a. The Contractor shall ensure and regularly verify that the processing of Client Data complies with this Agreement, including the scope of processing of Client Data specified in Annex 1, and with the Client's instructions.

b. Before processing begins and regularly during the term of the Main Agreement, the Client is entitled to verify, in an appropriate manner, the Contractor's compliance with statutory and contractual requirements, in particular the implementation of the technical and organisational measures set out in Annex 2, either itself or through a third party appointed by it. The Contractor shall allow such audits and contribute to them by all appropriate and reasonable measures, for example by:

- granting the necessary rights of access to premises, systems and data; and
- providing all necessary information.

c. The Client shall ensure that audit measures are proportionate and do not interfere with the Processor's operations more than necessary.

d. Audits shall primarily be carried out by providing suitable evidence and documentation (e.g. this Agreement and its annexes, and written information from the Contractor). Where this is insufficient in an individual case, the Contractor shall be given timely notice of on-site inspections, generally at least two weeks in advance; such inspections shall take place during normal business hours.

10. Liability and indemnification

a. The Contractor shall not be liable to the Client if the data processing giving rise to liability was carried out as a result of an instruction from the Client, pursuant to a statutory provision, or pursuant to a duty to cooperate (for example in the course of criminal prosecution). The statutory liability provisions (Article 82 GDPR) remain unaffected.

b. The Client shall reimburse the Contractor for losses and expenses arising from data protection breaches for which the Client is responsible, in particular from non-compliance with data protection requirements.

11. Final provisions

a. This Agreement becomes effective and binding on both parties upon confirmation during the opening of a customer account (conclusion of the Main Agreement). The Agreement applies for the term of the Main Agreement and may not be terminated separately. The Agreement ends upon expiry of the Main Agreement.

b. Amendments and ancillary agreements must be in text form.

c. Annexes 1 to 3 form an integral part of this Agreement.

d. If any provision of this Agreement is or becomes invalid or unenforceable after its conclusion, the validity of the remainder of the Agreement shall remain unaffected.

e. In the event of any conflict between this Agreement and the Main Agreement, the provisions of this Agreement shall prevail with regard to the processing of personal data.

Version dated 27 October 2026

Annex 1

Nature and purpose of processing, types of personal data and categories of data subjects

Purpose of processing

Audience measurement and statistical analysis of the use of the Client's websites, including the analysis of campaigns, events, conversions and e-commerce transactions.

Nature of processing

The Trackboxx services collect, process or store users' data, characteristics and activities relating to the use of the Client's websites in accordance with the Main Agreement.

Types of personal data pursuant to Article 4(1) GDPR

- IP address: used exclusively for a short period to generate pseudonymous hash values and not stored.
- Pseudonymous hash values (visitor and page identifiers): generated from the IP address, browser identifier (User-Agent), website ID, calendar date and a newly generated secret key each day; the page identifier additionally uses the hostname and path of the page accessed. Stored for a maximum of 24 hours, followed by automatic deletion. It is not possible to reverse the hash to obtain the IP address or to recognise visitors across different days.
- Browser data:
  - Browser type and version
  - Device type (desktop, tablet, mobile)
  - Referring website
- Pages accessed: URL including transmitted parameters, e.g. UTM/campaign parameters.
- Events: events configured by the Client, e.g. clicks, form submissions or downloads, including properties freely defined by the Client.
- E-commerce data: product views, shopping cart actions, cart abandonment and purchases, including order number, order value, currency and product data (name, ID, quantity, price).
- Other usage data such as country of origin, screen resolution, time of access or time zone.

Categories of data subjects

Visitors to the Client's websites and online shops in which Trackboxx services are integrated.

Annex 2

Technical and organisational measures

The Contractor has taken appropriate technical and organisational measures to protect Client Data pursuant to Article 32 GDPR. For example, the Contractor accesses Client Data only on the Client's instructions and in accordance with the authorisation framework, and such access is logged to ensure traceability.

1. Physical access control

Unauthorised access to premises must be prevented.

Technical and/or organisational measures to control physical access, in particular to verify the authorisation of persons entitled to access:

→ Keys / allocation of keys
→ Locking cabinets and offices when unattended

2. System access control

Unauthorised access to data processing systems must be prevented.

Technical (password protection) and organisational (user master records) measures for user identification and authentication:

→ Password procedures (including special characters, minimum length and regular password changes)
→ Automatic locking (e.g. password protection or locking during breaks)

3. Data access control

Unauthorised activities in data processing systems outside the permissions granted must be prevented.

Needs-based design of the authorisation framework and access rights, and their monitoring and logging:

→ Differentiated permissions (profiles, roles, transactions and objects)
→ Analysis
→ Viewing
→ Modification
→ Deletion

4. Transmission control

Personal data must not be read, copied, modified or removed without authorisation during electronic transmission.

Measures to secure data transmission:

→ Encrypted transmission of all connections (tracking script, customer account, interfaces) using HTTPS/TLS
→ Pseudonymisation of the IP address by hashing before storage (see Annex 1)

5. Input control

The traceability and documentation of data administration and maintenance must be ensured.

Measures to retrospectively verify whether and by whom data have been entered, modified or removed (deleted):

→ Logging and log analysis systems

6. Processing instruction control

Processing of data on behalf of the Client in accordance with instructions must be ensured.

Technical and organisational measures to delineate responsibilities between the Client and the Contractor:

→ Clear contractual arrangements
→ Formalised placement of orders (order form)
→ Monitoring of contract performance

7. Availability control

Data must be protected against accidental destruction or loss.

Physical and logical data backup measures:

→ Backup procedures
→ Hard disk mirroring, e.g. RAID procedures
→ Antivirus protection / firewall

8. Separation control

Data of different Clients must be processed separately.

Measures for separate processing:

→ Logical tenant separation: each data record is uniquely assigned to a website ID
→ Access through the customer account is restricted to data from the Client's own websites

The Contractor uses a sub-processor's server/IT infrastructure to store and process Client Data (see Annex 3). The sub-processor is selected with due care, particularly with regard to reliability, data security and resilience against outages.

In accordance with Article 32 GDPR, the sub-processor TK ENTERPRISES LTD assures the Contractor of a comprehensive security concept for the infrastructure it provides. This security concept is reviewed, evaluated and, where necessary, adapted by the sub-processor once a year and as circumstances require.

The Contractor reviews its own measures described in this Annex regularly and as circumstances require, and adapts them where necessary.

Annex 3

List of existing sub-processors

Company	Service	Address
TK ENTERPRISES LTD	Hosting, provision of IT/server infrastructure (data centre in Frankfurt am Main, Germany)	Tepeleniou 13 Tepelenio Court, 2nd floor 8010 Paphos Cyprus
BunnyWay d.o.o.	CDN services (delivery exclusively through locations in the EU/EEA)	Cesta komandanta Staneta 4A 1215 Medvode Slovenia