Data Processing Addendum
Trackboxx

With your registration and by creating a customer account you (hereafter: Controller) consent to the following Data Processing Addendum (DPA) presented to you by trackboxx for your acceptance:

trackboxx
Christian Pust
Dorfstr. 12
22956 Grönwohld

hereafter: "Processor"

The duration of this DPA corresponds to the duration of the Main Agreement and cannot be terminated separately.

1. General Information

To fulfill the Main Agreement, the Processor processes personal data provided by the Controller in order to render the services requested. The Controller acts as Controller in terms of data protection law (Controller Data). This Addendum specifies the data protection obligations and rights of the parties in connection with the processing of Controller Data to fulfill the Main Agreement.

The definition of the terms “data processing” or “processing” of data used in this agreement is based on Art. 4 (2), GDPR.

2. Scope and duration of the agreement

a. The scope and duration of the data processing are specified in the Main Agreement regarding the use of the trackboxx services by the Controller.

b. The processing of Controller data by the Processor comprises exclusively the type, scope and purpose determined in **Annex 1** to this Addendum. The processing relates exclusively to the types of personal data and categories of data subjects identified therein.

a. The duration of the processing corresponds to the duration of the Main Agreement.

3. Controller’s rights and obligations

a. If the Controller uses trackboxx services in the name of or on behalf of a third party, the Controller is fully responsible and shall ensure that he is authorized for acting in the name of or on behalf of the third party. Pursuant to this contract, the Controller shall commit the third party to comply with all Controller obligations under the data processing relationship including compliance with all Controller obligations under this contract. In this case the Controller further confirms that he is endued with all rights, consents and approvals that may be required for the contracted data processing. Prohibitions, restrictions and approval requirements in relation to the use of the Processor’s services for third parties remain unaffected, as do the consequences of a related breach of contract.

b. The Controller acts as Controller (Art. 4 (7) GDPR). According to Pt. 4, d. of this Addendum the Processor is entitled to inform the Controller if, in its opinion, an instruction issued by the Controller violates statutory provisions.

c. The Controller is responsible for the protection of data subjects’ rights. The Processor shall inform the Controller immediately if a data subject should contact the Processor directly with a request for claiming his or her rights in relation to Controller Data.

d. The Controller will use state-of-the-art encryption technology on his websites.

e. The Controller is entitled to issue supplemental instructions for the Processor about the type, extent and means of the data processing at any given time. Such Instructions must be documented in writing.

Instructions beyond the service as agreed-upon by the Main Agreement shall be deemed a Change Request.

f. The Controller shall inform the Processor immediately if he detects errors or irregularities in connection with the processing of personal data by the Processor.

g. The Controller is responsible to comply with any obligations to provide information to third parties in accordance with Art. 33, 34, GDPR or any other statutory reporting obligation applicable to the Controller.

4. Processor's general obligations

a. The Processor processes Controller Data exclusively on behalf of and in accordance with the Main Agreement and/or in compliance with additional instructions issued by the Controller, if necessary.

b. Excluded from this is compliance with mandatory European or Member State legislation (e.g. in the case of investigations by authorities/law enforcement) which require the Processor to oblige and change the processing.

c. The contractually agreed service is provided exclusively in a member state of the European Union or in a state party to the Agreement on the European Economic Area. Any transfer of the service or partial work to a third country requires the prior consent of the Controller and may only occur if the special conditions of Art. 44 (ff.), GDPR are fulfilled, in order to ensure an adequate data protection level.

d. The Processor will inform the Controller immediately should he deem any instruction issued by the Controller in violation with legal requirements. The Processor is entitled to suspend implementation of Controller instructions until these instructions are revised or confirmed by the Controller. The Processor is entitled to refuse execution of an evidently unlawful instruction. The Processor may suspend data processing if he can demonstrate that complying with Controller instructions may result in liability of the Processor under Art. 82, GDPR, until liability between the parties clarified.

e. The Processor has obliged all personnel engaged in the processing of Controller Data to confidentiality.

f. The Processor has taken all appropriate technical and organizational measures in accordance with Article 32, GDPR, to ensure a level of protection appropriate to the risk of Controller Data. Since the IT infrastructure of a subcontractor is used to provide services (see Pt. 5), the technical and organizational measures of the subcontractor are incorporated in this agreement (**Annex 2** and **2a**).

5. Use of subcontractors

a. The contractually agreed-upon services will be executed with the aid of subcontractors named in **Annex 3.** The Controller hereby authorizes the general use of subcontractors by the Processor. Upon conclusion of the Main Agreement, the consent of the Controller to the use of the subcontractors shall be deemed granted.

b. The Processor has a contractual agreement with the subcontractors to ensure that the agreements between Controller and Processor also apply to subcontractors. In particular, the technical and organizational measures taken by the service provider to ensure the security and integrity of the Controller data are documented in **Annex 2a**.

c. The Processor shall inform the Controller of any proposed changes in relation to the use or replacement of subcontractors. In the event of a change, the Processor will provide the Controller with an unsolicited updated list of subcontractors.

d. The Processor will contractually impose the same data protection obligations on each additional subcontractor as those set out in this Agreement with respect to the Processor.

e. The Processor will monitor prior to each assignment and regularly throughout the engagement, that appropriate technical and organizational measures have been taken by the subcontractor(s) and that these measures are executed in such a way that the processing of Controller Data is carried out in accordance with this Addendum. The results of the verifications are documented by the Processor.

6. Processor's obligations

a. The Processor shall, to a reasonable extent, assist the Controller with technical and organizational measures, to fulfill his obligation regarding the rights of data subjects.

b. In particular, the Processor shall:

- inform the Controller without undue delay if a data subject should contact the Processor directly with a request for exercising his or her rights in relation to Controller Data.
- on request, provide the Controller with all information available to him on the processing of Controller Data needed to respond to the request of a data subject and which the Controller does not have at his disposal.

7. Other support obligations of the Processor

a. The Processor shall notify the Controller without undue delay after becoming aware of any breach of Controller Data, in particular any incidents that lead to the destruction, loss, alteration or unauthorized disclosure of or access to Controller Data.

If possible, the notification shall contain a description of:

- the nature of the breach of Controller Data, indicating, as far as possible, the categories and the approximate number of affected data subjects, the categories and the approximate number of affected personal data sets.
- the likely consequences of the breach of Controller Data.
- the measures taken or proposed by the Processor to remedy the breach of Controller Data and, where appropriate, measures to mitigate their possible adverse effects.

b. In the event that the Controller is obligated to inform the supervisory authorities and/or data subjects in accordance with Art. 33, 34 of GDPR, the Processor shall, at the request of the Controller, assist the Controller to comply with these obligations.

8. Deletion and return of Controller Data

In the course of terminating the main contract, the Controller can choose whether the account should be terminated or deleted by making the appropriate entries in his customer account. In the event of termination, the data will be stored for 60 days before it is deleted. In case of deletion of the account, the controller data will be deleted immediately.

The data will be completely and irrevocably deleted, unless such deletion is prohibited by EU law or the laws of the Federal Republic of Germany.

9. Evidence and audits

a. The Processor shall ensure and regularly monitor that the processing of Controller Data is consistent with this Addendum, including the extent of the processing of Controller Data as specified in **Annex 1** and with the instructions of the Controller.

b. The Controller is entitled to appropriate auditing of the Processor by himself or through a commissioned auditor with regard to compliance with the provisions of this Addendum, in particular the implementation of the technical and organizational measures as defined in **Annex 2** prior to the start of the processing of Controller Data and regularly during the term of the Main Agreement. The Processor shall enable such audits and contribute to such audits by taking all appropriate and reasonable measures, including:

- the granting of the necessary access and access rights, and
- the provision of all necessary information.

c. The Controller shall ensure that the inspection measures are taken only to a reasonable extend and do not affect the operation of the Processor more than necessary.

10. Liability/exemption

a. The Processor shall not be liable to the Controller if the data processing causing liability was executed as a result of a Controller's instruction. The statutory liability regulations (Art. 82, GDPR) remain unaffected.

b. The Controller is obliged to reimburse the Processor for damages and expenses incurred as a result of violations of data protection laws that fall into the Controller's responsibility, in particular non-compliance with data protection requirements or the contractual implementation of the Controller's instructions.

11. Final provisions

a. This agreement becomes effective by confirmation when creating a customer account (conclusion of the Main Agreement) and shall be binding for both parties. The agreement is valid for the duration of the Main Agreement and ends upon its expiration. An isolated termination is excluded.

b. Modifications and side agreements must be rendered in writing.

c. Annexes 1 to 3 to this Agreement are integral part of the contract.

d. Should any provision of this Agreement be invalid or become partially or entirely invalid or unenforceable, the remainder of this Addendum shall remain valid and in force.

Annex 1

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

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

Type of personal data (according to Art. 4, No. 1, GDPR):

- IP address (encrypted/shortened, stored for a maximum of 24 hours)
- pseudonymized user-ID (hashed code, the code key is changed every 24 hours)
- Browser data:
    - Browser
    - Type of device (desktop, tablet, mobile)
    - Country
    - Referrer (referring website)

Categories of data subjects (according to Art. 4, No. 1, GDPR):

- Visitors to the Controller's websites in which trackboxx services are integrated.

Annex 2

Technical and organizational measures

The Processor has taken appropriate technical and organizational measures to protect Controller data to ensure an appropriate level of protection with regard to the risk for rights and freedoms of the data subjects, taking into account the state of the art, the implementation costs and the nature, the scope, circumstances and purposes of the processing of Controller Data.

These measures include:

1. Pseudonymization

The Controller Data is stored and processed in such a way that it can no longer be assigned to a specific natural person without adding additional information.

2. Confidentiality

a. Physical entry control:
The Processor ensures that unauthorized persons do not gain access to data processing equipment. This is accomplished, among other things, by measures of object protection (locked entrance doors, windows) and guidelines for accompanying guests in the building.

b. Access/Input Control:
The Processor prevents access of unauthorized users to data processing equipment/procedures and ensures that authorized users only have access to the data subject according to their access authorization by employing the measures listed below.
Retrospectively it is possible to determine if and who entered, changed or deleted Controller data:

- Use of secure passwords / regular password change
- User authorization (permissions assignment, revoke)
- Authorization concept (profile-/roll-based) with appropriate permission assignment
- Access to Controller data requires authentication (username/password)
- Logging of access (unsuccessful and successful authentication attempts)
- Logging of data entries, changes, deletions
- Obligation of the employees involved to maintain data secrecy

c. Separation control:
Data collected for different purposes is stored separately in the data processing system (separate databases/strictly segregated Controller accounts).

d. Transfer control:
Unauthorized reading, copying, alteration or deletion of Controller data during electronic transmission is prevented by the following measures:

- The electronic transmission of the data takes place exclusively via encrypted channels
- The Controller's websites are provided via an encrypted connection

3. Availability and resilience

The Processor has taken measures to ensure that Controller data is protected against accidental destruction or loss:

- Regular backups / tests of restore procedures
- System failover protection (SLA with IT service provider / processor)
- Use of anti-virus applications and firewalls

4. Regular review, assessment and evaluation

The Processor only accesses Controller data in accordance with the authorization concept and when instructed by the Controller. Access is logged to allow for tracking if and by whom personal data has been entered, changed or deleted.

The Processor employs the server/IT infrastructure of a subcontractor to store and process Controller Data. The subcontractor is selected according to strict criteria and due diligence – in particular with regard to reliability as well as data protection level and resilience. We have concluded a corresponding Data Processing Addendum which defines the rights and obligations.

The subcontractor shall provide the Processor with a comprehensive security concept in accordance with Article 32, GDPR, which contains the necessary safeguards to ensure the security of the data with regard to data protection and data security.

The Processor regularly checks compliance with the measures taken and regulations agreed.

The measures that were contractually assured by the subcontractor PHP-Friends (as of July 2020) can be found in the separate **Annex 2a** "TOM-PHP-Friends-GmbH-1.0. pdf"

The documented measures are examined, evaluated and adapted by the subcontractor once a year and on an occasional basis. The current list is provided under https://php-friends.de/tom.

For details on the currently engaged subcontractors, please see **Annex 3** to this Agreement.

Annex 3

List of currently engaged subcontractors:

Company	Service	Place of service provision	Current TOMs	Additional
PHP-Friends Ltd. Ruhrorter Straße 55a 46049 Oberhausen	Hosting Deploying the IT/Server Infrastructure	EU, EEA	https://php-friends.de/tom	Certification according to ISO 27001