This document is an English translation for convenience. The German version remains the contractual document.

Data Processing Agreement according to Art. 28 GDPR

between the client according to the main contract

and

Echometer GmbH, Hafenweg 16, 48155 Münster

as a processor (hereinafter referred to as "Contractor")

§ 1 Subject matter and term of the contract

(1) The Contractor shall provide services to the Customer on the basis of the SaaS contract for the use of Echometer ("Main Contract"). In doing so, the Contractor shall obtain access to personal data of the Customer and shall process such data exclusively on behalf of and in accordance with the instructions of the Customer. In order to specify the mutual rights and obligations under data protection law, the parties conclude the present contract. In case of doubt, the provisions of this contract shall take precedence over the provisions of the Main Contract insofar as data protection regulations are concerned.

(2) The term of this contract is based on the duration of the processing.

§ 2 Subject and duration of processing

(1) The object of the processing is the provision of a software solution with which the client initiates and controls a continuous improvement process. In the process, feedback is collected from employees and processed for the client in terms of employee, team and company development in online workshops and online result reports.

(2) The duration of the processing depends on the term of the Main Contract. Processing may continue beyond the term of the Main Contract until the return and deletion or destruction of the Client's personal data.

§ 3 Nature and purpose of processing

(1) The type of processing is the hosting, maintenance and further development of software and the personal data introduced therein by the Client or its employees, as well as support for the users of the software and any related development services.

(2) The purpose of the processing is to obtain employee feedback. This is processed for the client in the sense of employee, team and company development in online workshops and online result reports.

§ 4 Nature of personal data and categories of data subjects

(1) Types of personal data:

- Names
- E-mail addresses
- Passwords
- Feedback from employees
- Notes left by employees within the tool
- Classification of employees in team and organizational hierarchies
- Usage data (e.g. page views and clicks)
- Connection metadata (e.g. IP addresses)

(2) Categories of persons concerned:

- Employees

§ 5 Right of instruction

(1) The contractor may only process personal data on the instructions of the client; this applies in particular with regard to the transfer of personal data to a third country or to an international organization. If the Contractor is required by the law of the European Union or of the Member States to which it is subject to carry out further processing, it shall notify the Client of these legal requirements prior to the processing, unless the relevant law prohibits such notification due to an important public interest.

(2) The Client's instructions shall initially be determined by this Agreement and the Main Agreement and may thereafter be amended, supplemented or replaced by the Client in writing or in text form by individual instructions. All instructions issued shall be documented by both the Principal and the Contractor.

(3) The Customer shall be responsible for assessing the permissibility of the data processing. However, if the Contractor is of the opinion that an instruction of the Customer violates data protection provisions, it shall notify the Customer thereof without undue delay. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Customer. The Contractor may refuse to carry out an obviously illegal instruction.

§ 6 Confidentiality obligation

The Contractor shall oblige all persons entrusted by it with the processing of personal data to maintain confidentiality (Art. 28 para. 3 lit. b DS-GVO).

§ 7 Security measures

The Contractor shall take all necessary technical and organizational measures in accordance with Art. 32 DS-GVO to adequately protect the Client's personal data, in particular at least the measures of organizational control, access control, access control, transfer control, input control, order control, availability control and separation control listed in Annex 1. The Contractor reserves the right to change the security measures taken, while ensuring that the contractually agreed level of protection is not undercut. The Contractor shall inform the Customer immediately of any significant changes to the security measures.

§ 8 Subcontractor

(1) The contractually agreed services or the partial services described below shall be performed with the involvement of the subcontractors named in Annex 2. Within the scope of its contractual obligations, the Contractor shall be authorized to establish further subcontracting relationships with subcontractors. The Contractor shall inform the Client of this at least two weeks in advance. The Contractor shall be obliged to carefully select subcontractors according to their suitability and reliability. When engaging subcontractors, the Contractor shall oblige them in accordance with the provisions of this Agreement and shall ensure that the Customer can also exercise its rights under this Agreement (in particular its rights of control) directly against the subcontractors. If subcontractors in a third country are to be involved, the Contractor shall ensure that an appropriate level of data protection is guaranteed at the respective subcontractor (e.g. by concluding an agreement based on the EU standard contractual clauses).

(2) Subcontracting relationships with subcontractors within the meaning of these provisions shall not exist if the Contractor commissions third parties to provide services which are to be regarded as purely ancillary services. These include, for example, postal, transport and shipping services, cleaning services, telecommunication services without any specific reference to services provided by the Contractor to the Client and guarding services.

§ 9 Support obligations

(1) In view of the nature of the processing, the Contractor shall support the Client as far as possible with appropriate technical and organizational measures in fulfilling its obligation to respond to requests to exercise the rights of data subjects referred to in Chapter III of the GDPR.

(2) The Contractor shall support the Client in complying with its obligations under Articles 32 to 36 of the GDPR, taking into account the type of processing and the information available to the Contractor.

§ 10 Return and deletion or destruction

After termination of the Main Contract, the Contractor shall either delete or destroy all personal data at the Client's discretion or return and delete or destroy the existing copies, unless there is an obligation to retain the personal data under Union or Member State law.

§ 11 Control rights

(1) Upon request, the Contractor shall provide the Client with all information necessary to prove compliance with the Contractor's obligations under this Agreement and under Article 28 of the GDPR.

(2) For this purpose, the Contractor shall also enable and contribute to reviews - including inspections - carried out by the Customer or another inspector commissioned by the Customer. The Customer shall carry out inspections only to the extent necessary and shall not disproportionately disturb the Contractor's operations in the process.

§ 12 Update of this data processing agreement

(1) The data processing agreement, including the TOM, may be updated on an ongoing basis to reflect new circumstances.

(2) Updates to the GCU and TOM shall be shared with the Client no later than two weeks before they come into effect.

(3) During this time, the Client must object to the update in writing (e.g. via e-mail to support@echometer.de). If no such objection is made, the update shall be deemed accepted and shall enter into force.

(4) Updates to this AVV as well as the attached TOM will only be shared with the respective workspace admins stored in the Echometer app via email.

Appendix 1: Technical and organizational measures (“TOMs”) of Echometer GmbH

§ 1 General data

Responsible	Robin Roschlau, Managing Director (CIO) of Echometer GmbH
Date	01.05.2023
Survey by	Robin Roschlau, Managing Director (CIO) of Echometer GmbH
Type of survey	Initial survey x Update

§ 2 Survey

(1) Organization Control

TOM	Available?	Comment
Data privacy management (internal policies)	x	
Obligation of employees to confidentiality	x	
Obligation of the employees to the secrecy of telecommunications	x	
Obligation of external service providers to maintain data secrecy, unless they are order processors	x	
Designation of a contact person for data protection	x	Robin Roschlau, Managing Director (CIO) of Echometer GmbH

(2) Access control (data processing systems at network and server level)

TOM	Available?	Comment
(Encrypted) identification and authentication of users (user ID and password, two-step authentication with magnetic/chip card or token, biometric procedure, etc.)	x	
Password rules available	x	
Temporarily assigned passwords are immediately replaced by secure individual passwords	x	
Locking of terminal devices when leaving (screen lock with password protection automatically after timeout).	x	
Software firewall present and regularly updated	x	
Anti-virus software present and regularly updated	x	
Regular automatic application of security patches and/or updates for browsers	x	
Encryption of data carriers in mobile devices	x	
Secure deletion of data carriers before they are reused	x	
Encryption of mobile data carriers	x	

(3) Access control (data processing equipment)

TOM	Available?	Comment
Role-based permissions such as categories of roles and rights of roles, especially by "read, write, execute".	x	
Roles and rights concept with a definition and documentation of the roles and rights of the authorized persons	x	
Process for removing roles and rights that are no longer required	x	
Regular review of the necessity of the assigned roles and rights	x	

(4) Transfer control

TOM	Available?	Comment
Regular automatic/manual application of security patches and/or updates for e-mail programs	x	
Use of e-mail content filters	x	

(5) Input control

TOM	Available?	Comment
Logging of the setup/change of users and rights (documentation of all authorized	x	As far as supported by used software

users, rights profiles of authorized users, documentation of changes of users/rights, documentation of who ordered/set up the users and rights, history about the set up users and rights etc.).		
Logging of entries and changes (date and time of accesses with user identification, actions performed, especially deletions and copies, access to files with personal or confidential personal content, unauthorized and rejected access attempts, repeated entry of incorrect passwords to a login, unauthorized logins and exceeding of privileges, use of admin accounts, warnings about unauthorized intrusion, etc.).	x	As far as supported by used software

(6) Order control

TOM	**Available?**	**Comment**
Selection of the contractor under due diligence aspects (in particular with regard to data protection)	x	
Prior review of the technical and organizational measures taken by the contractor	x	
Conclusion of a contract or other legal instrument pursuant to Art. 28 GDPR and compliance with these regulations	x	
Contractually defined responsibilities	x	

(7) Availability control

TOM	Available?	Comment
Backup concept	x	
Regular automated data backups	x	
Secure transfer of data backups	x	
Regular checking of backup data for completeness and readability	x	
Recovery concept	x	
Verification of the reconstructability of the data sets through regular tests	x	
Administrator password/emergency passwords securely stored	x	
Dual control principle for sensitive administrator activities	x	
Test or development environment available	x	

(8) Separation control

TOM	Available?	Comment
Logical separation of different storing places (companies)	x	

Separation of test and production data	x	

§ 3 Conclusion

Comments	The Technical and Organizational Measures of Telekom Deutschland GmbH as hosting service provider are attached to these TOMs.
Next update	The survey of technical and organizational measures is updated annually. Accordingly, the next update will take place by 01.05.2024.

Appendix 2: Subcontractors

Telekom Deutschland GmbH provides the hosting infrastructure on which our software runs.

Telekom Germany GmbH
Landgrabenweg 151
53227 Bonn
Phone: 0228 - 181 0

Data Protection Officer:
Dr. Claus D. Ulmer,
Friedrich-Ebert-Allee 140,
53113 Bonn,
datenschutz@telekom.de

The TOMs of Telekom Deutschland GmbH can be viewed online at
https://geschaeftskunden.telekom.de/hilfe-und-service/hilfe-themen/dsgvo/otc-deutsch (German) or
https://geschaeftskunden.telekom.de/hilfe-und-service/hilfe-themen/dsgvo/otc-englisch (English).

For more information on Telekom Deutschland GmbH certifications, see:
https://open-telekom-cloud.com/en/security/data-protection-and-compliance

PostHog is a product development and analysis platform that enables new features to be rolled out sequentially as part of release management, ensures their stability and analyzes their usage. It also processes data for support and analysis purposes.

PostHog Inc
2261 Market Street #4008, San Francisco, CA 94114

Data Protection Officer:
Charles Cook (VP Operations)
privacy@posthog.com

Only PostHog's EU hosting is used. The TOMs of PostHog Inc can be viewed online at
https://docs.google.com/document/d/1xfpP1SCFoI1qSKM6rEt9VqRLRUEXiKj9_0Tvv2mP928/edit (English).

For more information on PostHog Inc certifications, see: https://posthog.com/handbook/company/security