Data Processing Agreement Pursuant to Article 28 GDPR

between

the legal entity whose registration for the use of the Processor's services has been confirmed by the Processor

– hereinafter referred to as the Controller –

and

Trace Mobility GmbH

– hereinafter referred to as the Processor –

Preamble

This Agreement governs the processing of personal data by the Processor on behalf of the Controller in accordance with Article 28 of the General Data Protection Regulation (GDPR), in connection with the Controller's use of the Processor's services as described in the Processor's Terms of Service. It is a prerequisite for the provision of such services and supplements the Terms of Service exclusively with respect to data protection matters.

This Agreement becomes legally effective upon the Controller's electronic acceptance and the Processor's confirmation of the registration request. Until such confirmation, no contractual relationship under this Agreement shall be deemed to exist.

Language Disclaimer: This English version is provided for convenience only. In the event of any conflict or legal uncertainty, the German version shall prevail and be legally binding.

Reference Basis: This Agreement is based on the model contract annex of Bitkom e.V., version 1.2.

1 Subject, Duration, and Specification of the Data Processing

1.1 The subject of this Agreement is the definition of the rights and obligations of the Parties in connection with the provision of services under the Agreement referred to above, insofar as the Processor processes personal data on behalf of the Controller in accordance with Article 28 GDPR. This includes all activities performed by the Processor in fulfillment of the Agreement that constitute commissioned (on-behalf) data processing.

1.2 The duration of the processing is determined by the actual period during which the Processor processes the Controller's personal data.

2 Scope of Application and Responsibility

2.1 The Processor shall process personal data on behalf of the Controller. This includes the activities specified in the Agreement and in the description of services. The Controller alone is responsible for compliance with the applicable data protection laws within the scope of this Agreement, in particular for the lawful transfer of personal data to the Processor and the lawfulness of the data processing itself ("Controller" within the meaning of Article 4(7) GDPR).

2.2 The instructions to the Processor are defined by the Agreement and may subsequently be amended, supplemented, or replaced by the Controller through individual instructions in written or text form (e.g., by email) to the contact point designated by the Processor.

Instructions not provided for in the Agreement shall be treated as a request for a change in the scope of services. Oral instructions must be confirmed by the Controller without undue delay in written or text form.

3 Obligations of the Processor

3.1 The Processor shall process personal data covered by this Agreement only within the scope of the Agreement and in accordance with the Controller's instructions, unless an exception pursuant to Article 28(3)(a) GDPR applies and its conditions are met.

3.2 The Processor shall immediately inform the Controller if it believes that an instruction violates applicable laws. The Processor is entitled to suspend the execution of such instruction until it has been confirmed or amended by the Controller.

3.3 The Processor shall implement appropriate technical and organizational measures to adequately protect the Controller's data in accordance with Article 32 GDPR. These measures must ensure, in particular, the confidentiality, integrity, availability, and resilience of systems and services related to the processing, in light of the risk to the rights and freedoms of data subjects.

The Processor shall document these measures before the start of processing and make them available to the Controller for review. The specific measures are set out in Annex 1.

The technical and organizational measures are subject to technological progress and development. The Processor may implement alternative, appropriate measures, provided that the security level of the measures specified in Annex 1 is not reduced. Such changes must be documented by the Processor.

3.4 The Processor shall assist the Controller, to a reasonable extent, in responding to data subjects' requests and claims under Chapter III of the GDPR and in complying with the obligations set out in Articles 33 to 36 GDPR.

3.5 The Processor shall ensure that employees and any other persons acting on its behalf who are involved in processing the Controller's data are prohibited from processing such data outside the scope of instructions. The Processor shall further ensure that such individuals are subject to a confidentiality obligation that continues beyond the termination of their engagement.

3.6 The Processor shall notify the Controller without undue delay of any personal data breach affecting the Controller's data. Such notification shall, at a minimum, include the following:

- a description of the incident, including the nature of the personal data breach, the categories and approximate number of data subjects affected, the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point for further information;
- a description of the likely consequences of the breach;
- a description of the measures taken or proposed to address the breach and, where appropriate, measures to mitigate its possible adverse effects.

3.7 The Processor shall designate a contact person for all data protection matters arising under this Agreement and inform the Controller accordingly.

3.8 The Processor shall implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing (Article 32(1)(d) GDPR).

3.9 During the term of the Agreement, the Processor shall, upon instruction by the Controller, rectify or delete the personal data covered by the Agreement. If compliant deletion is not possible, the Processor shall ensure the secure destruction of any data carriers and documents containing such data.

If deletion or restriction of processing is not feasible, the Processor shall carry out secure destruction of such materials upon separate instruction from the Controller or return the data carriers to the Controller, unless otherwise specified in the Agreement.

3.10 Upon termination of the Agreement, the Processor shall, at the Controller's request (submitted in writing or text form), return all data, data carriers, and documents owned by the Controller or securely delete them.

4 Obligations of the Controller

4.1 The Controller shall promptly and fully inform the Processor if it identifies any errors or irregularities in the results of the commissioned processing.

4.2 If the Processor is subject to claims for damages brought by a data subject pursuant to Article 82 GDPR, Section 3.4 of this Agreement shall apply accordingly.

5 Data Subject Requests

5.1 If a data subject submits a request to the Processor pursuant to Articles 15 to 21 GDPR, the Processor shall promptly refer the data subject to the Controller and forward the request to the Controller without delay.

5.2 The Processor shall assist the Controller, to the extent necessary, in fulfilling such data subject requests.

6 Proof of Compliance

6.1 The Processor shall demonstrate compliance with the obligations set forth in this Agreement using appropriate means. Upon request, the Processor shall provide the Controller with documented controls and the necessary information. In particular, the implementation of the technical and organizational measures pursuant to Article 32 GDPR must be verifiable.

6.2 Proof of compliance with the obligations under this Agreement may be provided by:

- current attestations, reports, or report extracts from independent third parties (e.g., auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors);
- self-audits;
- appropriate certifications by IT security or data protection audits (e.g., based on BSI Basic Protection, ISO 27001, ISO 27018, ISO 27701);
- adherence to approved codes of conduct pursuant to Article 40 GDPR;
- certification under an approved certification mechanism pursuant to Article 42 GDPR.

6.3 The Processor shall support the Controller, to the extent appropriate and necessary, in audits carried out pursuant to Article 28(3), sentence 2, point (h) GDPR to verify compliance with data protection laws and with the provisions of this Agreement.

6.4 Audits may be carried out by the Controller or by a third party appointed by the Controller. If the appointed third party is in a competitive relationship with the Processor, the Processor shall have the right to object. The Controller shall ensure that any third party is subject to a confidentiality obligation. The Processor may require a separate confidentiality agreement to be signed by the third party, particularly where professional or statutory confidentiality duties are concerned.

7 Subprocessors

7.1 A subprocessing relationship requiring approval exists where the Processor engages additional processors to carry out processing of personal data as set out in this Agreement. The Processor shall enter into appropriate agreements with such third parties to ensure adequate data protection and information security measures.

7.2 The Controller agrees that the Processor may engage subprocessors. Before engaging or replacing subprocessors, the Processor shall inform the Controller. The Controller may object to such changes within a reasonable period of time and only for compelling data protection reasons. If no objection is raised within the deadline, the change shall be deemed approved. If the objection is based on a legitimate data protection concern and the parties are unable to reach a mutual resolution, the Controller shall have the right to terminate this Agreement for cause.

7.3 The following subprocessors are deemed approved for the provision of cloud services and email services: (i) Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA; (ii) Snowflake Inc., 106 East Babcock Street, Bozeman, MT 59715, USA; (iii) STRATO AG, Otto-Ostrowski-Straße 7, 10249 Berlin, Germany.

7.4 If the Processor commissions subprocessors, it is the Processor's responsibility to impose the data protection obligations arising from this Agreement on such subprocessors.

8 Transfers to Third Countries

8.1 Transfers of personal data to third countries outside the EU or EEA shall only take place on the basis of documented instructions from the Controller and provided that the requirements under Articles 44 et seq. GDPR are fulfilled.

8.2 The Parties record in this Agreement the mechanisms by which an adequate level of protection is ensured for processing activities in third countries:

- For transfers to the United States of America, an adequate level of protection is ensured through the use of appropriately adapted EU Standard Contractual Clauses (SCCs), possibly including supplementary protective measures (Articles 46(2)(c) and (d) GDPR);
- For transfers to the United Kingdom of Great Britain and Northern Ireland, an adequacy decision issued by the European Commission applies (Article 45(3) GDPR).

8.3 Where no such arrangements are specified in this Agreement, data processing in a third country may only take place with the prior consent of the Controller. The Processor shall inform the Controller in advance of the third country or countries involved and the legal

mechanism used to ensure an adequate level of protection pursuant to Articles 44 et seq. GDPR.

8.4 The Processor shall provide a contact point that the Controller may communicate to data subjects as the point of contact for accessing or requesting a copy of the applicable safeguards.

9 Liability

The Controller and the Processor shall be liable to data subjects in accordance with the provisions of Article 82 GDPR.

10 Duty to Inform, Form Requirements, Governing Law

10.1 If the Controller's data held by the Processor is endangered by attachment, seizure, insolvency or composition proceedings, or by other events or measures taken by third parties, the Processor shall inform the Controller without undue delay. The Processor shall promptly notify all relevant parties that ownership and control of the data lie exclusively with the Controller as the "Controller" within the meaning of the General Data Protection Regulation.

10.2 Amendments and additions to this Annex and all of its components – including any warranties or commitments made by the Processor – must be agreed in writing, which may also be in text form (e.g., electronic format), and must expressly state that the provision is being amended or supplemented. This also applies to any waiver of this written form requirement.

10.3 In the event of any conflict, the provisions of this Annex relating to data protection shall take precedence over the Processor's General Terms and Conditions. If any part of this Annex is held to be invalid, the validity of the remainder shall remain unaffected.

10.4 This Agreement shall be governed by the laws of the Federal Republic of Germany.

Annex 1
Technical and Organizational Measures pursuant to Article 32 GDPR

1	**Confidentiality**	
1.1	Physical Access Control	• Access to office and server rooms is restricted via keys, keycards, or PIN codes • Entry permitted only to authorized individuals; visitor access is logged
1.2	System Access Control	• Use of username-password systems with complex password requirements • Two-factor authentication (2FA) for access to sensitive systems and data • Regular review and deactivation of inactive user accounts
1.3	Data Access Control	• Implementation of a role-based access concept following the need-to-know principle • Logging and monitoring of access activities • Regular review and adjustment of access rights
1.4	Data Separation Control	• Separation of customer data through multi-tenant systems or dedicated databases • Use of test data in development environments; real data avoided whenever possible
2	**Integrity**	
2.1	Data Transfer Control	• Encryption of data in transit (e.g., SSL/TLS, VPN) • Binding subprocessors to data protection obligations through data processing agreements • Logging and monitoring of data transfers
2.2	Input Control	• Logging of all changes and deletions in databases • Use of audit logs to ensure traceability of data modifications • Regular validation of data integrity
3	**Availability and Resilience**	
3.1	Availability Control	• Regular backups of all relevant data • Storage of backups in secure, geographically separate locations • Use of high-availability systems (e.g., load balancers, redundancy)
3.2	Resilience	• Regular stress testing to ensure system stability • Monitoring systems in place to oversee performance and resource usage
3.3	Disaster Recovery	• Business Continuity Plan (BCP) in place • Regular testing of system and data recovery procedures (Disaster Recovery)
4	**Restoreability**	
	• Regular creation and encryption of backups • Testing of backup restoration at least twice per year • Ensuring integrity and availability of backup data	

5	**Review, Assessment, and Evaluation Procedures**	
5.1	Data Protection Management	• Appointment of a data protection officer or responsible person • Annual data protection audits • Regular risk assessments for all data processing operations
5.2	Training	• Annual staff training on data protection and IT security • Ongoing awareness efforts regarding handling of personal data
5.3	Subprocessor Monitoring	• Regular checks of data protection compliance by subprocessors • Verification of documentation (e.g., certificates, audit reports)
6	**Pseudonymization and Encryption**	
• Encryption of sensitive data at rest using AES-256 • Use of TLS/SSL for encrypted data transmission • Pseudonymization of personal data prior to analysis, where feasible		
7	**Other Organizational Measures**	
• Maintenance of a record of processing activities (Article 30 GDPR) • Implementation of a process for reporting data breaches (Article 33 GDPR) • Regular review of the legal basis for all data processing activities		