Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

zwischen

der juristischen Person, deren Registrierung für die Nutzung der Dienste des Auftragnehmers vom Auftragnehmer bestätigt wurde

– nachfolgend Auftraggeber genannt –

und

Trace Mobility GmbH

– nachfolgend Auftragnehmer genannt –

Präambel

Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers gemäß Art. 28 DSGVO im Rahmen der Nutzung der Leistungen des Auftragnehmers gemäß dessen Allgemeinen Geschäftsbedingungen (AGB). Sie ist Voraussetzung für die Leistungserbringung und ergänzt die AGB ausschließlich in datenschutzrechtlicher Hinsicht.

Dieser Vertrag wird elektronisch geschlossen und wird rechtswirksam mit der elektronischen Zustimmung des Auftraggebers sowie der Bestätigung der Registrierungsanfrage durch den Auftragnehmer. Bis zur Bestätigung durch den Auftragnehmer gilt kein Vertragsverhältnis im Sinne dieses Vertrags als zustande gekommen.

Vertragsgrundlage: Dieser Vertrag basiert auf der Mustervertragsanlage des Bitkom e.V., Version 1.2 (2023).

1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß dem oben genannten Vertrag, soweit eine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber als Verantwortlicher gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen.

1.2 Die Dauer der Verarbeitung richtet sich nach der tatsächlichen Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer.

2 Anwendungsbereich und Verantwortlichkeit

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO)

2.2 Die Weisungen werden durch den Vertrag festgelegt und können vom Auftraggeber danach schriftlich oder in Textform (z.B. E-Mail) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die

im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform vom Auftraggeber zu bestätigen.

3 Pflichten des Auftragnehmers

3.1 Der Auftragnehmer darf personenbezogene Daten, die Gegenstand des Auftrags sind, nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor und dessen Voraussetzungen werden gewahrt.

3.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.3 Der Auftragnehmer wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat insbesondere technische und organisatorische Maßnahmen zu treffen, gemessen am Risiko für die Rechte und Freiheiten der betroffenen Personen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer gewährleisten.

Der Auftragnehmer hat die erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung zu dokumentieren und dem Auftraggeber zur Prüfung bereitzustellen. Die Einzelheiten dieser technischen und organisatorischen Maßnahmen ergeben sich aus **Anlage 1**.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Diese sind vom Auftragnehmer entsprechend zu dokumentieren. Dabei darf das Sicherheitsniveau der in **Anlage 1** genannten Maßnahmen nicht unterschritten werden.

3.4 Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Artt. 33 bis 36 DSGVO genannten Pflichten.

3.5 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die mit der Verarbeitung der personenbezogenen Daten zuständigen Personen zur Vertraulichkeit verpflichtet haben und diese Vertraulichkeitsverpflichtung auch nach Beendigung des Auftrags fortbesteht.

3.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Eine Meldung von Datenschutzverletzungen muss mindestens enthalten:

- eine Beschreibung des Vorfalls, soweit möglich mit Angabe der Art der Verletzung des Schutzes personenbezogener Daten, Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen des gemeldeten Vorfalls, eine Beschreibung der ergriffenen Maßnahmen zur Behebung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

3.7 Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

3.8 Der Auftragnehmer gewährleistet, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen (Art. 32 Abs. 1 lit. d DSGVO).

3.9 Während der Vertragslaufzeit berichtigt oder löscht der Auftragnehmer auf Weisung des Auftraggebers die vertragsgegenständlichen Daten. Sofern eine datenschutzkonforme Löschung dieser Daten nicht möglich ist, stellt der Auftragnehmer eine datenschutzkonforme Vernichtung der Datenträger und Unterlagen, die vertragsgegenständliche Daten enthalten, sicher.

Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

3.10 Daten, Datenträger sowie sämtliche Dokumente sind nach Auftragsende auf Verlangen (schriftlich oder in Textform) des Auftraggebers entweder herauszugeben, sofern sie im Eigentum des Auftraggebers sind, oder zu löschen.

4 Pflichten des Auftraggebers

4.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten feststellt.

4.2 Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO, gilt Abs. 3.4 entsprechend.

5 Anfragen betroffener Personen

5.1 Wendet sich eine betroffene Person mit Anträgen gemäß Art. 15 bis 21 DSGVO an den Auftragnehmer, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen und leitet den Antrag an den Auftraggeber weiter.

5.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung dieser Anträge der betroffenen Personen im erforderlichen Umfang.

6 Nachweismöglichkeiten

6.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die dokumentierten Kontrollen und erforderlichen

Auskünfte zur Verfügung zu stellen. Insbesondere ist die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art 32 DSGVO nachzuweisen.

6.2 Der Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten kann erfolgen durch

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT- Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- Selbstaudits;
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001, ISO 27018, ISO 27701);
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO.

6.3 Der Auftragnehmer verpflichtet sich, den Auftraggeber bei seinen Prüfungen gemäß Art. 28 Abs. 3 Satz 2 lit. h DSGVO zur Einhaltung der Vorschriften zum Datenschutz sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang zu unterstützen.

6.4 Die Prüfungen werden durch den Auftraggeber selbst oder einen von ihm beauftragten Dritten durchgeführt. Sollte der durch den Auftraggeber beauftragte Dritter in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Beauftragte Dritte müssen durch den Auftraggeber zur Verschwiegenheit verpflichtet werden. Dem Auftragnehmer steht das Recht zu, die Abgabe einer separaten Verschwiegenheitserklärung des beauftragten Dritten zu verlangen. Dies gilt insbesondere für die Abgabe von Erklärungen zur berufsrechtlichen oder gesetzlichen Verschwiegenheit.

7 Weitere Auftragsverarbeiter (Subunternehmer)

7.1 Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit im Vertrag vereinbarten Verarbeitung personenbezogener Daten beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

7.2 Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem datenschutzrechtlichem Grund – gegenüber dem Auftragnehmer widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

7.3 Die folgenden Subunternehmer gelten für Cloud-Services und E-Mail-Dienste als genehmigt: (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.

7.4 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

8 Übermittlung in Drittstaaten

8.1 Eine Übermittlung findet nur auf dokumentierte Weisung des Verantwortlichen in Drittstaaten außerhalb der EU und des EWR statt, sofern die Voraussetzungen nach Art. 44ff DSGVO eingehalten werden.

8.2 Die Vertragsparteien halten in diesem Vertrag fest, auf welche Art und Weise das angemessene Schutzniveau für die Verarbeitung im Drittstaat sichergestellt ist:

- Das angemessene Schutzniveau in den Vereinigten Staaten von Amerika (USA) wird eingehalten durch entsprechend modulierte EU-Standarddatenschutzklauseln ggf. inklusive zusätzlicher Schutzmaßnahmen (Art. 46 Abs. 2 litt. c und d DSGVO).
- Das angemessene Schutzniveau im Vereinigten Königreich Großbritannien und Nordirland wird eingehalten durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO)

8.3 Ist hierzu nichts im Vertrag vereinbart, ist die Verarbeitung in einem Drittstaat nur mit vorheriger Zustimmung des Auftraggebers zulässig. Der Auftragnehmer teilt dem Auftraggeber vorab mit, um welche(n) Drittstaat(en) es sich handelt und auf welche Weise das angemessene Schutzniveau im Sinne von Art. 44 ff DSGVO für die Verarbeitung dort sichergestellt ist.

8.4 Der Auftragnehmer stellt einen Kontakt zur Verfügung, den der Auftraggeber Betroffenen als Stelle mitteilen kann, bei dem die Garantien verfügbar sind bzw. eine Kopie der Garantie angefordert werden kann.

9 Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

10 Informationspflichten, Schriftformklausel, Rechtswahl

10.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

10.2 Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

10.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen der Allgemeinen Geschäftsbedingungen (AGB) des Auftragnehmers vor. Sollten

einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

10.4 Es gilt deutsches Recht.

Anlage 1
Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

1	**Vertraulichkeit**	
1.1	Zutrittskontrolle	• Zugangsregelung zu Büro- und Serverräumen durch Schlüssel(karten) oder PIN-Codes • Zutritt nur für autorisierte Personen, Protokollierung von Besuchern
1.2	Zugangskontrolle	• Einsatz von Benutzername-Passwort-Systemen mit komplexen Passwortanforderungen • Zwei-Faktor-Authentifizierung (2FA) für Zugriff auf sensible Systeme und Daten • Regelmäßige Überprüfung und Deaktivierung inaktiver Benutzerkonten
1.3	Zugriffskontrolle	• Implementierung eines Rollenkonzepts mit Zugriffsrechten nach dem Need-to-Know-Prinzip • Protokollierung und Überwachung der Zugriffsvorgänge • Regelmäßige Überprüfung und Anpassung von Zugriffsberechtigungen
1.4	Trennungskontrolle	• Trennung von Daten verschiedener Kunden durch mandantenfähige Systeme oder separate Datenbanken • Nutzung von Testdaten in Entwicklungsumgebungen, idealerweise keine Verwendung von Echtdaten
2	**Integrität**	
2.1	Weitergabekontrolle	• Verschlüsselung von Daten bei der Übertragung (SSL/TLS, VPN) • Verpflichtung von Subdienstleistern zur Einhaltung der Datenschutzvorgaben durch Auftragsverarbeitungsverträge • Protokollierung und Überwachung von Datenübertragungen
2.2	Eingabekontrolle	• Protokollierung aller Änderungen und Löschungen in Datenbanken • Implementierung von Audit-Logs zur Nachvollziehbarkeit von Veränderungen • Regelmäßige Überprüfung der Integrität der Daten
3	**Verfügbarkeit und Belastbarkeit**	
3.1	Verfügbarkeitskontrolle	• Regelmäßige Sicherung (Backups) aller relevanten Daten • Speicherung von Backups an einem sicheren, geographisch getrennten Standort • Einsatz hochverfügbarer Systeme (Load Balancer, Redundanz)
3.2	Belastbarkeit	• Regelmäßige Stresstests zur Sicherstellung der Systemstabilität • Monitoring-Systeme zur Überwachung von Systemressourcen und Performance
3.3	Katastrophenmanagement	• Erstellung eines Business Continuity Plans (BCP) • Regelmäßige Tests zur Wiederherstellung von Systemen und Daten im Notfall (Disaster Recovery)

4	**Wiederherstellbarkeit**	
• Regelmäßige Erstellung und Verschlüsselung von Backups • Test der Wiederherstellung von Backups mindestens halbjährlich • Sicherstellung der Integrität und Verfügbarkeit von Backup-Daten		
5	**Verfahren zur Überprüfung, Bewertung und Evaluierung**	
5.1	Datenschutzmanagement	• Benennung eines Datenschutzverantwortlichen • Durchführung von jährlichen Datenschutz-Audits • Regelmäßige Risikoanalyse für alle Verarbeitungsprozesse
5.2	Schulungen	• Jährliche Schulungen für Mitarbeiter zu Datenschutz und IT-Sicherheit • Sensibilisierung für den Umgang mit personenbezogenen Daten
5.3	Überprüfung von Subdienstleistern	• Kontrolle der Einhaltung von Datenschutzstandards durch eingesetzte Subdienstleister • Sicherstellung der Dokumentation (z. B. Zertifikate, Auditberichte)
6	**Pseudonymisierung und Verschlüsselung**	
• Verschlüsselung sensibler Daten mit AES-256-Standard im Ruhezustand • Nutzung von TLS/SSL zur Verschlüsselung von Daten bei der Übertragung • Pseudonymisierung von personenbezogenen Daten vor der Analyse, soweit möglich		
7	**Weitere organisatorische Maßnahmen**	
• Erstellung und Pflege eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO) • Implementierung eines Prozesses zur Meldung von Datenschutzverletzungen (Art. 33 DSGVO) • Regelmäßige Überprüfung der Rechtsgrundlagen für alle Verarbeitungen		