Vereinbarung zwischen [Unternehmensname und Adresse] („**Auftraggeber**“) und der Visitor Analytics GmbH, Seestraße 76, 82335 Berg „**Auftragnehmer**“ oder „**TWIPLA**“; gemeinsam die „**Parteien**“ oder jeweils eine „**Partei**“) über die Verarbeitung von personenbezogenen Daten im Auftrag („**AVV**“). Die Begriffe „personenbezogene Daten“, „verarbeiten“, „betroffene Person“, „Verantwortlicher“ und „Auftragsverarbeiter“ sind in Art. 4 der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 („**DSGVO**“) definiert.

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand des Auftrags

Der Gegenstand des Auftrags der Datenverarbeitung durch den Auftragnehmer ergibt sich aus dem Twipla-Servicevertrag zwischen den Parteien („**Hauptvertrag**“). Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber. Der Auftraggeber ist dabei als Verantwortlicher für die Verarbeitung personenbezogener Daten, für die Beurteilung der gesetzlichen Zulässigkeit der Verarbeitung personenbezogener Daten sowie für die Wahrung der Rechte betroffener Personen verantwortlich.

1.2. Dauer des Auftrags

Diese AVV wird zwischen den Parteien für die Dauer vereinbart, während der der Auftragnehmer für den Auftraggeber personenbezogene Daten auf Basis des Hauptvertrags verarbeitet.

2. Konkretisierung des Auftragsinhalts

2.1. Umfang, Art und Zweck

Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind im Hauptvertrag konkret beschrieben.

2.2. Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / -kategorien („**Auftraggeberdaten**“)

- Daten über die Verbindung eines Besuchers mit der Kundenwebseite (z.B. Zeitstempel, Anzahl der aufgerufenen Seiten, IP-Adresse - wenn die IP-Anonymisierung nicht aktiviert ist); Informationen über das Gerät des Besuchers (z.B. Mobiltelefon, oder Computer, Betriebssystem und Version, Browser, Bildschirmgröße); ungefähre Geolokalisierungsdaten, die vom Standort der IP-Adresse des Besuchers abgeleitet werden, weitere Nutzungsdaten.
- Zusätzlich werden die Technologien von TWIPLA eingesetzt, um die Services bereitzustellen, wenn und soweit der Kunde dies wünscht:

Cookie und Name	Zweck	Gesammelte Daten	Nutzungsdauer	Kategorie
*_ignore_Visits_UniqueHash	Die TWIPLA-App platziert diesen Cookie auf Wunsch des Auftraggebersfür eine bestimmte Webseite, um das Tracking der TWIPLA-Webseitenanalyse für diese bestimmte Webseite zu deaktivieren.	Besuche ignorieren	365 Tage	Unbedingt erforderlich
*_ignoreVisits_all	Die TWIPLA-App platziert dieses Cookie auf Wunsch des Auftraggebers, um die Webseiten-Tracking-Analyse für alle Webseiten, die TWIPLA verwenden, zu deaktivieren.	Besuche ignorieren	365 Tage	Unbedingt erforderlich

2.3. Kreis der Betroffenen

Der Kreis der durch die Verarbeitung personenbezogener Daten im Rahmen dieses Auftrags betroffenen Personen umfasst:

- Nutzer der Website oder anderer digitaler Angebote des Auftraggebers.

3. Weisungsbefugnis des Auftraggebers / Ort der Datenverarbeitung

3.1. Die Verarbeitung der Auftraggeberdaten erfolgt ausschließlich nach dokumentierten Weisungen des Auftraggebers. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (inTextform) bestätigen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Entstehende Zusatzaufwände sind vom Auftraggeber auf Time- und Material-Basis zu vergüten.

3.2. Der Auftragnehmer verarbeitet Auftraggeberdaten nur außerhalb der Weisungen des Auftraggebers, soweit er aufgrund von anwendbarem Recht dazu verpflichtet ist. In einem solchen Fall informiert der Auftragnehmer den Auftraggeber über diesen Umstand vorab, sofern das jeweilige Gesetz dies nicht verbietet.

3.3. Der Auftragnehmer informiert den Auftraggeber, wenn er der Meinung ist, eine Weisung verstoße gegen einschlägige datenschutzrechtliche Vorschriften. Der

Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

3.4. Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer findet innerhalb der EU / des EWR statt. Eine Verlagerung der Verarbeitung in Länder außerhalb der EU / des EWR durch den Auftragnehmer findet nur nach Rücksprache mit dem Auftraggeber statt.

4. Vertraulichkeit

Die zur Verarbeitung der Auftraggeberdaten befugten Personen haben sich zu Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht.

5. Technisch-organisatorische Maßnahmen

5.1. Der Auftragnehmer trifft technische und organisatorische Maßnahmen zum Schutz der Auftraggeberdaten, die den Anforderungen des Art. 32 DSGVO genügen. Diese technischen und organisatorischen Maßnahmen sind in Anhang 1 dieser AVV beschrieben. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

5.2. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6. Unterauftragsverhältnisse

6.1. Der Auftraggeber stimmt dem Einsatz von Unterauftragnehmern durch den Auftragnehmer zu:

6.1.1. Der Auftraggeber stimmt dem Einsatz der in Anhang 2 dieser AVV aufgeführten Unterauftragnehmer sowie den in der EU ansässigen verbundenen Unternehmen des Auftragnehmers bei Abschluss dieser AVV zu.

6.1.2. Der Auftraggeber stimmt dem Einsatz weiterer bzw. der Änderung bestehender Unterauftragnehmer zu, wenn der Auftragnehmer den Einsatz bzw. die Änderung vierzehn (14) Tage vor Beginn der Datenverarbeitung schriftlich (E-Mail ausreichend) dem Auftraggeber mitteilt. Der Auftraggeber kann dem Einsatz eines neuen Unterauftragnehmers bzw. der Änderung aus wichtigen datenschutzrechtlichen Gründen innerhalb von zehn (10) Tagen widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zum Einsatz oder zur Änderung als gegeben. Der Auftraggeber nimmt zur Kenntnis, dass in bestimmten Fällen die Leistung ohne den Einsatz eines bestimmten Unterauftragnehmers nicht mehr erbracht werden kann. Liegt ein wichtiger datenschutzrechtlicher Grund für den Widerspruch vor und ist eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich, haben die Parteien jeweils ein Sonderkündigungsrecht in Bezug auf die den abgelehnten Unterauftragnehmer betreffende Leistung des Auftragnehmers.

6.2. Der Auftragnehmer schließt mit dem / den Unterauftragnehmer / n unter Berücksichtigung der Art und des Umfangs der Datenverarbeitung im Rahmen des Unterauftrags schriftliche (dies schließt die elektronische Form ein) Auftragsverarbeitungsvereinbarungen, die inhaltlich dieser AVV entsprechen.

7. Betroffenenrechte

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen nach Kapitel III der DSGVO.

8. Mitwirkungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen.

9. Informations- und Überprüfungsrecht des Auftraggebers

9.1. Der Auftraggeber hat das Recht, erforderliche Informationen zum Nachweis der Einhaltung der vereinbarten Pflichten des Auftragnehmers anzufordern und Überprüfungen im Einvernehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen.

9.2. Die Parteien vereinbaren, dass der Auftragnehmer zum Nachweis der Einhaltung seiner Pflichten und Umsetzung der technischen und organisatorischen Maßnahmen berechtigt ist, dem Auftraggeber aussagekräftige Dokumentationen vorzulegen. Eine aussagekräftige Dokumentation kann durch die Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter), einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001) oder einer durch die zuständigen Aufsichtsbehörden genehmigten Zertifizierung erbracht werden.

9.3. Das Recht des Auftraggebers Vor-Ort-Kontrollen durchzuführen, wird hierdurch nicht beeinträchtigt. Der Auftraggeber wird jedoch abwägen, ob nach Vorlage von aussagekräftiger Dokumentation eine Vor-Ort-Kontrolle noch erforderlich ist, insbesondere unter Berücksichtigung der Aufrechterhaltung des ordnungsgemäßen Betriebs des Auftragnehmers. Der Auftraggeber wird nur in Absprache mit dem Auftragnehmer Vor-Ort-Kontrollen durchführen.

10. Löschung von Daten und Rückgabe von Datenträgern

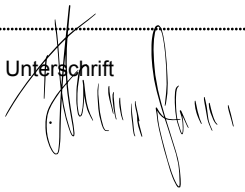
Nach Wahl und Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Auftragsverarbeitung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen oder zu deren Aufbewahrung der Auftragnehmer gesetzlich verpflichtet ist, dürfen durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden.

11. Haftung; Rechtswahl; Gerichtsstand

Für die Haftung des Auftragnehmers im Zusammenhang mit dieser AVV sowie für die Wahl des auf diese AVV anwendbares Recht und Gerichtsstand gelten die im Hauptvertrag getroffenen Vereinbarungen.

Unterschriften

Für und im Namen des Auftraggebers:	**Für und im Namen des Auftragnehmers:**
	Visitor Analytics GmbH
.....	.....
Datum	Datum
.....	.....
Name / Position	Name / Position Tim Hammermann (CEO)
.....	.....
Unterschrift	Unterschrift 

Anlage 1: Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, die von TWIPLA ergriffen werden.

TWIPLA hat die folgenden technischen und organisatorischen Sicherheitsmaßnahmen ergriffen, um die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste zu gewährleisten:

1. Vertraulichkeit

TWIPLA hat die folgenden technischen und organisatorischen Sicherheitsvorkehrungen getroffen, um insbesondere die Vertraulichkeit der Verarbeitungssysteme und -dienste zu gewährleisten, im Einzelnen:

1.1. TWIPLA verarbeitet alle Personenbezogenen Nutzungsdaten auf Servern innerhalb der Bundesrepublik Deutschland, die sich im Besitz von branchenführenden Cloud-Service-Anbietern befinden und von diesen betrieben werden, die hoch entwickelte Maßnahmen zum Schutz vor dem Zugriff Unbefugter auf Datenverarbeitungsgeräte (nämlich Telefone, Datenbank- und Anwendungsserver und die zugehörige Hardware) anbieten. Solche Maßnahmen umfassen:

1.1.1. Rechenzentren werden rund um die Uhr von hochauflösenden Innen- und Außenkameras überwacht, die Eindringlinge erkennen und verfolgen können;

1.1.2. Zugangsprotokolle, Aktivitätsaufzeichnungen und Kameraaufnahmen sind für den Fall eines Vorfalls verfügbar;

1.1.3. Rechenzentren werden außerdem routinemäßig von erfahrenen Sicherheitsbeamten patrouilliert, die sich strengen Hintergrundprüfungen und Schulungen unterzogen haben;

1.1.4. Dokumentierte Verteilung von Schlüsseln an Mitarbeiter und Colocation-Kunden für Coocation-Racks;

1.1.5. Nur autorisierte Mitarbeiter mit bestimmten Rollen dürfen auf die Server zugreifen.

1.2. TWIPLA setzt geeignete Maßnahmen ein, um zu verhindern, dass seine Datenverarbeitungssysteme von Unbefugten benutzt werden. Dies wird erreicht durch:

1.2.1. Automatische Erkennung von wiederholtem oder massenhaftem unberechtigtem Zugriff; Zulassung des Zugriffs auf die TWIPLA App ausschließlich auf der Grundlage eines verschlüsselten Schlüssels, der nur von TWIPLA mit Hilfe eines Geheimnisses entschlüsselt werden kann;

1.2.2. SSL-Verschlüsselung auf allen öffentlichen Kunden-Endpunkten

1.2.3. Alle Zugriffe auf Dateninhalte werden protokolliert, überwacht und nachverfolgt.

1.3. Mitarbeiter von TWIPLA, die zur Nutzung der Datenverarbeitungssysteme von TWIPLA berechtigt sind, können nur im Rahmen und im Umfang ihrer jeweiligen Zugriffsberechtigung (Berechtigung) auf Personenbezogene Daten zugreifen. Insbesondere basieren die Zugriffsrechte und -ebenen auf der Funktion und der Rolle der Mitarbeiter, wobei die Konzepte der geringsten Privilegien und des Wissensbedarfsverwendet werden, um die Zugriffsrechte an definierten Verantwortlichkeiten anzupassen. Dies wird erreicht durch:

1.3.1. Mitarbeiterrichtlinien und -schulungen;

1.3.2. Wirksame und maßvolle Disziplinarmaßnahmen gegen Personen, die unbefugt auf Personenbezogene Daten zugreifen;

1.3.3. Beschränkter Zugriff auf Personenbezogene Daten nur für autorisierte Personen;

1.3.4. Verschlüsselung nach Industriestandard; und

1.3.5. Richtlinien zur Kontrolle der Aufbewahrung von Sicherungskopien.

2. Integrität

TWIPLA hat die folgenden technischen und organisatorischen Sicherheitsvorkehrungen getroffen, um insbesondere die Integrität der Verarbeitungssysteme und -dienste zu gewährleisten:

2.1. TWIPLA trifft geeignete Maßnahmen, um zu verhindern, dass Personendaten bei der Übermittlung, oder beim Transport der Datenträger von Unbefugten gelesen, kopiert, verändert, oder gelöscht werden können. Dies wird erreicht durch:

2.1.1. Einsatz modernster Firewall- und Verschlüsselungstechnologien zum Schutz der Gateways und Pipelines, durch die die Daten transportiert werden;

2.1.2. Verschlüsselung nach Industriestandard; und

2.1.3. Vermeidung der Speicherung Personenbezogener Daten auf tragbaren Speichermedien für Transportzwecke und auf firmeneigenen Laptops, oder anderen mobilen Geräten.

2.2. TWIPLA greift nicht auf Kundeninhalte zu, es sei denn, dies ist notwendig, um dem Kunden die vom Kunden ausgewählten TWIPLA Services zur Verfügung zu stellen, oder um Systemfehler zu beheben. TWIPLA greift für keine anderen Zwecke auf die Inhalte des Kunden zu. Dementsprechend weiß TWIPLA nicht, welche Inhalte der Kunde zum Speichern auf seinen Systemen auswählt, und kann nicht zwischen Personenbezogenen Daten und anderen Inhalten unterscheiden, so dass TWIPLA alle Kundeninhalte gleich behandelt. Auf diese Weise profitieren alle Kundeninhalte von den gleichen robusten Sicherheitsmaßnahmen von TWIPLA, unabhängig davon, ob diese Inhalte Personenbezogenen Daten enthalten, oder nicht.

3. Verfügbarkeit

TWIPLA hat insbesondere die folgende technische und organisatorische Sicherheitsmaßnahmen umgesetzt, um die Verfügbarkeit von Verarbeitungssystemen und -diensten zu gewährleisten:

3.1. TWIPLA führt geeignete Maßnahmen durch, um sicherzustellen, dass personenbezogene Daten vor unbeabsichtigter Zerstörung, oder Verlust geschützt sind. Dies wird erreicht durch:

3.1.1. Redundanz der Infrastruktur;

3.1.2. Richtlinien, die eine permanente lokale (Arbeitsplatz-)Speicherung von Personenbezogenen Daten verbieten; und

3.1.3. Durchführung regelmäßige Datensicherungen.

4. Belastbarkeit

Visitors Analytics verwendet einen Webserver mit Thread-Pooling für eine bessere Leistung, um sicherzustellen, dass wir eine große Anzahl von Verbindungen unterstützen können. Der größte Teil unseres Projekts basiert auf einem Produzenten/Konsumenten-Muster, um sicherzustellen, dass die Verbindungen so schnell wie möglich geschlossen werden, damit Ressourcen für anstehende Verbindungen verfügbar sind. Außerdem werden unsere Datenbanken gesichert, um sicherzustellen, dass wir im Falle unvorhergesehener Umstände auf eine ältere Version zurückgreifen können.

Auch die Einrichtungsprozesse der Server sind automatisiert (und mit Ausnahme der Datenbanken zustandsfrei), um sicherzustellen, dass wir einen neuen Server neu erstellen und starten können, falls mit der alten Instanz etwas passiert.

Anlage 2 – Subunternehmer

Name des Unterauftrag nehmers	**Adresse**	**Funktion/durchgeführte Verarbeitungsschritte**	**Welche Daten werden an den Unterauftrag nehmer weitergeleitet?**
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Germany	Web-Hosting-Anbieter	Alle im Auftrag des Kunden verarbeiteten Daten der Webseitenbesucher werden in einer bei Hetzner gehosteten Datenbank gespeichert.
ALL-INKL.COM - Neue Medien Münnich	Hauptstraße 68, 02742 Friedersdorf, Germany	E-Mail-Anbieter	Vorname, Nachname und E-Mail-Adressen für den Versand von Statusberichten und Newslettern