Agreement between [company name and address] ("**Client**") and Visitor Analytics GmbH, Seestraße 76, 82335 Berg "**Contractor**" or "**TWIPLA**"; collectively the "**Parties**" or each a "**Party**") on the processing of personal data on behalf ("**DPA**"). The terms "personal data", "process", "data subject", "controller" and "processor" are defined in Art. 4 of the General Data Protection Regulation (Regulation (EU) 2016/679 ("**GDPR**")).

1. Object and duration of the order

1.1. Object of the order

The object of the order for data processing by the Contractor is set out in the Twipla Service Agreement between the Parties ("**Main Agreement**"). The Contractor processes personal data for the Client. The Client is responsible for the processing of personal data, for assessing the legal admissibility of the processing of personal data and for safeguarding the rights of data subjects.

1.2. Duration of the order

This DPA is agreed between the parties for the duration during which the Contractor processes personal data for the Client on the basis of the main contract.

2. Specification of the order content

2.1. Scope, nature and purpose

The scope, nature and purpose of the processing of personal data by the contractor for the client are specifically described in the main contract.

2.2. Type of data

The following types/categories of data ("**client data**") are subject to the processing of personal data

- Data about a visitor's connection to the customer website (e.g., timestamp, number of pages viewed, IP address - if IP anonymization is not activated); information about the visitor's device (e.g. cell phone, or computer, operating system and version, browser, screen size); approximate geolocation data derived from the location of the visitor's IP address, other usage data.
- In addition, TWIPLA's technologies are used to provide the services if and insofar as the customer so wishes:

Cookie and name	Purpose	Collected data	Useful life	Category
*_ignore_Visits_UniqueHash	The TWIPLA app places this cookie at the request of the client for a specific website in order to deactivate the tracking of the TWIPLA website analysis for this specific website.	Ignore visits	365 days	Absolutely necessary
*_ignoreVisits_all	The TWIPLA app places this cookie at the request of the client in order to deactivate website tracking analysis for all websites that use TWIPLA.	Ignore visits	365 days	Absolutely necessary

2.3. Circle of data subjects

The group of data subjects affected by the processing of personal data within the scope of this contract includes

- Users of the website or other digital offerings of the client.

3. Authority of the client / place of data processing

3.1. The client data shall be processed exclusively in accordance with documented instructions from the client. The client shall confirm verbal instructions immediately in writing or by e-mail (in text form). Changes to the object of processing and procedural changes must be jointly agreed and documented. Any additional expenses incurred shall be remunerated by the client on a time and material basis.

3.2. The Contractor shall only process Client Data outside the instructions of the Client insofar as it is obliged to do so under applicable law. In such a case, the Contractor shall inform the Client of this circumstance in advance, unless the relevant law prohibits this.

3.3. The Contractor shall inform the Client if it is of the opinion that an instruction violates relevant data protection regulations. The contractor is entitled to suspend the implementation of the corresponding instruction until it is confirmed or amended by the controller at the client.

3.4. The processing of the client data by the contractor takes place within the EU/EEA. Any transfer of processing to

countries outside the EU/EEA by the Contractor shall only take place after consultation with the Client.

4. Confidentiality

The persons authorized to process the client data have undertaken to maintain confidentiality or are subject to a statutory duty of confidentiality.

5. Technical and organizational measures

5.1. The Contractor shall take technical and organizational measures to protect the Client Data that meet the requirements of Art. 32 GDPR. These technical and organizational measures are described in Annex 1 of this DPA. The client is aware of these technical and organizational measures and is responsible for ensuring that they offer an appropriate level of protection for the risks of the data to be processed.

5.2. The technical and organizational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes must be documented.

6. Subcontracting relationships

6.1. The Client agrees to the use of sub-processors by the Contractor:

6.1.1. The Client agrees to the use of the sub-processors listed in Annex 2 of this DPA and the Contractor's affiliated companies based in the EU upon conclusion of this DPA.

6.1.2. The Client agrees to the use of additional sub-processors or the modification of existing sub-processors if the Contractor notifies the Client of the use or modification in writing (e-mail is sufficient) fourteen (14) days before the start of data processing.
The client may object to the use of a new sub-processor or the change for important data protection reasons within ten (10) days. If no objection is made within this period, consent to the assignment or change shall be deemed to have been given. The client acknowledges that in certain cases the service can no longer be provided without the use of a specific sub-processor. If there is an important data protection reason for the objection and if it is not possible for the parties to reach an amicable solution, the parties shall each have a special right of termination in relation to the service of the Contractor concerning the rejected sub-processor.

6.2. The Contractor shall conclude written (including electronic form) data processing agreements with the sub-processor(s), taking into account the type and scope of the data processing within the scope of the subcontract, which correspond to the content of this DPA.

7. Rights of data subjects

The Contractor shall support the Client within the scope of its possibilities in fulfilling the requests and claims of data subjects in accordance with Chapter III of the GDPR.

8. Obligations of the contractor to cooperate

The Contractor shall support the Client in complying with the obligations set out in Art. 32 to 36 GDPR regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations.

9. Information and inspection rights of the client

9.1. The Client has the right to request the necessary information to prove that the Contractor is complying with the agreed obligations and to carry out inspections in agreement with the Contractor or to have them carried out by inspectors to be named in individual cases.

9.2. The parties agree that the Contractor shall be entitled to submit meaningful documentation to the Client as proof of compliance with its obligations and implementation of the technical and organizational measures. Meaningful documentation can be provided by submitting a current certificate, reports or report extracts from independent bodies (e.g. auditor, audit, data protection officer), suitable certification through an IT security or data protection audit (e.g. in accordance with ISO 27001) or certification approved by the responsible supervisory authorities.

9.3. This shall not affect the Client's right to carry out on-site inspections. However, the Client shall consider whether an on-site inspection is still necessary after submission of meaningful documentation, in particular taking into account the maintenance of the Contractor's proper operation. The Client shall only carry out on-site inspections in consultation with the Contractor.

10. Deletion of data and return of data carriers

At the Client's option and request - at the latest upon termination of the data processing - the Contractor shall, at the Client's discretion, either hand over to the Client all documents that have come into its possession, processing and usage results and data pertaining to the contractual relationship or, with the Client's prior consent, destroy them in accordance with data protection regulations.

Documentation that serves as proof of proper data processing in accordance with the order or that the contractor is legally obliged to retain may be retained by the contractor beyond the end of the contract in accordance with the respective retention periods.

11. Liability; choice of law; place of jurisdiction

The agreements made in the main contract shall apply to the Contractor's liability in connection with this DPA and to the choice of law and place of jurisdiction applicable to this DPA.

Signatures

For and on behalf of the client:	**For and on behalf of the contractor:**
	Visitor Analytics GmbH
.....	.....
Date	Date
.....	.....
Name / Position	Name / Position Tim Hammermann (CEO)
.....	.....
Signature	Signature

Appendix 1: Description of the technical and organizational security measures taken by TWIPLA.

TWIPLA has taken the following technical and organizational security measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services:

1. Confidentiality

TWIPLA has taken the following technical and organizational security precautions, in particular to ensure the confidentiality of the processing systems and services, in detail:

1.1. TWIPLA processes all Personal Usage Data on servers within the Federal Republic of Germany that are owned and operated by industry-leading cloud service providers that offer sophisticated measures to protect against unauthorized access to data processing devices (namely telephones, database and application servers and related hardware). Such measures include:

1.1.1. Data centers are monitored around the clock by high-resolution indoor and outdoor cameras that can detect and track intruders;

1.1.2. Access logs, activity recordings and camera footage are available in the event of an incident;

1.1.3. Data centers are also routinely patrolled by experienced security officers who have undergone rigorous background checks and training;

1.1.4. Documented distribution of keys to employees and colocation customers for co-location racks;

1.1.5. Only authorized employees with specific roles may access the servers.

1.2. TWIPLA takes appropriate measures to prevent its data processing systems from being used by unauthorized persons. This is achieved by:

1.2.1. Automatic detection of repeated or mass unauthorized access; allowing access to the TWIPLA app exclusively on the basis of an encrypted key that can only be decrypted by TWIPLA using a secret;

1.2.2. SSL encryption on all public customer endpoints

1.2.3. All access to data content is logged, monitored and tracked.

1.3. TWIPLA employees who are authorized to use TWIPLA's data processing systems may only access Personal Data within the scope and to the extent of their respective access rights (authorization). In particular, access rights and levels are based on the function and role of employees, using the concepts of least privilege and need-to-know to align access rights with defined responsibilities. This is achieved by:

1.3.1. Employee guidelines and training;

1.3.2. Effective and moderate disciplinary measures against persons who access personal data without authorization;

1.3.3. Restricted access to personal data for authorized persons only;

1.3.4. Industry standard encryption; and

1.3.5. Guidelines for controlling the storage of backup copies.

2. Integrity

TWIPLA has taken the following technical and organizational security precautions, in particular to ensure the integrity of the processing systems and services:

2.1. TWIPLA shall take suitable measures to prevent personal data from being read, copied, modified or deleted by unauthorized persons during transmission or transport of the data carriers. This is achieved by

2.1.1. Use of the latest firewall and encryption technologies to protect the gateways and pipelines through which the data is transported;

2.1.2. Industry standard encryption; and

2.1.3. Avoiding the storage of personal data on portable storage media for transportation purposes and on company-owned laptops or other mobile devices.

2.2. TWIPLA shall not access customer content unless this is necessary to provide the customer with the TWIPLA services selected by the customer or to rectify system errors. TWIPLA shall not access the customer's content for any other purpose. Accordingly, TWIPLA does not know which content the customer selects to store on its systems and cannot distinguish between personal data and other content, so

TWIPLA treats all customer content equally. In this way, all Customer Content benefits from TWIPLA's same robust security measures, regardless of whether that content contains Personal Data or not.

3. Availability

In particular, TWIPLA has implemented the following technical and organizational security measures to ensure the availability of processing systems and services:

3.1. TWIPLA takes appropriate measures to ensure that personal data is protected against accidental destruction or loss. This is achieved by:

3.1.1. Redundancy of the infrastructure;

3.1.2. Policies that prohibit permanent local (workplace) storage of Personal Data; and

3.1.3. Carrying out regular data backups.

4. Load capacity

Visitors Analytics uses a web server with thread pooling for better performance to ensure we can support a large number of connections. The majority of our project is based on a producer/consumer pattern to ensure that connections are closed as quickly as possible so that resources are available for pending connections. In addition, our databases are backed up to ensure that we can fall back to an older version in case of unforeseen circumstances.

Server setup processes are also automated (and, with the exception of databases, stateless) to ensure that we can recreate and restart a new server if something happens to the old instance.

Annex 2 – Sub-processors

Name of the sub-processor	Address	Function/processing steps performed	What data is forwarded to the sub-processor?
Hetzner Online GmbH	Industriestrasse 25 91710 Gunzenhausen Germany European Union	Web hosting provider	All website visitor data processed on behalf of the customer is stored in a database hosted by Hetzner.
ALL-INKL.COM - New Media Münnich	Hauptstraße 68 02742 Friedersdorf Germany European Union	E-mail provider	First name, surname and e-mail addresses for sending status reports and newsletters
OVH SAS	2 rue Kellermann 59100 Roubaix France European Union	Web hosting provider	All data processed on behalf of the customer is temporarily (usually less than 1 second) stored and processed on the CDN nodes for further processing.
Hostinger UAB	Švitrigailos str. 34 03230 Vilnius Lithuania European Union	Web hosting provider	All data processed on behalf of the customer is temporarily (usually less than 1 second) stored and processed on the CDN nodes for further processing.