Data Processing Agreement
("DPA")

between

("**Customer**".)
and

Visitor Analytics GmbH
Seestraße 76
82235 Berg

("TWIPLA")

(each a "**Party**" and together the "**Parties**")

PREAMBLE

(A) TWIPLA provides Customer with the Services described in Section 4.1. of the Terms of Service. To enable Customer to use the Services, the Parties have entered into the Agreement described in Sections 1.1. and 3. of the Terms of Service. This DPA forms an integral part of the Agreement.

(B) The provision of the Services involves the Processing of Personal Data. Under the Agreement, Customer shall remain responsible for the Processing of Personal Data, for the assessment of the legal admissibility of the Processing of Personal Data, and for adhering to the rights of the Data Subjects (as defined below).

(C) The Parties wish to enter into this DPA in accordance with the provisions of the EU General Data Protection Regulation (Regulation (EU) 2016/679) and applicable national data protection laws

In consideration of the mutual covenants and obligations declared herein, THE PARTIES AGREE:

1. Definitions and interpretation

The following definitions apply in addition to those set forth in Section 2. of the Terms of Service.

1.1. Definitions

"**Data Protection Laws**" means all applicable data protection laws and regulations in the jurisdiction where Customer is located, including Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation, "GDPR**"), Directive 2002/58/EC of the European Parliament and of the Council of 12. July 2002 concerning the Processing of Personal Data and the protection of privacy in the electronic communications sector (ePrivacy Directive) and applicable local data protection laws.

"**Instruction**" means an instruction given by Customer to TWIPLA directing it to perform a specific action in relation to Personal Data, as further set out in Section 3.2 of this DPA.

"**Personnel**" means all persons authorised to process Personal Data under the Agreement.

"**Purposes**" means the purposes for which TWIPLA processes Personal Data, as set out in Section 2 and *Annex 2* of this DPA.

"**Personal Data Breach**" means a breach of security that results in the accidental, or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

1.2. All capitalized terms used but not defined in this DPA shall have the meaning ascribed to such terms in the Terms of Service. In the event of any conflict or ambiguity, between any provision of this DPA and any provision of the Terms of Service, the provision of the Terms of Service shall prevail.

1.3. References to the terms "Personal Data", "Processing", "Processed" and "Data Subject" in this DPA shall be construed in accordance with the meanings ascribed to them in the GDPR.

1.4. All words following the terms "including", "including", or "in particular", or any similar phrase are illustrative and shall not limit the generality of the words associated with them.

1.5. Unless the context otherwise requires, words in the singular include the plural, and words in the plural include the singular.

1.6. A reference to a statute or regulation is a reference to the statute or regulation in force at the time of the conclusion of the Agreement. Such reference shall include any subordinate legislation in force under that law or legislation at the time of the conclusion of the Agreement.

2. Subject of the DPA

The subject of this DPA is the Processing of Personal Data pursuant to *Annex 1* in connection with the following Services:

A simple and straightforward analytics tool for non-technical people, TWIPLA provides easy-to-understand web analytics and a user-friendly user experience for people who are not very technical. Once integrated into a website, the TWIPLA app ("**App**") provides real-time insights about each visitor and their behavior. This information can be used to interact with visitors and significantly improve Customer's sales process. Customer can monitor their visitors, new visitors, IP addresses (if IP anonymization is not enabled), page visits, bounce rates, conversions, and even live visitors from the moment they visit the website.

3. Rights and obligations of Customer

3.1. Customer acknowledges and agrees to this:

3.1.1. It is Customer's responsibility as a Controller to ensure that its use of the Services complies with all Data Protection Laws applicable to it (including, in particular, in relation to obtaining all necessary consents that must be obtained from Data Subjects);

3.1.2. If Customer requests TWIPLA to transfer Personal Usage Data (including Personal Data) to a third party, Customer shall be solely responsible and liable for such transfer and in no event shall Customer act or fail to act in a manner that would cause TWIPLA to violate any Data Protection Laws;

3.1.3. TWIPLA has no obligation to investigate the completeness, accuracy, or sufficiency of Personal Usage Data, including Personal Data.

3.2. TWIPLA Processes Personal Usage Data only based on instructions by Customer. Customer instructs TWIPLA to Process the types of Personal Data set out in Annex 1. This is Customer's final instruction to TWIPLA with respect to the Processing of Personal Usage Data. If Customer requests TWIPLA to Process Personal (Usage) Data outside the scope of the Agreement, Customer is required to enter into an additional agreement with TWIPLA and Customer shall bear the cost of such additional Processing.

3.3. In the event of a request by a Data Subject against TWIPLA, Customer agrees to assist TWIPLA in verifying active legitimacy and subject matter in defending the claim.

4. TWIPLA Rights and Responsibilities

4.1. TWIPLA will only Process Personal Data to the extent and in the manner reasonably necessary for the purposes and in accordance with the Agreement and Customer's documented instructions from time to time, unless the exception in Art. 28 (3) (a) GDPR applies.

4.2. TWIPLA may only transfer, store, or Process Personal Data outside the European Economic Area, or the country where Customer is located if an adequate level of data protection is ensured, unless TWIPLA is required to do so by applicable law. In such case, TWIPLA must inform Customer of such legal requirement prior to the Processing unless such law prohibits such information for important reasons of public interest. Section 8 of this DPA remains unaffected.

4.3. TWIPLA shall maintain records of any Processing of Personal Data it performs on behalf of Customer and shall not disclose such records to any third party without the prior written consent of Customer, except as otherwise provided by applicable law.

4.4. At Customer's request and at Customer's sole expense, TWIPLA will provide Customer with a copy of all Personal Data in its possession under the Agreement in a commonly used and machine-readable format.

4.5. TWIPLA shall promptly (and in any event within five (5) business days of receipt) notify Customer in writing of any communication received from a Data Subject regarding his or her rights of access, rectification, erasure, or blocking of his or her Personal Data.

4.6. To the extent not prohibited by Data Protection Laws and applicable national laws, TWIPLA shall notify Customer in writing as soon as reasonably practicable of any subpoena or other judicial or administrative order or proceeding involving access to, or disclosure of, Customer’s Personal Data. TWIPLA acknowledges that Customer may, at its own expense, attempt to defend or contest any such action in place of and on behalf of TWIPLA.

4.7. TWIPLA will assist Customer, to the extent it is able, to comply with the requests and claims of Data Subjects set forth in Chapter III of the GDPR and to comply with the obligations set forth in Articles 32 to 36 of the GDPR. Insofar as Customer has reporting or notification obligations in the event of a Personal Data Breach, TWIPLA undertakes to provide Customer with cooperation and support at Customer's sole expense.

4.8. TWIPLA will notify Customer immediately if it believes an instruction violates Data Protection Laws. TWIPLA is not obligated to actively monitor instructions for violations of Data Protection Laws.

4.9. TWIPLA complies with its obligation to implement a procedure for the regular testing, assessment, and evaluation of the effectiveness of the technical and organisational measures to ensure the security of the Processing in accordance with Article 32(1)(d) of the GDPR.

5. TWIPLA Security Commitments

5.1. TWIPLA shall take appropriate technical and organizational measures to protect Personal Usage Data that comply with the requirements of Article 32 GDPR. In particular, TWIPLA shall take technical and organizational measures to ensure the confidentiality, integrity, availability, and resilience of the Processing systems and Services on an ongoing basis. The technical and organisational measures are described in *Annex 2.* Customer is aware of these technical and organisational measures and is responsible for ensuring that they provide an adequate level of protection against the risks posed by the Processed Personal Usage Data. TWIPLA may update or amend the measures set out in *Annex 2* from time to time, provided that such updates or amendments do not materially change the level of security of the Personal Usage Data.

5.2. TWIPLA shall notify Customer without undue delay upon becoming aware of a Personal Data Breach and shall assist Customer in its notification and reporting obligations towards third parties, taking into account the nature of the Processing and the information available to TWIPLA. However, Customer shall be solely responsible for fulfilling its notification and notification obligations to third parties. TWIPLA will take steps, as appropriate, to mitigate the potential adverse effects of the Personal Data Breach.

5.3. In the event of loss or corruption of Personal Usage Data, TWIPLA will use commercially reasonable efforts to restore the lost or corrupted Personal Usage Data from the most recent backup of such Personal Usage Data maintained by TWIPLA in accordance with its standard archiving procedures.

5.4. TWIPLA is not responsible for the destruction, loss, alteration, or disclosure of Personal Usage Data caused by third parties (other than third parties engaged by TWIPLA to perform services related to maintaining and securing Personal Usage Data).

6. Personnel

6.1. TWIPLA shall ensure that access to the Personal Usage Data is limited to those employees who need access to the Personal Usage Data in order to perform TWIPLA' obligations under this DPA and/or other parts of the Agreement.

6.2. TWIPLA ensures that all employees authorised to Process Personal Usage Data have committed to confidentiality or are subject to an equivalent legal obligation of confidentiality.

7. Information to demonstrate compliance

7.1. At the request of Customer, TWIPLA shall provide Customer with the information necessary to demonstrate compliance with the legal obligations in a commonly used and machine-readable format.

7.2. As of the effective date of this DPA, TWIPLA is certified to ISO 27001. If Customer requires audits, including inspections, to be conducted, TWIPLA will use external auditors to demonstrate compliance with the obligations set forth in this DPA. Such audit shall be conducted annually by an external auditor in accordance with ISO 27001 standards or other standards substantially equivalent to ISO 27001, at TWIPLA' option and expense. Upon written request of Customer, TWIPLA shall provide the audit report to Customer.

7.3. In the event of official inquiries by data protection authorities responsible for Processing under this DPA, or if Customer has reasonable grounds to believe that a Personal Data Breach has occurred, Customer may, upon at least fourteen (14) days prior written notice to TWIPLA, have a representative of Customer, or an independent third party, conduct an on-site visit to TWIPLA at Customer's expense. Such audits shall be conducted during normal business hours without disrupting TWIPLA' ongoing business operations. TWIPLA may condition the audits on the signing of a non-disclosure agreement with TWIPLA. If the auditor engaged by Customer has a competitive relationship with TWIPLA, TWIPLA has the right to object to the conduct of the audit.

8. Subprocessors

8.1. Customer agrees that TWIPLA is authorized to subcontract TWIPLA' obligations set forth in this DPA. Customer agrees to the Subprocessors currently used by TWIPLA as set forth in *Annex 3.*

8.2. Before adding a new Subprocessor or replacing an existing Subprocessor, TWIPLA must inform Customer and grant Customer a reasonable period of time to object for good cause. If Customer does not object within the time limit, the consent to the change of the Subprocessor shall be deemed granted. If an important reason exists and a mutually agreeable solution between the Parties is not possible, the Parties shall be granted a special right of termination.

8.3. TWIPLA agrees in the agreement with the Subprocessor to provide the same level of protection for Personal Usage Data as set forth in this DPA.

9. Term and termination

The term of this DPA begins together with the Term of the Agreement and ends with the termination of the Agreement. Unless otherwise agreed by the Parties, the termination of this DPA shall automatically terminate the entire Agreement.

10. Limitation of liability

The limitation of liability agreed between the Parties on the basis of the Terms of Service shall also apply to this DPA unless expressly agreed otherwise.

11. Indemnity

Customer shall defend TWIPLA against any claim for damages arising from a breach of the Data Protection Laws, unless the damage was caused because TWIPLA failed to comply with the obligations of the Data Protection Laws specifically addressed to Processors or if it acted outside or contrary to the lawful instructions of Customer or the Agreement.

12. General

12.1. Upon expiration or termination of the entire Agreement or this DPA, or at Customer's earlier request, TWIPLA will, at Customer's option, return to Customer, or securely delete or destroy, all Personal Usage Data and existing copies (including Personal Data) in a manner appropriate to the sensitivity of the data, unless Data Protection Laws require retention of the Personal Usage Data. TWIPLA will confirm in writing to Customer that the deletion process has been completed.

12.2. No waiver of any right under this DPA shall be effective unless in writing and shall apply only to the circumstances for which it is granted. No failure, or delay by any Party in exercising any right or remedy under this DPA, or by law, shall constitute a waiver of such (or any other) right, or remedy, and shall not preclude or limit its further exercise. No single or partial exercise of any such right or remedy shall preclude, or limit, the further exercise of that (or any other) right, or remedy. Except as otherwise expressly provided, rights arising under this DPA are cumulative and not exclusive of any rights provided by law.

12.3. If and to the extent that any provision of this DPA is found to be illegal, void, or unenforceable, the validity of the remaining provisions of this DPA shall not be affected. The Parties agree to replace any such invalid provision with a valid provision that comes as close as possible to the original intent of the parties with respect to this DPA.

12.4. Neither Party may assign its rights or obligations under this DPA without the prior written consent of the other Party, except that either Party may assign this DPA in its entirety without such consent to an entity of good standing (other than a direct competitor of the other Party) capable of performing the rights and obligations under this DPA, with the result that all or substantially all of the assets or business of the assigning Party shall pass to the other Party. A person who is not a party to this DPA shall have no rights under or in connection with this DPA.

12.5. This DPA shall be governed by and construed in accordance with the local laws at TWIPLA', notwithstanding any laws that might otherwise apply in accordance with the principles of private international law. The Parties hereby submit exclusively and irrevocably to the jurisdiction of TWIPLA' principal place of business with respect to any dispute arising out of this DPA. TWIPLA' Terms of Service apply. Customer's general terms and conditions do not apply.

12.6. The DPA is an annex to the Terms of Service and an integral part of the Agreement. Notwithstanding Section 1.2. of this DPA, in the event of any inconsistency between the clauses of the Terms of Service and this DPA, the clauses of this DPA shall prevail.

Attachments

Signatures

For and on behalf of	**For and on behalf of "Visitor Analytics GmbH":**
	Tim Hammermann, Managing Director
Name	Name
	
Signature	Signature

Annex 1 – Categories of data and Data Subjects

Permitted Purpose:

Collecting information about how Visitors use the Customer's Website via the App. Analyze this information via the App and provide it to Customer on a web-based Platform in statistics dashboards with charts, graphs and maps. Customers can export portions of the statistics data. Customers can use the Services through their own standalone account, or allow Customer's employees to use the Services by adding an employee.

Categories of Data Subjects

The categories of Data Subjects are Visitors of Customer’s Website.

Processing operations

The affectd Personal Data is subject to basic activities such as the collection of usage data on Customer’s Website, the provision of Processed information and statistics to Customer, the export of statistics and the exclusion of Customer visits to the Customer Website.

Categories of data

TWIPLA Processes the following Personal Data or categories of data:

Data about a Visitor's visit to the Customer Website (timestamp, number of pages viewed, IP address - if IP anonymization is not enabled); information about the Visitor's device (e.g. mobile phone, or computer, operating system and version, browser, screen size); approximate geolocation data derived from the location of the visitor's IP address.

Sensitive data (if applicable)

The Parties do not anticipate that sensitive data will be Processed.

Data collected through cookies

In addition, the following cookies are set by TWIPLA on Visitors' devices to provide the Services:

Name	Purpose	Collected data	Useful life	Category
*_ignore_Visits_UniqueHash	The TWIPLA App places this cookie at the Customer's request for a specific web page to disable TWIPLA website analytics tracking for that specific web page.	Ignore visits	365 days	Absolutely necessary
*_ignoreVisits_all	The TWIPLA App places this cookie at the Customer's request to disable website tracking analytics for all websites that use TWIPLA.	Ignore visits	365 days	Absolutely necessary

Annex 2 – Technical and organisational measures

in accordance with Art. 32 GDPR

Description of the technical and organisational security measures taken by TWIPLA.

TWIPLA has adopted the following technical and organizational security measures to ensure the ongoing confidentiality, integrity, availability and resilience of its Processing systems and Services:

1. Confidentiality

TWIPLA has adopted the following technical and organizational security measures, in particular to ensure the confidentiality of the Processing systems and Services, in detail:

1.1. TWIPLA Processes all Personal Usage Data on servers located remotely within the Federal Republic of Germany, 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 records, and camera footage are available in case 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 co-location customers for co-location racks;

1.1.5. Only authorized employees with specific roles are allowed to access the servers.

1.2. TWIPLA employs appropriate measures to prevent its data Processing systems from being used by unauthorised persons. This is achieved by:

1.2.1. Automatic detection of repeated or mass unauthorized access; allowing access to the TWIPLA app based solely on 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' data Processing systems may access Personal Data only to the extent and within the scope of their respective access rights (authorization). Specifically, access rights and levels are based on employee function and role, 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 policies and training;

1.3.2. Effective and measured disciplinary action against individuals who access Personal Data without authorization;

1.3.3. Restricted access to Personal Data only for authorized persons;

1.3.4. Industry standard encryption; and

1.3.5. Guidelines for controlling the retention of backup copies.

2. Integrity

TWIPLA has implemented the following technical and organisational security measures, in particular to ensure the integrity of the Processing systems and Services:

2.1. TWIPLA takes appropriate measures to prevent Personal Data from being read, copied, modified, or deleted by unauthorized persons during transmission, or transport of the data media. This is achieved by:

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

2.1.2. Industry standard encryption; and

2.1.3. Avoid storing Personal Data on portable storage devices for transport purposes and on company-owned laptops, or other mobile devices.

2.2. TWIPLA does not access Customer content except as necessary to provide Customer with the TWIPLA Services selected by Customer or to troubleshoot system errors. TWIPLA does not access Customer content for any other purpose. Accordingly, TWIPLA does not know what content 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 the same robust security measures from TWIPLA, regardless of whether that content contains Personal Data or not.

3. Availability

TWIPLA has implemented, in particular, the following technical and organizational security measures to ensure the availability of Processing systems and Services:

3.1. TWIPLA implements appropriate measures to ensure that Personal Data is protected from accidental destruction, or loss. This is achieved by:

3.1.1. Infrastructure redundancy;

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

3.1.3. Carrying out regular data backups.

4. Resilience

Visitors Analytics uses a thread-pooling web server for better performance to ensure we can support a large number of connections. Most 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 upcoming connections. In addition, our databases are backed up to ensure that we can revert 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 start a new server if something happens to the old instance.

Annex 3 – Subprocessors

Name of Subprocessor	Address	Function/Processing steps performed	What data is forwarded to the Subprocessor?
Hetzner Online GmbH	Industriestraße 25 91710 Gunzenhausen Germany	Web hosting provider	All Visitor data Processed on behalf of Customer is stored in a database hosted by Hetzner.
Visitor Analytics SRL	Calea Dorobantilor 18 400121 Cluj-Napoca Romania	Group companies & infrastructure providers	Where appropriate, data is shared for the implementation of technical functionalities.
ALL-INKL.COM - Neue Medien Münnich	Hauptstraße 68 02742 Friedersdorf Germany	Email provider	First name, last name and email addresses for sending status reports and newsletters