Data Processing Agreement

("DPA")

between

and

Visitor Analytics GmbH

Stefan-George-Ring 19, 81929 Munich, Germany

("**Visitor Analytics**")

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

WHEREAS

(A) Visitor Analytics offers the Services described in Section 4.1. of the Service Terms to Customer. To enable Customer to use the Services, the Parties entered into the Contract described in Sections 1.1. and 3. of the Service Terms. This DPA forms an integral part of the Contract.

(B) The provision of the Services involves the Processing of Personal Data. Within the framework of the Contract, the Customer shall remain the responsible body for the Processing of Personal Data, for assessing the legal admissibility of Processing the Personal Data and for respecting the rights of Data Subjects (as defined below).

(C) The Parties wish to enter into this DPA in compliance with the provisions of the EU General Data Protection Regulation (Regulation (EU) 2016/679) and the applicable national Data Protection Laws.

In consideration of the mutual covenants and undertakings stated herein, THE PARTIES AGREE AS FOLLOWS:

1. Definitions and Interpretation

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

1.1. Definitions

"Data Protection Laws" means all applicable data protection laws and regulation in the jurisdiction where the 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 (Directive on privacy and electronic communications), and

applicable local data protection laws.

"Instruction" means an instruction, issued by Customer to Visitor Analytics, and directing the same to perform a specific action with regard to Personal Data as further set out in Section 3.2 of this DPA.

"**Personnel**" means all persons authorized to process Personal Data under the Contract.

"Purposes" means the purposes for which Visitor Analytics Processes Personal Data as listed in Section 2 and *Exhibit 1* of this DPA.

"Security Incident" means a breach of security leading to 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 Service Terms. In the case of conflict or ambiguity between any provision in this DPA and any provision contained in the Service Terms, the provision in the Service Terms 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 attributed to them in the GDPR.

1.4. Any words following the terms "including", "include" or "in particular" or any similar phrase are illustrative and shall not limit the generality of the related words.

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

1.6. A reference to a statute or statutory provision is a reference to it as it is in force as at the date of the Contract. Such reference shall include all subordinate legislation made as at the date of the Contract under that statute or statutory provision.

2. Subject-Matter of the DPA

The subject matter of this DPA is the Processing of Personal Data as set forth in *Exhibit 1* in connection with the following services:

As a simple and straightforward analytics tool for non-technical people, the Visitor Analytics provides easy-to-understand web analytics and a friendly user experience for people that are not very technical. Once integrated into a Website, the Visitor Analytics' application provides real time insights about each Visitor and its behavior. This information can be used to interact with the Visitors and significantly improve Customer's sales processes. Basically, Customer may monitor its Visitors, new Visitors, IP addresses (if ip anonymization is not enabled), page visits, bounce rates, conversions and even live Visitors from the very moment they join the Website.

3. Rights and obligations of Customer

3.1. Customer acknowledges and agrees that:

3.1.1. It is Customer's responsibility as Customer to ensure that its use of the Services complies with all Data Protection Laws applicable to Customer (including, in particular, in respect of the capturing of any necessary consents required to be obtained from the Data Subjects);

3.1.2. If Customer requests Visitor Analytics to transfer Personal Use Data (including Personal Data) to a third party, Customer is solely responsible and liable for this transfer and in any

event, Customer shall not act or omit to act in a way which places Visitor Analytics in breach of any applicable Data Protection Laws;

3.1.3. Visitor Analytics is under no duty to investigate the completeness, accuracy or sufficiency of the Personal Use Data, including Personal Data.

3.2. Visitor Analytics shall Process Personal Use Data only on Instructions from Customer. The Customer instructs Visitor Analytics to Process the types of Personal Data listed in our Terms of Use under *Exhibit 1* and Annex *1 – Description of Services and Prices* for the Purposes. This is the final Instruction of Customer to Visitor Analytics with regard to the Processing of Personal Use Data. If Customer requests Visitor Analytics to Process Personal (Use) Data outside the scope of the Contract, it is Customer's obligation to enter into an additional agreement with Visitor Analytics and Customer will have to bear the costs for such additional Processing.

3.3. In case of a claim of a Data Subject against Visitor Analytics, Customer undertakes to assist Visitor Analytics with regard to the verification of the active legitimation and subject matter in the defense of the claim.

4. Rights and obligations of Visitor Analytics

4.1. Visitor Analytics shall Process Personal Data only to the extent, and in such a manner, as is reasonably necessary for the Purposes and in accordance with the Contract and Customer's written Instructions from time to time, unless the exception in Art. 28 (3) (a) GDPR applies.

4.2. Visitor Analytics may only transfer, store or Process Personal Data outside the European Economic Area or the country where Customers are located if an adequate level of data protection is established, unless Visitor Analytics is required to do so by applicable law. In such a case, Visitor Analytics shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Section 8 of this DPA remains unaffected.

4.3. Visitor Analytics shall keep a record of any Processing of Personal Data it carries out on behalf of Customer and shall only disclose such records to third parties with the prior written consent of Customer, unless provided otherwise by applicable law.

4.4. At Customer's request and sole expense, Visitor Analytics shall provide to Customer a copy of all Personal Data held by it under the Contract in a commonly used and machine-readable format.

4.5. Visitor Analytics shall notify Customer promptly in writing (and in any event within five (5) working days of receipt) of any communication received from a Data Subject relating to its rights to access, modify, correct, erase or block his or her Personal Data.

4.6. To the extent not prohibited by applicable Data Protection Laws and applicable national laws, Visitor Analytics shall notify Customer as soon as reasonably practicable in writing of any subpoena or other judicial or administrative order or proceeding seeking access to or disclosure of Personal Data. Visitor Analytics acknowledges that Customer may, at its sole expense, seek to defend against or contest such action in lieu of and on behalf of Visitor Analytics.

4.7. Visitor Analytics shall assist Customer within the scope of its ability to fulfil the requests and claims of Data Subjects laid down in Chapter III of the GDPR and to comply with the obligations pursuant to Articles 32 to 36 of the GDPR. To the extent Customer has notification or communication obligations in case of a Security Incident, Visitor Analytics undertakes to provide cooperation and support to Customer at Customer's sole expense.

4.8. Visitor Analytics shall notify Customer immediately if, in its opinion, an Instruction infringes Data Protection Laws. Visitor Analytics is not obliged to actively monitor Instructions for infringements of Data Protection Laws.

4.9. Visitor Analytics shall comply with its obligation to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing pursuant to Art. 32 (1) (d) of the GDPR.

5. Security obligations of Visitor Analytics

5.1. Visitor Analytics shall implement appropriate technical and organizational measures to protect the Personal Use Data which shall meet the requirements of Art. 32 GDPR. In particular, Visitor Analytics shall implement technical and organizational measures to provide the on-going confidentiality, integrity, availability and resilience of processing systems and services. The technical and organizational measures are described in *Exhibit 2*. Customer has knowledge of these technical and organizational measures and is responsible for ensuring that they provide an appropriate level of protection for the risks of the Personal Use Data being Processed. Visitor Analytics may update or modify the measures listed *Exhibit 2* from time to time provided that such updates or modifications do not result in any material degradation of the security of the Personal Use Data.

5.2. Visitor Analytics shall notify Customer without undue delay after becoming aware of a Security Incident and assist Customer with its third party notification and communication obligations, taking into account the nature of Processing and the information available to Visitor Analytics. However, Customer is solely responsible for fulfilling any third party notification and communication obligations. Visitor Analytics will take, where appropriate, measures to mitigate the possible adverse effects of the Security Incident.

5.3. In the event of any loss or damage to Personal Use Data, Visitor Analytics shall use commercially reasonable endeavors to restore the lost or damaged Personal Use Data from the latest back-up of such Personal Use Data maintained by Visitor Analytics in accordance with its standard archiving procedures.

5.4. Visitor Analytics shall not be responsible for any destruction, loss, alteration or disclosure of Personal Use Data caused by any third party (except any third parties subcontracted by Visitor Analytics to perform services related to Personal Use Data maintenance and back-up).

6. Personnel

6.1. Visitor Analytics shall provide that access to Personal Use Data is limited to those Personnel who need access to the Personal Use Data to meet Visitor Analytics' obligations under this DPA and/or other parts of the Contract.

6.2. Visitor Analytics shall provide that all Personnel authorized to Process Personal Use Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7. Information to demonstrate compliance

7.1. At Customer's request, Visitor Analytics makes available to Customer the information necessary to demonstrate compliance with the statutory obligations, in a commonly used and machine-readable format.

7.2. As of the date of this Contract, Visitor Analytics is certified under ISO 27001. If Customer requests to conduct audits, including inspections, Visitor Analytics will use external auditors to demonstrate compliance with the obligations laid down in this DPA. This audit will be performed by a third party auditor annually according to ISO 27001 standards or other standards that are substantially equivalent to ISO 27001 at the selection and expense of Visitor Analytics. Visitor Analytics will provide the audit report to Customer at Customer's written request.

7.3. In cases of official requests of data protection authorities with jurisdiction over the Processing hereunder, or in case Customer has reasonable grounds to assume that a Security Incident has taken place, Customer may upon at least fourteen (14) days prior written notice to Visitor Analytics conduct a site visit at Visitor Analytics' at Customer's expense by a representative of Customer or its independent third party auditor. Such audits shall be carried out at normal business hours without disrupting the ongoing business operations of Visitor Analytics. Visitor Analytics may make the audits dependent on the signing of a nondisclosure agreement with Visitor Analytics. If the auditor commissioned by Customer is in a competitive relationship with Visitor Analytics, Visitor Analytics shall have the right to object to Customer.

8. Subprocessors

8.1. Customer consents that Visitor Analytics shall be entitled to subcontract the Visitor Analytics' obligations specified in this DPA to Subprocessors. Customer approves the Sub Processors listed in *Exhibit 3* that are currently used by Visitor Analytics.

8.2. Prior to adding new Subprocessor or replacing existing Subprocessor, Visitor Analytics shall inform Customer thereof and provide a reasonable deadline to Customer to object for important reasons. If Customer does not object within the deadline, the consent to the change of Subprocessor shall be deemed to be given. If there is an important reason and an amicable solution is not possible between the Parties, the Parties are granted a special right of termination.

8.3. Visitor Analytics undertakes in the Subprocessor agreement to provide for the same protection level of Personal Use Data as set out in this Contract.

9. Term and termination

The term of this DPA shall commence along with the Term of the Contract and end upon termination of the Contract. Unless otherwise agreed by the Parties termination of this DPA shall automatically terminate the whole Contract.

10. Limitation of Liability

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

11. Indemnity

Customer shall defend Visitor Analytics against any damage claim as a result of an infringement of Data Protection Laws, unless the damage was caused because Visitor Analytics did not comply with obligations of the Data Protection Laws specifically directed to Processors or where it has acted outside or contrary to lawful Instructions of Customer or the Contract.

12. General

12.1. Upon expiry or termination of the whole Contract or this DPA, or upon earlier request by Customer, Visitor Analytics shall – at the choice of Customer - return to Customer or securely delete or destroy all Personal Use Data and existing copies (including Personal Data) in a manner appropriate to the sensitivity thereof, unless applicable Data Protection Laws require storage of the Personal Use Data. Visitor Analytics shall provide written confirmation to Customer that the deletion process has been completed.

12.2. A waiver of any right under this DPA is only effective if it is in writing and it applies only to the circumstances for which it is given. No failure or delay by a Party in exercising any right or remedy under this DPA or by law shall constitute a waiver of that (or any other) right or remedy, nor preclude or restrict its further exercise. No single or partial exercise of such right or remedy shall preclude or restrict the further exercise of that (or any other) right or remedy. Unless specifically provided otherwise, rights arising under this DPA are cumulative and do not exclude rights provided by law.

12.3. If and to the extent that one of the provisions of this DPA is held to be illegal, void or unenforceable, the validity of the remaining provisions of this DPA shall not be affected. The Parties agree to replace such an invalid provision by a valid one which comes as close as possible to the Parties' original objective as regards this DPA.

12.4. Neither Party may assign any of its rights or obligations under this DPA without the prior written consent of the other Party, except that either Party may assign this DPA as a whole without such consent to an entity of good standing (other than any direct competitor of the other Party) capable of complying with the rights and obligations under this DPA succeeding to all or substantially all of such assigning Party's assets or business. A person who is not a party to this DPA shall not have any rights under or in connection with it.

12.5. This DPA shall be governed by the local laws at Visitor Analytics' and is to be interpreted accordingly, notwithstanding the laws which could otherwise apply in accordance with the principles of international private law. The Parties hereby exclusively and irrevocably submit to the place of jurisdiction of the principal place of business of Visitor Analytics, concerning any legal disputes which arise from this DPO. Visitor Analytics' Service Terms apply. Customer's general terms and conditions shall not apply.

12.6. The DPA is an attachment to the Service Terms and integral part of the Contract. Notwithstanding section 1.2. of this DPA, in case of contradictions between clauses of the Service Terms and this DPA, the clauses of this DPA shall prevail.

Exhibits

Signatures

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

Exhibit 1 – Categories of Data and Data Subjects

Permitted Purpose:

Collecting information on Visitors' use of Customer Website via the App. Analyzing this information via the App and making it available to Customer on a web-based platform in statistics dashboards featuring charts, graphs and maps. Customers may export parts of the Statistics Data. Customers can use the Services via their own account or enable Customer's employees to use the Services by means of adding a contributor.

Categories of Data Subjects

The **c**ategories of Data Subjects affected by the Processing are Customer; **t**hird parties related to Customer such as employees or other authorized persons; Visitors; and persons authorized by Visitor Analytics such as employees or other authorized Personnel.

Processing operations

Depending on the person of the Data Subject, the Personal Data inserted will be subject to basic activities such as Customer's registration to implement the App; providing Customer with edited information (Visitor Analytics) and statistics; export of statistics; the exclusion of Customer's visits to Customer Website; and Customer account management.

Categories of data

Depending on the person of the Data Subject, the Personal Data inserted concern the following categories of data: name; company name; email address, website; data on the connection of a Visitor to Customer Website (timestamp, number of pages viewed, IP address — if IP anonymization is not enabled); information about the Visitor's device (e.g. mobile or computer, OS and version, browser, screen size); approximate geolocation data inferred from Visitor's IP address location.

Sensitive data (if appropriate)

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

Data collected by Cookies

Additionally, the following Cookies are set by the Visitor Analytics on the Visitors' devices to provide the Services:

Name	Purpose	Collected Data	Lifespan	Category
*_visitor_analytics_WEBSITE_UNIQUE_HASH	The Visitor Analytics App uses this cookie in order to track the actions that the user is doing on the website such as the pages visited, frequency and so on.	Visitor ID	365 days	Strictly Necessary
*_ignore_Visits_UniqueHash	The Visitor Analytics app places this cookie at the request of the user for a specific website, in order to disable Visitor Analytics website analytics tracking for that specific website.	Ignore Visits	365 days	Strictly Necessary
*_ignoreVisits_all	The Visitor Analytics app places this cookie at the request of the user in order to disable the website analytics tracking for all the websites using Visitor Analytics.	Ignore Visits	365 days	Strictly Necessary

Exhibit 2 - Technical and organizational measures

in accordance with Art. 32 GDPR

Description of the Technical and Organizational Security Measures taken by Visitor Analytics.

Visitor Analytics has implemented the following technical and organizational security measures to provide the on-going confidentiality, integrity, availability and resilience of processing systems and services:

1. Confidentiality

Visitor Analytics has implemented the following technical and organizational security to provide the confidentiality of processing systems and services, in particular:

1.1. Visitor Analytics Processes all Personal Use Data on servers solely located in the Republic of Germany owned and operated by industry leading cloud service providers that offer highly sophisticated measures to protect against unauthorized persons gaining access to data processing equipment (namely telephones, database and application servers and related hardware). Such measures include:

1.1.1. Data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders;

1.1.2. Access logs, activity records, and camera footage are available in case an incident occurs;

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

1.1.4. Documented distribution of keys to employees and colocation customers for colocation racks

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

1.2. Visitor Analytics implements suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished by:

1.2.1. Automatic detection of repeated or mass unauthorised access; Allowing access to Visitor Analytics App solely based on an encrypted key which can be decrypted only by Visitor Analytics through the means of 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. Visitor Analytics' employees entitled to use its data processing systems are only able to access Personal Data within the scope of and to the extent covered by their respective access permission (authorization). In particular, access rights and levels are based on employee job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. This is accomplished 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. Limited access to Personal Data to only authorized persons;

1.3.4. Industry standard encryption; and

1.3.5. Policies controlling the retention of backup copies.

2. Integrity

Visitor Analytics has implemented the following technical and organizational security to provide the integrity of processing systems and services, in particular:

2.1. Visitor Analytics implements suitable measures to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

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

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 issued laptops or other mobile devices.

2.2. Visitor Analytics does not access any Customer content except as necessary to provide Customer with the Visitor Analytics Services Customer has selected or to repair system faults. Visitor Analytics does not access Customers' content for any other purposes. Accordingly, Visitor Analytics does not know what content Customer choose to store on its systems and cannot distinguish between Personal Data and other content, so Visitor Analytics treats all Customer content the same. In this way, all Customer content benefits from the same robust Visitor Analytics security measures, whether this content includes Personal Data or not.

3. Availability

Visitor Analytics has implemented the following technical and organizational security measure to provide the availability of processing systems and services, in particular:

3.1. Visitor Analytics implements suitable measures to provide that Personal Data is protected from accidental destruction or loss. This is accomplished by:

3.1.1. Infrastructure redundancy;

3.1.2. Policies prohibiting permanent local (workstation) storage of Personal Data; and

3.1.3. Performing regular data backups.

4. Resilience

Visitors Analytics is using a thread-pooled web server for better performance to make sure that we can support a huge number of connections. Most of our project is based on a producer/consumer pattern to make sure that connections are closed as soon as possible to make resources available for pending connections. Also, our databases are backed-up to make sure that we can revert to an older version in case of unforeseen circumstances.

Also the servers setup processes are automatized (and except for databases, stateless) to make sure that we can recreate and start a new server in case something happens with the old instance.

Exhibit 3 - Sub Processors

Name of Subprocessor	Address	Function/Processing steps performed	What data is forwarded to the subprocessor?	Basis of data processing
Hetzner Online GmbH	Industriestraße 25 91710 Gunzenhausen Deutschland	Web Hosting provider	All the data related to website owners and their visitors is being stored in a database hosted at Hetzner.	Legitimate interest
rapidmail GmbH	Wentzingerstraße 21 79106 Freiburg i.Br. Deutschland	Email Provider	First name, last name and email address to send status reports and newsletters.	Legitimate interest
Digital1 Ventures Development SRL	Blvd. 21 Decembrie 1989, Nr. 72, 400124 Cluj-Napoca, Cluj, Romania	Subcontractor & infrastructure provider	Potential data is shared for implementation	Legitimate interest