Data Processing Addendum to the Bugfender Terms of Service

Last updated: February 14, 2020

This Data Processing Addendum ("DPA") is made as of the Effective Date by and between Beenario GmbH (“Bugfender”), and Customer, pursuant to the Bugfender Terms of Service for Bugfender offered as a service or Software License Agreement for Bugfender offered as Private Instance ("Agreement").

This DPA is supplemental to the Agreement and sets out the terms that apply when Personal Data is processed by Bugfender under the Agreement. The purpose of the DPA is to ensure such processing is conducted in accordance with applicable laws and with due respect for the rights and freedoms of individuals whose Personal Data are processed. Other capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement.

1. Definitions

1.1. For the purposes of this DPA:

a. “EEA" means the European Economic Area, which constitutes the member states of the European Union, the United Kingdom, Norway, Iceland and Liechtenstein.
b. “EU Data Protection Legislation” means Regulation 2016/679 of the European Parliament and of the Council 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of personal data and on the free movement of such data, and repealing Directive 95/46/EC (as amended, replaced or superseded) ("GDPR");
c. “Controller”, “Processor” and “Personal Data” have the meaning set out in the GPDR;
d. “CCPA” means the California Consumer Privacy Act Regulations.
e. “Service provider” has the meaning set out in the CCPA.
f. "Application Data" or “Data” means all data, regardless of format or owner, uploaded or provided by Customer to Beenario or identified to be uploaded to the Services, or in any other manner sent or transferred by Customer or on its behalf to Beenario or processed by Customer.

2. Object of DPA.

2.1. Scope. The subject-matter of the data processing is the provision of the Services under the Agreement with respect to the Application Data under the responsibility of the Customer and the processing will be carried out for the duration of the Agreement. Exhibit A sets out the nature, the type of Personal Data Bugfender processes and the categories of data subjects whose Personal Data is processed.

2.2. Compliance. Each party shall comply with all applicable laws relating to privacy and data protection, including, when applicable, the GDPR, the EU Privacy and Electronic Communications Directive (2002/58/EC) as implemented in each jurisdiction, and any amending or replacement legislation from time to time (collectively and individually, “Data Protection Laws”).

2.3. Purpose. This DPA will apply only to the extent that Bugfender processes Personal Data from the EEA on behalf of the Customer. The data processing performed by Bugfender in its capacity as Processor is carried out

for the sole purpose of providing the services contemplated in the Terms of Service, i.e. to ensure the proper functioning of the platform by users by providing the required support and customer support. Bugfender will process the Personal Data only for the purpose of providing the Services and in accordance with Controller's lawful instructions. If Bugfender is required to process the Personal Data for any other purpose by European Union or national law to which Bugfender is subject, Bugfender shall inform Customer of this requirement before the processing, except where otherwise required by such law.

2.4. Application. The parties agree that this DPA will only apply while Customer keeps a subscription with Bugfender, the subscription payments are fulfilled and such subscription is eligible for processing Personal Data.

3. Roles and responsibilities

3.1. Parties' Roles. To the extent that Bugfender processes Personal Data in the course of providing the Services in accordance with the requirements of the Agreement, Bugfender may access certain personal data under the responsibility of the Customer (as Controller), in particular (but without limitation), the data set out below ("Categories of personal data") relating to the indicate persons ("Data subjects"). Under applicable privacy regulations, the Customer is responsible for its data and is known under privacy regulation as the Data Controller. The Customer appoints Beenario as a Data Processor, to process Personal Data on Customer's behalf, for the purpose of providing the Service.

3.2. Rights and responsibilities of the Customer as Data Controller

As established in the GDPR and CCPA, the Customer as Data Controller shall:

a. Implement appropriate technical and organizational measures to ensure and be able to demonstrate that the processing is carried out in accordance with applicable legislation, especially in compliance with information obligations regarding the collection of personal information, not selling personal information, financial incentives and other requirements under applicable law.
b. Perform its own risk analysis and impact assessment, if applicable, when special categories of personal data have to be processed by Beenario, as a Data Processor, under this Agreement.
c. Adopt data protection policies.
d. Ensure that the Data Protection Officer or, in his / her absence, the Privacy Officer is involved in an adequate and timely manner in all matters relating to the protection of Client Personal Data.
e. Adhere to a code of conduct that can be approved by the Commission or other competent authority.
f. Keep a record of processing activities in the case of processing Client Personal Data that may pose a risk to the rights and freedoms of the data subject and / or in a non-occasional manner, or which involves the processing of special categories of data and / or data relating to convictions and infractions.
g. Make available to the interested parties the essential aspects of this agreement, at the request of the Data Processor.

3.3. Rights and responsibilities of Bugfender as the Data Processor

As established in the GDPR and CCPA, Bugfender, as Data Processor or Service provider, shall:

a. Process Customer Personal Data only on the basis of documented instructions from the Data Controller regarding to its business purposes, including transfers of Customer Personal Data to a third country or international organization, unless otherwise required to do so under applicable law; in such case, the Data Processor will inform the Data Controller of that legal requirement prior to the processing, unless otherwise prohibited by such law or in the public interest.
b. Ensure that the persons authorised to process Customer Personal Data have undertaken to respect confidentiality or are subject to an obligation of confidentiality of a statutory nature.
c. Take all appropriate technical and organisational measures to ensure a level of safety appropriate to the risk of processing.
d. Respect the conditions for having recourse to another Data Processor, as established in the current legislation on protection of Customer Personal Data.
e. Assist the Data Controller, taking into account the nature of the processing, through appropriate technical and organisational measures, whenever possible, so that it can comply with its obligation to respond to requests for the exercise of the rights of the data subjects.
f. Assist the Data Controller in ensuring that they comply with their obligations, taking into account the nature of the processing and the information that is available to the Data Processor.
g. At the choice of the Data Controller, either destroy or return all Customer Personal Data once the processing services have been completed, and destroy any existing copies unless the retention of Customer Personal Data is required under Union or applicable Member State law.
h. Make available to the Data Controller all information necessary to demonstrate compliance with the obligations established in herein, as well as to allow and contribute to the performance of audits, including inspections, by the controller or other authorised auditors for the Data Controller.
i. Process the Customer Personal Data placed at the disposal of the Data Processor in a way that ensures that the personnel in charge follow the instructions of the Data Controller.
j. Ensure that the Data Protection Officer or, in his / her absence, the Privacy Officer is involved in an adequate and timely manner in all matters relating to the protection of Customer Personal Data.
k. Adhere to a Code of Conduct that is approved by the Commission or other competent authority.
l. keep a record of processing activities in the case of processing Customer Personal Data that may pose a risk to the rights and freedoms of the data subject and / or in a non-occasional manner, or which involves the processing of special categories of data and / or data relating to convictions and infractions.

Bugfender certifies that it understand its contractual restrictions instructed by the Data Controller and will comply with them, including the obligations stated in the CCPA, and any other applicable regulation, such as:

- Do not sell the personal information.
- Do not retain, use, or disclose the Personal Information for any purpose other than providing the services specified in the Agreement. Specifically, Vendor shall not retain, use, or disclose the Personal Information for a Commercial Purpose.
- Do not retain, use, or disclose the Personal Information outside of the direct business relationship between the person and Looker.

4. Security

4.1. Bugfender will have in place and maintain throughout the term of this Agreement appropriate technical and organizational measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing (a “Security Incident”).

4.2. Upon becoming aware of a Security Incident, Bugfender shall notify Customer without undue delay and shall provide such timely information as Customer may reasonably require, including to enable Customer to fulfil any data breach reporting obligations under EU Data Protection Legislation. Bugfender shall promptly take appropriate steps to remedy or mitigate any damage arising from such Security Incident.

4.3. Bugfender will ensure that any person that it authorizes to process the Personal Data (including its staff, agents and subcontractors) shall be subject to a duty of confidentiality (whether a contractual or a statutory duty).

4.4. Customer deems the security measures indicated in Exhibit B as sufficient for the categories of data being processed.

5. Subprocessing

5.1. Customer agrees that Bugfender may engage Bugfender affiliates and third-party sub-processors (collectively, "Sub-processors") to process the Personal Data on Bugfender’s behalf. A list of sub-processors who have been authorized by the Customer are indicated in Exhibit C.

5.2. Bugfender shall impose on such Sub-processors data protection obligations that protect the Personal Data to the same or substantially similar standard provided for by this DPA and shall remain liable for any breach of the DPA caused by a Sub-processor.

5.3. Bugfender may, by giving reasonable notice to the Customer, add or make changes to the Sub-processors. If the Customer objects to the appointment of an additional Sub-processor within thirty (30) calendar days of such notice on reasonable grounds relating to the protection of the Personal Data, then Bugfender will work in good faith with the Customer to find an alternative solution.

6. International transfers

6.1. Bugfender may transfer Personal Data outside the EEA to its subprocessors indicated in Exhibit C below, who have entered into contract with Bugfender with appropriate contractual safeguards. These Sub-processors established in other countries, including the USA, indicated in the table below are approved by the Customer.

7. Exercise of rights by data subject

7.1. If a Data Subject addresses any request or exercises any of the rights established in the current Personal Data Protection regulations to Bugfender, Bugfender shall notify the Customer as Data Controller and will provide all reasonable support to provide the data subject with the information on the actions requested and carried out, without delay and at the latest within one month from the receipt of the request, which may be

extended by a maximum of another two months if necessary, taking into account the complexity of the request and the number of requests.

7.2. If Customer does not act on the request of the person concerned, Bugfender may inform the Data Subject without delay, and at the latest within one month of receipt of the request, of the reasons for not acting and of the possibility of making a complaint to a supervisory authority and of taking legal action.

8. Audit

8.1. Whilst it is the parties' intention ordinarily to rely on the provision of the documentation to verify Bugfender's compliance with this DPA, Bugfender shall permit the Customer (or its appointed third party auditors) to carry out an audit of Bugfender processing of Personal Data under the Agreement following a Security Incident suffered by Bugfender, or upon the instruction of a data protection authority.

8.2. Customer must give Bugfender reasonable prior notice of such intention to audit, conduct its audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to Bugfender's operations. Any such audit shall be subject to Bugfender's security and confidentiality terms and guidelines.

9. Miscellaneous

9.1. Except as amended by this DPA, the Agreement will remain in full force and effect.

9.2. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control.

9.3. Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

9.4. Customer acknowledges that Bugfender may disclose the privacy provisions in the Agreement to the European data protection authority, or any other EU judicial or regulatory body upon their lawful request.

10. Termination, resolution and expiration

In the event of termination, resolution or expiration of the Agreement, the Data Processor shall not keep the Customer Personal Data unless otherwise legally required to do so. Otherwise, upon termination, resolution or expiration, or when no longer legally required to keep the data, the Data Processor shall destroy or return to the Data Controller all Client Personal Data and any copies of it, as well as any support or other document containing any Client Personal Data.

Bugfender	The Client
…….	…….
Name:	Name:
Position:	Position:
Date:	Date:
	Bugfender account ID:

Exhibit A – Data Processing details

Last updated: February 14th, 2020

Data subjects

The personal data transferred concern the following categories of data subjects:

- Application Users – individuals who interact with the applications where Customer installed the Bugfender SDK.

Processing operations

Bugfender service consists primarily of storing application logs and making them available online on behalf of the Customer.

Bugfender captures some additional data, such as the details of the device running such application or the location of the Application Users. Bugfender makes it easy to find the logs of a specific user by allowing the Customer to tag the devices of a specific Application Users.

The contents of those logs are determined primarily by the Customer in its sole discretion and responsibility. If Customer makes available any personal data not strictly necessary for the provision of the Services, Bugfender shall return it immediately to the Customer, and Customer assume all responsibilities for this action.

Bugfender also provides other services on the data, such as search and analytics on the Customer's behalf.

Categories of data

The personal data transferred concern the following categories of data:

- Device name where the application is running, which might contain the Application Users' name.
- IP address and/or location of the Application Users.
- Device associated data, which might contain personal data to the discretion of Customer.
- Application logs, which might contain personal data to the discretion of Customer.

Special categories of data

Customer explicitly agrees not to use the service for any of the Special categories defined in GDPR.

Exhibit B – Bugfender Security Measures

Last updated: February 14th, 2020

Network-level Controls

- Bugfender will use firewalls to protect the hosts/infrastructure handling Personal Data
- Bugfender will encrypt communications on public networks
- Bugfender will use strong encryption (TLS) for transmission of Personal Data that is considered Personal Data.

Host Level Controls

- Bugfender will implement operating system hardening including at least: strong password authentication/use of keys, inactivity time-out, disabling or removal of unused or expired accounts and services, turning off unused ports, and log management.
- Bugfender will perform patch management on systems that host or handle Personal Data. Bugfender will implement critical patches within vendor recommended time frames on systems that host or handle Personal Data, not to exceed 30 days after the patch is identified.
- Bugfender will implement access control processes and restrict access to operating system configurations based on the least privilege principle.
- Bugfender will implement specific controls to log activities of users with elevated access to systems that host or handle Personal Data.
- Physical servers will be protected with appropriate physical security mechanisms, including but not limited to badged access, locked cages, secure perimeter, cameras, alarms, and enforced user provisioning controls.

Application Level Controls

- Bugfender will employ secure programming guidelines and protocols in the development of applications processing or handling Personal Data.
- Bugfender will regularly perform patch management on applications that host or handle Personal Data. Bugfender will implement critical patches within vendor recommended time frames on all applications that host or handle Personal Data, not to exceed 30 days.
- Bugfender will employ change management standards for applications hosting or handling Personal Data.
- Bugfender will implement access control processes and restrict access based on the least privilege principle.
- Bugfender will perform backups of the Personal Data at least daily.

Exhibit C – Bugfender Subprocessors

Last updated: February 14th, 2020

The following entities are subcontracted by Bugfender to process your data:

Entity Name	Location	Processing activities
Amazon Web Services EMEA SARL	Luxembourg	Hosting
Brutalsys S.L.	Spain	Hosting and system administration
Google Ireland Limited	Ireland	Productivity and communication tools
Inspectlet	USA	Customer support tools
Intercom R&D Unlimited Company	Ireland	Customer support tools
SendGrid, Inc.	USA	Communication tools
Wasabi Technologies, Inc.	USA, with servers in Netherlands	Hosting
Zemantics OÜ	Estonia	Customer support and development services