webtrends®

WEBTRENDS
DATA PROTECTION ADDENDUM

Effective Date: May 25, 2018

This Data Protection Addendum ("**Addendum**") is entered into by and between Webtrends, Inc., by and on behalf of itself and its subsidiaries ("Webtrends") and Client. This Addendum sets out terms that will apply to Webtrends' Processing of Client Data subject to the European Union General Data Protection Regulation ("GDPR") on and after this Addendum has been properly executed in accordance with the terms set forth herein. This Addendum, together with the existing Terms of Subscription Service, as may have been amended ("Agreement") reflects the parties' agreement related to Processing of Client Data, including Personal Data, in accordance with the GDPR.

Executing this Addendum
This Addendum has been signed by Webtrends. In order to make this Addendum effective, it must be completed by Client by inserting the relevant information on Page 4, scanning and emailing to dpa@webtrends.com. Upon receipt of a validly completed Addendum to the email address indicated, the Addendum will become legally binding.

1. DEFINITIONS AND INTERPRETATIONS

1.1. Definitions – Capitalized terms not defined in this Addendum shall have the meaning as defined in the Agreement.

a) "**Adequate Country**" means a country which is deemed adequate by the European Commission under Article 25(6) of Directive 95/46/EC or Article 45 of GDPR.
b) "**Agreement**" means the terms of subscription service incorporated in a Quote, or the master subscription agreement between Webtrends and Client.
c) "**Data Controller**" means the party that determines the purposes and means of the Processing of Personal Data.
d) "**Data Processor**" means the party that Processes Personal Data on behalf of, or under the instruction of, the Data Controller.
e) "**Data Protection Authority**" means the competent body in the relevant jurisdiction charged with enforcement of applicable Law.
f) "**Data Subject**" means the identified or identifiable person who is the subject of Personal Data.
g) "**EEA**" means the European Economic Area and shall be deemed to include Switzerland.
h) "**GDPR**" means European Union Regulation (EU) 2016/679.
i) References to "**instructions**" or "**written instructions**" and related terms mean Data Controller's written instructions for Processing of Client Data, which consist of (1) the terms of the Agreement and this Addendum, and (2) Processing enabled by Data Controller through the Solutions.
j) "**Law(s)**" means, with respect to a party, all privacy, data protection, data transfer, information security-related and other laws and regulations applicable to such party, including without limitation the GDPR.
k) "**Model Contracts**" means the Standard Contractual Clauses for Processors as approved by the European Commission under Decision 2010/87/EU, in the form provided by Webtrends and executed by the parties.
l) "**Processing**" means any operation or set of operations which is performed upon Client Data by the Solutions, as further described in **Annex A**.
m) "**Personal Data**" means any information included in the Client Data relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as identification number location data, an online identifier or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Client acknowledges and agrees that in no event will Personal Data include Prohibited Data.
n) "**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data in Data Processor's control.
o) "**Solutions**" means the specific online software-as-a-service products ordered by Client as identified on the applicable Quote. The term "Solutions" includes the related Tagging Methods and Documentation (but excludes Professional Services).
p) "**Subprocessor**" means any third party processor engaged by Data Processor or its affiliates to assist in fulfilling its processing obligations with respect to providing the Solutions pursuant to the Agreement or this Addendum. Third Party Platforms shall not be deemed Subprocessors.

q) "**Third Party**" shall mean any natural or legal person, public authority, agency or any other body other than the Data Subject, Data Controller, Data Processor, or Subprocessors or other persons who, under the direct authority of the Data Controller or Data Processor, are authorized to Process the Client Data.

1.2 Interpretation - In this Agreement, the words "including" and "in particular" and any similar words or expressions are by way of illustration and emphasis only and do not operate to limit the generality or extent of any other words or expressions. Further, headings in this Agreement are for convenience only and do not affect its interpretation.

2. PROCESSING

2.1. Client will act as the Data Controller and Webtrends will act as the Data Processor in connection with the Solutions. Both the Data Controller and Data Processor shall be subject to applicable Law in the carrying out of their respective responsibilities as set forth in this Addendum.

2.2. Data Controller retains all ownership rights in the Client Data, as set forth in the Agreement. Except as expressly authorized by Data Controller or as instructed by the Data Controller in writing, Data Processor shall have no right directly or indirectly to sell, rent, lease, combine, display, perform, modify, transfer or disclose the Client Data or any derivative work. Notwithstanding the foregoing, Data Controller acknowledges that Data Processor shall have a right to use Client Data for the purpose of providing the Solutions to Client and as otherwise set forth in the Agreement.

2.3. Data Processor shall act only in accordance with Data Controller's instructions regarding the Processing of the Client Data which are more fully set forth in the Agreement. In the event that Data Processor reasonably believes it cannot follow an instruction issued by Data Controller due to applicable Law, Data Processor will promptly inform Data Controller and the parties will cooperate in good faith to resolve the conflict. Data Processor shall be excused from performance of the Solutions to the extent of the conflict and until the conflict can be resolved.

2.4. Additional instructions require prior written agreement of the parties, including agreement on any additional fees payable by Data Controller.

2.5. Data Processor shall not disclose the Client Data to any Third Party than in compliance with the Agreement, in compliance with Data Controller's instructions, or in compliance with an independent legal obligation requiring disclosure. Data Processor shall inform Data Controller in writing prior to making any such legally required disclosure, to the extent permitted by Law.

2.6. For clarity, nothing in this Addendum prevents Data Processor from transmitting Client Data (including without limitation Personal Data) as instructed by Data Controller through the Solutions, including without limitation to Third Party Platforms. The parties agree that such Third Party Platforms are not considered Subprocessors of Data Processor and Data Processor shall have no responsibility or liability associated with Data Controller's election to use such Third Party Platforms.

3. SUBPROCESSING

3.1. Data Processor's obligations under this Addendum shall apply to Data Processor's employees, agents, and Subprocessors who may have access to the Personal Data.

3.2. Data Controller agrees that Data Processor is authorized to use Subprocessors (including without limitation cloud infrastructure providers) to Process the Personal Data, provided that Data Processor (i) ensures that any Subprocessor is bound by data protection obligations substantially similar to this Addendum and (ii) remains liable for their compliance with this Addendum as if they were Data Processor. The Subprocessors currently engaged by Data Processor are listed in **Annex C**.

3.3. Data Processor shall (i) provide an up-to-date list of the Subprocessors that it has appointed upon written request from Data Controller; and (ii) notify Data Controller (email sufficient) if it adds or removes Subprocessors at least ten (10) days prior to any such changes. Data Controller may object in writing to Data Processor's appointment of a new Subprocessor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. Any such notice shall be provided via Webtrends' client portal located at https://my.webtrends.com, Webtrends' RSS feed, or other reasonable means.

4. SECURITY

4.1. Data Processor shall implement and maintain appropriate technical and organizational security measures to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Personal Data, in accordance with Data Processor's security standards described in **Annex B** ("**Solutions Security**").

4.2. Data Controller is responsible for reviewing the information made available by Data Processor relating to data security and making an independent determination as to whether the Solutions Security meets Data Controller's requirements and legal obligations under applicable Laws. Data Controller acknowledges that the measures used for Solutions Security are subject to technical progress and that Data Processor may update or modify these measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Solutions.

4.3. Data Processor shall ensure that any person who is authorized by Data Controller to process Personal Data (including its employees, agents, and Subprocessors) shall be under an appropriate contractual or statutory obligation of confidentiality.

4.4. Upon becoming aware of a Security Incident, Data Processor shall notify Data Controller without undue delay and will provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Data Controller. Data Processor shall promptly take reasonable steps to mitigate and, where possible, to remedy the effects of, any Security Incident.

5. ONWARD TRANSFER

5.1. U.S.-EU Privacy Shield Self-Certification. Webtrends self-certifies that: (i) it complies with the U.S.-EU Privacy Shield principles and meets the requirements of the U.S.-EU Privacy Shield framework; and (ii) all Client Data transferred from the EU to the U.S. will be processed in accordance with those requirements. Webtrends' Privacy Statement provides further information.

5.2. U.S.-Swiss Privacy Shield Self-Certification. Webtrends self-certifies that: (i) it complies with the U.S.-Swiss Privacy Shield principles and meets the requirements of the U.S.-Swiss Privacy Shield framework; and (ii) all Client Data transferred from Switzerland to the U.S. will be processed in accordance with those requirements. Webtrends' Privacy Statement provides further information.

6. REGULATORY COMPLIANCE

6.1. At Data Controller's request and expense, Data Processor shall reasonably assist Data Controller as necessary to meet its obligations to regulatory authorities, including Data Protection Authorities.

6.2. At Data Controller's request and expense, Data Processor shall reasonably assist Data Controller to respond to requests from individuals in relation to their rights of data access, rectification, erasure, restriction, portability and objection. In the event that any such request is made directly to Data Processor, Data Processor shall not respond to such communication directly without Data Controller's prior authorization, other than to acknowledge receipt of the request, unless required by applicable Laws.

6.3. To the extent Data Processor is required under Laws, at Data Controller's request and expense, Data Processor shall provide reasonably requested information regarding the Solutions to enable Data Controller to carry out data protection impact assessments or prior consultations with Data Protection Authorities.

7. REVIEWS OF DATA PROCESSING

This Section is only applicable if Client does not have a right to a security audit under the terms of the Agreement or, if entered into by the parties, the Model Clauses.

7.1. At Data Controller's request, Data Processor shall provide Data Controller with reasonable information regarding Data Processor's facilities, systems, and security procedures relevant to the Processing of Personal Data under this Addendum, solely for Data Controller's review of Data Processor's compliance with this Addendum.

7.2. Data Processor will provide such information within fifteen (15) business days of Data Controller's written request, unless shorter notice is required by Data Controller's regulatory authorities.

7.3. If Data Controller wishes that Data Processor provide Third Parties with access or information regarding Client Data management, such a request will be made to Data Processor in writing and will waive Data Processor's confidentiality obligations under the Agreement with respect to such information. Where appropriate, any such Third Party may be required to enter into an agreement to maintain the confidentiality of the information shared by Data Processor.

7.4. At Data Controller's request, Data Processor agrees to allow Data Controller to perform an onsite audit of Data Processor as follows:

During Data Processor's regular business hours, but not any more frequently than once a year, Data Controller may, at its sole expense, perform a confidential audit to confirm Data Processor's compliance with this Addendum. Any onsite audit shall be conducted on a mutually agreed upon date, which shall not be sooner than thirty (30) calendar days after Data Processor's receipt of Data Controller's written request for such audit. Such audits shall be limited to the security systems as they pertain to the Solutions. The onsite portion of the audit shall not exceed a cumulative four (4) hours at Data Processor's facilities. If the audit shall exceed such four (4) hour period, Data Controller shall be responsible for payment of professional services fees to Data Processor at the current hourly rate for professional services. If the audit is to be performed by a third party on Data Controller's behalf, such third party shall (i) not be a direct or indirect competitor of Data Processor, and (ii) execute a confidentiality and non-disclosure agreement as presented by and for the benefit of Data Processor. Upon completion of the audit, Data Controller shall promptly provide Data Processor a summary of the findings from each report prepared in connection with any such audit and discuss results, including any remediation plans. Data Processor agrees to work with Data Controller to identify reasonable remediation actions and to promptly take action at Data Processor's expense to correct those matters or items upon which Data Processor and Data Controller mutually agree are identified in any such audit that require correction.

7.5 Any information provided by Data Processor under this Section constitutes Data Processor's Confidential Information under the Agreement.

8. GENERAL; TERMINATION

8.1. This Addendum forms part of the Agreement and all activities under this Addendum (including without limitation Processing of Personal Data) remain subject to the applicable limitations of liability set forth in the Agreement.

8.2. Data Controller agrees that any regulatory fines or penalties incurred by Data Processor in relation to the Client Data that arise as a result of, or in connection with, Data Controller's failure to comply with its obligations under this Addendum or any applicable Laws shall count toward and reduce Data Processor's liability under the Agreement as if it were liability to Data Controller under the Agreement.

8.3. If and to the extent language in this Addendum conflicts with the Agreement, this Addendum shall control.

8.4. This Addendum will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Laws.

8.5. This Addendum (and Model Contracts, if executed by the parties) will automatically terminate upon expiration or termination of the Agreement.

8.6. Data Processor shall, within ninety (90) days after request by Data Controller at the termination or expiration of the Agreement, Erase the Personal Data from Data Processor's systems. Within a reasonable period following deletion, at Data Controller's request, Data Processor will provide written confirmation that Data Processor's obligations with regard to Erasure have been fulfilled.

8.7. Notwithstanding the foregoing, Data Controller understands that Data Processor may retain Client Data as required by Laws, which Client Data will remain subject to the requirements of this Addendum.

Accepted and agreed to as of the date of Client's signature below by the authorized representative of each party:

_____("CLIENT")	**WEBTRENDS INC. ("WEBTRENDS")**
Address:	555 SW Oak Street, Suite 300 Portland, OR 97204
	Michael J Laber Michael J. Laber (Mar 22, 2018)
Signature	Signature
	Michael J. Laber
Print Name	Print Name
	CEO
Title	Title
	mike.laber@webtrends.com
Email	Email
	3/22/2018
Date	Date

webtrends®

Annex A - Details of Processing

Data exporter
The data exporter is: Client, which uses the Solutions to track visitors to Client Applications for analysis, reporting, testing and targeting.

Data importer
The data importer is: Webtrends Inc., which is the parent entity of WT EMEA Acquisitions Limited and Webtrends Nordic AB. Webtrends Inc. produces and operates the Solutions and the software-as-a-service infrastructure, and provides technical support to Client and its users of the Solution pursuant to the applicable Quote and Agreement as the designated processor. Webtrends is the distributor of the Solutions and provider of services related to the Solutions in the Client's territory and the contracting party to the Quote and the Agreement.

Data subjects
The personal data transferred concern the following categories of data subjects: Data subjects include visitors to the Client Applications, and Client's employees who use the Solutions or support contract governance.

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

- Personal data collected from Client Applications are: IP address, cookie visitor ID and, if Client purchases Webtrends Analytics for Sharepoint or Webtrends Infinity Analytics for Sharepoint, the Sharepoint ID.

- Client determines any additional categories of data collected by the Solution subject to the restrictions set forth in the Quote and the Agreement between the parties. Client's data fields can be configured as part of the implementation or in ongoing Tagging Method updates on Client Applications.

- Name, email address, business phone number of data exporter employees who use the Solutions or support contract governance.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data: Not applicable.

Processing operations
The personal data transferred will be subject to the following basic processing activities:

- use of personal data to provide the Solutions and to provide assistance and technical support;

- storage of personal data in dedicated Solution data centers in a multi-tenant architecture;

- back-up of personal data and storage of back-up in a secure location;

- computer processing of personal data, including data transmission, data retrieval, data access; and

- processing for governance of the Agreement.

webtrends®

Annex B – Security Measures

Security Control	Measures Adopted by Webtrends
Admittance control (Physical access control) Physical access control means to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data.	Access to data centers is controlled by formal procedures. Access is restricted to persons authorized by Webtrends SaaS Operations Director. All persons requesting access must identify themselves to the facility's security personnel. Visitor records are kept. Each data center follows industry best practices with regards to security measures and access procedures, such as using electronic access control systems, alarm systems, indoor- and outdoor-cameras and security personnel.
System access control Access control is the prevention of data processing systems from being used without authorization.	Authentication processes are implemented to control access to Webtrends production systems. Access restrictions are managed via a commercial authentication system. Access to internal support-tools is restricted to authorized persons by means of Access Control Lists (ACL). Remote access to Webtrends production network requires prior login through Webtrends over a secure VPN connection. All authentication information is encrypted during transmission over public network. Webtrends follows a formal process to authorize or deny access to Webtrends SaaS Solutions production resources. Accesses to Webtrends production network are revoked immediately in case of termination. Unique user-ID, strong passwords and periodic review of access logs ensure appropriate use of user accounts. All accesses to Webtrends production network are subject to regular verifications. Routers configuration protect Webtrends production network against unauthorized external connections and violation of Webtrends logical access policy. Webtrends maintains and follows formal change management processes. All changes to the production environment (network, systems, platform, application, configuration, etc.) are implemented by a dedicated team. All key business owners such as Support, Engineering, DevOps, Security, SaaS Operations are represented at the change management meeting.

	Webtrends employs properly configured stateful firewalls with access controls between all network subnets and between Webtrends' networks and any untrusted network.
Data access control Access control is to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording.	Access rights are granted based on job-responsibilities or need-to-know-basis and must be authorized by Webtrends SaaS Operations Director. Webtrends clients (data controllers) can adjust their security options via administration settings only accessible to admin users. Webtrends clients (data controllers) control all roles and rights associated with users granted access to their accounts.
Disclosure control Disclosure control means that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities.	All accesses to Webtrends SaaS Solutions UIs are performed over secure protocols (such as HTTPS and SFTP). All accesses to the Webtrends SaaS Solutions and key security events are logged and this information is accessible to administrators for review.
Input control Input control is to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom.	Transmission of personal data is controlled through data configuration mechanisms by Webtrends clients (data controllers). All collected data (including personal data) are identified by a unique DCSID associated with a specific client. Access to collected personal data is controlled by access control mechanisms (authentication, authorization). Collected data cannot be modified or deleted by clients. Any access, change, or deletion of data (including personal data) within Webtrends SaaS Solutions production network is logged.
Job control Job control is to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions.	Webtrends clients control what data is collected by providing the necessary Instructions within the data collection mechanism. Webtrends further provides clients with administration functions within the SaaS Solutions' UI to control which reports (processed data) are created. Webtrends SaaS Solutions provides clients (data controllers) with user management functionality allowing them to control who may access their accounts and what roles and rights users have.
Availability control Availability control is to ensure that personal data are protected against accidental destruction or loss.	Webtrends adopts the following measures to ensure that personal data are protected against accidental destruction or loss: Webtrends uses a redundant data collection infrastructure to protect client data against loss during the data collection process. Webtrends further uses industry security best practices to secure its infrastructure against data destruction and loss, and implements data backup mechanisms to protect and recover client data.

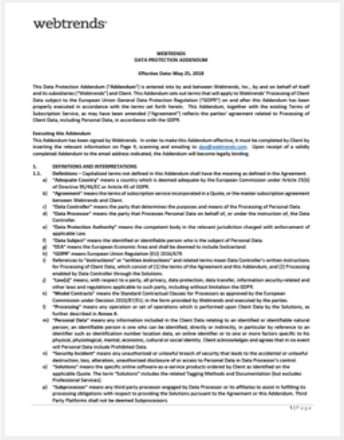
Separation control (Checking the intended use) Separation control is to ensure that data collected for different purposes can be processed separately.	All collected data (including personal data) are identified by a unique DCSID associated with a specific client. Processing of all client data (including personal data) is performed in Webtrends SaaS Solutions production network, physically and logically separated from Webtrends corporate network. All data processing is performed solely on behalf and under the Instructions of the data controller.

webtrends®

Annex C - List of Data Processor Subprocessors

Data Processor uses a range of Subprocessors to assist it in providing the Solutions:

Entity Name	Location
Amazon, Inc. Amazon Web Services (AWS) Privacy Shield Certified	P.O. Box 81226 Seattle, WA 98108-1226 www.aws.amazon.com



webtrends

WEBTRENDS
DATA PROTECTION ADDENDUM

Effective Date: May 25, 2018

Webtrends Data Protection Addendum

Adobe Sign Document History 03/22/2018

Created:	03/21/2018
By:	Ashley Spencer (ashley.spencer@webtrends.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAgKw3dbnlwZdfuQ_X4Tipef9WFZb7DrcP

"Webtrends Data Protection Addendum" History

Document uploaded by Ashley Spencer (ashley.spencer@webtrends.com) from Acrobat
03/21/2018 - 4:29:10 PM PDT- IP address: 216.64.169.10

Document emailed to Michael J. Laber (mike.laber@webtrends.com) for signature
03/21/2018 - 4:31:06 PM PDT

Document viewed by Michael J. Laber (mike.laber@webtrends.com)
03/22/2018 - 8:49:26 AM PDT- IP address: 216.64.169.10

Document e-signed by Michael J. Laber (mike.laber@webtrends.com)
Signature Date: 03/22/2018 - 8:51:57 AM PDT - Time Source: server- IP address: 216.64.169.10