WEBTRENDS
DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**Addendum**") is entered into by and between Webtrends, Inc., by and on behalf of itself and its subsidiaries (collectively, "**Webtrends**") and Client. This Addendum, effective as of the date of the last signature below, sets out the parties' agreement with respect to Webtrends' Processing of Personal Data subject to Applicable Data Protection Law, 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 be updated from time to time (collectively, "**Agreement**"), reflects the parties' entire agreement related to Processing of Personal Data and supersedes any previous Data Protection Addendum between the parties.

Executing this Addendum
This Addendum has been signed by Webtrends. To make this Addendum effective and binding, Client must insert the relevant information on Pages 5 and 25, sign, and then scan and email the completed/signed Addendum to legal@webtrends.com. Upon Webtrends' receipt of a validly completed and signed Addendum, the Addendum will become legally binding on the parties.

1. DEFINITIONS AND INTERPRETATIONS

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

a) "**Adequate Country**" means a country which is deemed adequate by the European Commission (e.g., under Article 45 of the GDPR).

b) "**Applicable Data Protection Law**" means, with respect to a party, all privacy, data protection, data transfer, information security-related and other laws and regulations applicable to such party, in respect to the Processing of Personal Data, including without limitation the GDPR and CCPA (both as defined below).

c) "**Agreement**" means the terms of subscription service incorporated in a Quote, or the master subscription agreement between Webtrends and Client.

d) "**CCPA**" means the California Consumer Privacy Act, California Civil Code Section 1798.100, et seq., and its implementing regulations.

e) "**Data Controller**" means the party that determines the purposes and means of the Processing of Personal Data, including as applicable a "business" as that term is defined under the CCPA.

f) "**Data Processor**" means the party that Processes Personal Data on behalf of, or under the instruction of, the Data Controller, including as applicable a "service provider" as that term is defined by the CCPA.

g) "**Data Protection Authority**" means the competent body in the relevant jurisdiction charged with enforcement of Applicable Data Protection Law.

h) "**Data Subject**" means the identified or identifiable person who is the subject of Personal Data, including as applicable a "consumer" as that term is defined by the CCPA and, with regard to the FADP (as defined below), legal entities (until the entry into force of the revised FADP).

i) "**EEA**" means the European Economic Area and will be deemed to include Switzerland.

j) "**GDPR**" means the General Data Protection Regulation, (EU) 2016/679, and—as used in this Addendum—includes the UK-GDPR (with regard to the United Kingdom), and the Federal Act on Data Protection or "FADP" (with regard to Switzerland).

k) References to "**instructions**" or "**written instructions**" and related terms mean Data Controller's written instructions for Processing of Personal Data (as that term is defined in the Agreement), which consist of (1) the terms of the Agreement and this Addendum, and (2) Processing enabled by Data Controller through the Solutions.

l) "**Model Clauses**" means the Standard Contractual Clauses for Controller-to-Processor transfers, applicable to Personal Data from the EEA and Switzerland, as approved by the European Commission under Decision (EU) 2021/914, in the form provided by Webtrends and attached hereto as **Annex D** and executed by the parties. To the extent necessary for compliance with transfers from Switzerland, the parties agree that the Model Clauses are amended to provide for supervision by the Swiss Federal Data

Protection and Information Commissioner ("FDPIC"), and the term "member state" will not be interpreted in such a way as to exclude Swiss data subjects from the possibility of enforcing their rights in Switzerland.

m) "**Processing**" means:
   i) Any operation or set of operations which is performed upon Client Data (as defined in the Agreement) by the Solutions, as further described in **Annex A**; and
   ii) Any access, collection, use, or disclosure of Personal Data by Webtrends when it is providing Professional Services. For the avoidance of doubt, Webtrends "Processes" Client Data and Personal Data when it is engaged in Processing activities.

n) "**Personal Data**" means any information included in the Client Data or processed by Data Processor in connection with the provision of Professional Services, in each case to the extent it relates to an identified or identifiable natural person or their household (collectively, "identifiable person"); an identifiable person is one who can be identified, associated with, or reasonably linked, directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, address (IP, email, or physical), an online identifier, or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity. Client acknowledges and agrees that in no event will it allow Personal Data to include Prohibited Data.

o) "**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.

p) "**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).

q) "**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 or Professional Services pursuant to the Agreement or this Addendum. Third Party Platforms will not be deemed Subprocessors.

r) "**Third Party**" means 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, Data Processor, or Subprocessors, are authorized to Process the Personal Data.

1.2 **Interpretation –** In this Addendum, 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 Addendum 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 and Professional Services. Both the Data Controller and Data Processor will be subject to Applicable Data Protection Law in the carrying out of their respective responsibilities as set forth in this Addendum. Data Processor is generally unable, however, to determine where Data Subjects are located or whether Data Controller is subject to particular laws; accordingly, Data Controller must notify Data Processor if the Personal Data is subject to any Applicable Data Protection Law other than the CCPA or GDPR so the parties can take steps to enter into additional contractual provisions (if any) necessary to comply with such Law.

2.2. Data Controller retains all ownership rights in Personal Data, including 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 will not sell, rent, lease, combine, display, perform, modify, transfer, or disclose the Personal Data. Notwithstanding the foregoing, Data Controller acknowledges that Data Processor will have a right to use Personal Data for the purpose of providing the Solutions and Professional Services to Client and as otherwise set forth in the Agreement.

2.3. Data Processor will act only in accordance with Data Controller's instructions regarding the Processing of Personal Data which are more fully set forth in the Agreement. If Data Processor reasonably believes it cannot follow an instruction issued by Data Controller due to the Agreement or Applicable Data Protection Law, Data

Processor will promptly inform Data Controller and the parties will cooperate in good faith to resolve the conflict. Data Processor will be excused from performance of the Solutions and Professional Services 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 will not disclose Personal Data to any Third Party other 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 will inform Data Controller in writing before making any such legally required disclosure, to the extent prior notification is permitted by Applicable Data Protection Law.

2.6. For clarity, nothing in this Addendum prevents Data Processor from transmitting 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 will have no responsibility or liability associated with Data Controller's election to use such Third Party Platforms.

2.7. The parties acknowledge that Data Processor is deemed a "service provider" as defined under CCPA. Further, Data Processor's processing of any Personal Data is necessary for Data Processor to deliver the Solutions and Professional Services and Data Controller will not receive any monetary or other valuable consideration from Data Processor in exchange for Data Processor's access to and processing of Personal Data in accordance with the Agreement.

3. SUBPROCESSING

3.1. Data Processor's obligations under this Addendum will 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, including restrictions on use and sale of any Personal Data 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 B**.

3.3. Data Processor will (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 is sufficient) if it adds or removes Subprocessors at least ten (10) days before 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.

4. SECURITY

4.1. Data Processor will 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 C** ("**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 Data Protection Law. Data Controller acknowledges that these measures 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 a material degradation of the overall security regarding Personal Data.

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

4.4. Upon becoming aware of a Security Incident, Data Processor will 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 will promptly take reasonable steps to mitigate and, where possible, to remedy the effects of, any Security Incident; provided that the responsibility, costs, and expenses associated with mitigation and remediation will be the responsibility of Data Controller if the Security Incident arises out of any actions or omissions of Data Controller or any of its employees, agents, or subcontractors.

5. ONWARD TRANSFER

On July 16, 2020, the Court of Justice of the European Union invalidated transfers of personal data from the EU to the U.S. under the EU-U.S. Privacy Shield framework. On September 8, 2020, the FDPIC released a position statement stating that the Swiss-U.S. Privacy Shield framework did not provide adequate protection. Before this ruling, Webtrends certified its compliance with both the EU-U.S. and Swiss-U.S. Privacy Shield frameworks (the "Frameworks"). Any Personal Data transferred to Webtrends in its capacity as a Data Processor under the Frameworks will be maintained in accordance with the Privacy Shield Principles (as required by the Frameworks). Beginning on July 17, 2020, Personal Data transferred to Webtrends from the EEA is received and processed in accordance with the Model Clauses. If a data-transfer mechanism being used by the parties is subsequently modified, revoked, or held by a competent regulator or other governmental authority to be invalid, or if another jurisdiction applicable to the parties' relationship subsequently requires a transfer mechanism (e.g., the United Kingdom), Data Controller and Webtrends will cooperate in good faith to—as applicable—terminate the transfers being done under that mechanism or pursue a suitable alternate mechanism with a view to seamlessly transition to a suitable alternate mechanism.

6. REGULATORY COMPLIANCE

6.1. At Data Controller's request and expense, Data Processor will 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 will reasonably assist Data Controller to respond to requests from individuals in relation to their rights (e.g., as applicable, rights of data access, rectification, erasure, restriction, portability, and objection/opt-out). If any such request is made directly to Data Processor, Data Processor will not respond to such communication directly without Data Controller's prior authorization, other than to acknowledge receipt of the request, unless required by Applicable Data Protection Law.

6.3. If Data Processor is required under Applicable Data Protection Law, and at Data Controller's request and expense, Data Processor will provide reasonably requested information regarding the Solutions and Professional Services 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 and expense, Data Processor will 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. Data Processor will provide such information within fifteen (15) business days of Data Controller's written request, unless otherwise required by Applicable Data Protection Law.

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

7.3. Unless Applicable Data Protection Law provides otherwise, Data Controller may make a request under this Section only once per calendar year. 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 damages, attorney fees and expenses, regulatory fines, and penalties incurred by Data Processor in relation to Personal 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 Data Protection Law will 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 will control. If any provision of this Addendum is adjudged to be unenforceable or invalid, that provision will be limited to the minimum extent necessary so that this Addendum will otherwise remain in effect.

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 Data Protection Law.

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

8.6. Data Processor will, within sixty (60) days after the termination or expiration of the Agreement, Erase the Personal Data from the Solutions and received through its provision of Professional Services. Upon Data Controller's request, Data Processor will provide written confirmation that Data Processor's obligations regarding Erasure have been fulfilled.

8.7. Notwithstanding the foregoing, Data Controller understands that Data Processor may retain Personal Data as required by Applicable Data Protection Law, which Personal 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:	317 SW Alder Street, Suite 850 Portland, OR 97204
	DocuSigned by: Jim Goings B55AF6EE8648464...
Signature	Signature
	Jim Goings
Print Name	Print Name
	CTO
Title	Title
	Jimbo@webtrends.com
Email	Email
	9/17/2021
Date	Date

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 and other Professional Services 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 Professional Services or who 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 Solutions 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, and business phone number of data exporter employees who use the Solutions or Professional Services, 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.

Annex B – List of Data Processor Subprocessors

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

Entity Name	Location	Subprocessing Activities
Amazon, Inc. Amazon Web Services (AWS)	P.O. Box 81226 Seattle, Washington, USA 98108-1226 www.aws.amazon.com	Cloud infrastructure provider

Annex C - 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.

Additional information regarding Data Processor's security measures can be found here: https://www.webtrends.com/legal/security-statement/.

ANNEX D
European Data Transfer Annex

This Annex D will apply in addition to the data protection and security requirements set out in the Data Protection Addendum if and to the extent that Webtrends receives and processes any Personal Data outside the European Economic Area or Switzerland. In the event of any conflict between this Annex D and the other requirements of the Data Protection Addendum, the provisions of this Annex D will prevail to the extent of that conflict.

Commission Implementing Decision (EU) 2021/914
STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 [*and, as applicable the Parties' relationship, the Swiss Federal Act on Data Protection as it may be amended or restated from time to time*] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its [sic] content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter ‘sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree [sic] a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter:

i. is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority;

ii. is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority; and

iii. is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(c) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*
Name: Client

Address: ____

Contact person's name, position and contact details: ________________________

____

Activities relevant to the data transferred under these Clauses:

The data exporters are the EU and Swiss affiliates of Client, using the Solutions and Professional Services to track visitors to Client Applications for analysis, reporting, testing, and targeting.

Signature and date: ____

Role: controller.

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*
Name: Webtrends, Inc.

Address: P.O. Box 8129, Portland, Oregon, USA 97207

Contact person's name, position and contact details: Jim Goings; CTO, DPO; privacy@webtrends.com.

Activities relevant to the data transferred under these Clauses:

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 and other Professional Services 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.

Signature and date: DocuSigned by: Jim Goings B55AF6EE8648464... ____

Role: processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Data subjects include visitors to the Client Applications, and Client's employees who use the Solutions or Professional Services, or who support contract governance.

Categories of personal data transferred:

- 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 Solutions 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 Professional Services, or who support contract governance.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The transfer will occur whenever Client is using the Solutions for Client Applications, when using Professional Services, and when engaged in contract governance.

Nature of the processing

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.

Purpose(s) of the data transfer and further processing

As stated above in "*Nature of the processing*."

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data processor will retain personal data as required by the Agreement or Applicable Data Protection Law. Otherwise, within 60 days after the termination or expiration of the Agreement, data processor will erase the personal data from the Solutions.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Data processor's subprocessors and their respective subprocessing activities are set forth in the Data Protection Addendum. Data processor passes through relevant obligations (e.g., duration of processing) to its subprocessors such that data processor can comply with the Agreement and Applicable Data Protection Law.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority/ies is the one identified in accordance with Clause 13.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

As specified in the Agreement and Data Protection Addendum.

ANNEX III

LIST OF SUB-PROCESSORS

As specified in the Data Protection Addendum.