ThousandEyes

MASTER DATA PROTECTION ADDENDUM

This MASTER DATA PROTECTION ADDENDUM ("**MDPA**") to the applicable Master Subscription Agreement or Terms of Use entered into by and between the Parties for the supply of Services by ThousandEyes to Customer (the "**Agreement**") reflects the Parties' agreement regarding information security and data protection.

This MDPA is governed by the terms of the Agreement. In the event of a conflict between this MDPA, including any attachments herein, and the Agreement, the provisions of this MDPA will control but only with respect to the subject matter hereof.

SCOPE OF AGREEMENT. This MDPA is comprised of the following Articles A-C attached hereto, which are incorporated by reference:

1. Article A INFORMATION SECURITY ARTICLE
2. Article B DATA PROTECTION ARTICLE
3. Article C GLOSSARY

ARTICLE A

INFORMATION SECURITY ARTICLE

1. Scope

This Information Security Article ("**ISA**") applies to the extent that ThousandEyes Processes or has access to Protected Data in the Performance of its obligations to the Customer. This ISA outlines the information security requirements between Customer and ThousandEyes and describes the technical and organizational security measures that shall be implemented by ThousandEyes to secure Protected Data prior to the Performance of any Processing under the Agreement.

Unless otherwise stated, in the event of a conflict between the Agreement and this ISA, the terms of this ISA will control as it relates to the Processing of Protected Data.

All capitalized terms not defined in the Glossary have the meanings set forth elsewhere in the MDPA.

2. General Security Practices

a. ThousandEyes has implemented and shall maintain appropriate technical and organizational measures designed to protect Protected Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures, and internal controls set forth in this ISA for its personnel, equipment, and facilities at ThousandEyes's locations involved in Performing any part of the Agreement.

3. General Compliance

a. **Compliance**. ThousandEyes shall document and implement processes and procedures designed to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements. Such processes and procedures shall be designed to provide appropriate security to protect Protected Data given the risk posed by the nature of the data Processed by ThousandEyes. ThousandEyes shall implement and operate information security in accordance with ThousandEyes's own policies and procedures, which shall be no less strict than the information security requirements set forth in this ISA.

b. **Protection of records**. ThousandEyes shall implement appropriate procedures designed to protect records from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, and contractual requirements.

c. **Review of information security.** ThousandEyes's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures) shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.

d. **Compliance with security policies and standards.** ThousandEyes's management shall regularly review the compliance of information processing and procedures with the appropriate applicable security policies and standards.

e. **Technical compliance review.** ThousandEyes shall regularly review information systems for compliance with ThousandEyes's information security policies and standards.

f. **Information Risk Management ("IRM").** ThousandEyes shall implement and utilize an appropriate information risk management process to frame, assess, respond and monitor risk, consistent with applicable contractual and legal obligations. ThousandEyes is required to have a risk management framework and conduct periodic (i.e., at least annual) risk assessments of its environment and systems to understand the risks and apply appropriate controls to manage and mitigate such risks. Threat and vulnerability assessment must be periodically reviewed and prompt remediation actions taken where material weaknesses are found. ThousandEyes will provide Customer with relevant summary reports and analysis upon written request, provided the disclosure of which would not violate ThousandEyes's own information security policies, or applicable law.

4. Technical and Organizational Measures for Security

a. **Organization of Information Security**

i. **Security Ownership**. ThousandEyes shall appoint one or more security officers responsible for coordinating and monitoring the security requirements and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, information security within the organization.

ii. **Security Roles and Responsibilities**. ThousandEyes shall define and allocate information security responsibilities in accordance with ThousandEyes's approved policies for information security. Such policies (or summaries thereof) shall be published and communicated to employees and relevant external parties required to comply with such policies.

iii. **Project Management**. ThousandEyes shall address information security in project management to identify and appropriately address information security risks.

iv. **Risk Management**. ThousandEyes shall have a risk management framework and conduct periodic (i.e., at least annual) risk assessment of its environment and systems to understand its risks and apply appropriate controls to manage and mitigate risks before Processing Protected Data.

b. **Human Resources Security**

i. **General**. ThousandEyes shall ensure that its personnel are under a confidentiality agreement that includes the protection of Protected Data and shall provide adequate training about relevant privacy and security policies and procedures. ThousandEyes shall further inform its personnel of possible consequences of breaching ThousandEyes's security policies and procedures, which must include disciplinary action, including possible termination of employment for ThousandEyes's employees and termination of contract or assignment for contractors and temporary personnel.

ii. **Training**. ThousandEyes personnel with access to Protected Data shall receive appropriate, annual periodic education and training regarding privacy and security procedures for services to aid in the prevention of unauthorized use (or inadvertent disclosure) of Protected Data and training regarding how to effectively respond to security incidents. Training shall be provided before ThousandEyes personnel are granted access to Protected Data or begin providing services. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.

iii. **Background Checks**. In addition to any other terms in the Agreement related to this subject matter, ThousandEyes shall conduct relevant background checks for its personnel in compliance with applicable law and ThousandEyes's policies.

iv. **Asset Management**. Access to Protected Data shall be restricted to ThousandEyes personnel who are authorized and who need to have such access for the Performance of ThousandEyes's obligations to the Customer.

v. **Information Classification**. ThousandEyes shall classify, categorize, and/or tag Protected Data to help identify it and to allow for access and use to be appropriately restricted.

vi. **Personnel Access Controls**

1. **Access.**

A. Limited Use. ThousandEyes understands and acknowledges that Customer may be granting ThousandEyes access to sensitive and proprietary information and computer systems in order for ThousandEyes to Perform its obligations to the Customer. ThousandEyes will not (i) access the Protected Data or computer systems for any purpose other than as necessary to Perform its obligations to Customer; or (ii) use any system access information or log-in credentials to gain unauthorized access to Protected Data or Customer's systems, or to exceed the scope of any authorized access.

B. Authorization. ThousandEyes shall restrict access to Protected Data and systems at all times solely to those Representatives whose access is necessary to Performing ThousandEyes's obligations to the Customer.

C. Suspension or Termination of Access Rights. At Customer's reasonable request, ThousandEyes shall promptly and without undue delay suspend or terminate the access rights to Protected Data and systems for any ThousandEyes's personnel or its Representatives reasonably suspected of breaching any of the provisions of this ISA; and ThousandEyes shall remove access rights of all employees and external party users upon suspension or termination of their employment, or engagement.

2. **Access Policy**. ThousandEyes shall determine appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. ThousandEyes shall maintain a record of security privileges of its personnel that have access to Protected Data, networks, and network services. ThousandEyes shall restrict and tightly control the use of utility programs that might be capable of overriding system and application controls.

3. **Access Authorization**.

A. ThousandEyes shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Customer's systems and networks. ThousandEyes shall use an enterprise access control system that requires revalidation of its personnel by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

B. ThousandEyes shall maintain and update a record of personnel authorized to access systems that contain Protected Data and ThousandEyes shall review users' access rights at regular intervals.

C. For systems that process Protected Data, ThousandEyes shall revalidate (or where appropriate, deactivate) access of users who change reporting structure and deactivate authentication credentials that have not been used for a period of time not to exceed six (6) months.

D. ThousandEyes shall restrict access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

4. **Network Design**. For systems that process Protected Data, ThousandEyes shall have controls to avoid personnel assuming access rights beyond those that they have been assigned to gain unauthorized access to Protected Data.

5. **Least Privilege**. ThousandEyes shall limit access to Protected Data to that personnel with Performance obligations and, to the extent technical support is needed, its personnel performing such technical support.

6. **Authentication**

A. ThousandEyes shall use industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords/PINs, ThousandEyes shall require that the passwords/PINs are renewed and changed regularly, at least every 180 days.

B. Where authentication mechanisms are based on passwords, ThousandEyes shall require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability).

C. ThousandEyes shall ensure that de-activated or expired identifiers and log-in credentials are not granted to other individuals.

D. ThousandEyes shall monitor repeated failed attempts to gain access to the information system.

E. ThousandEyes shall maintain industry standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.

F. ThousandEyes shall use industry standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they are assigned and distributed, and during storage (e.g., log-in credentials shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential log-in credentials.

vii. **Physical and Environmental Security**

1. **Physical Access to Facilities**

A. ThousandEyes shall limit access to facilities where systems that Process Protected Data are located to authorized individuals.

B. Security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.

C. Facilities shall be monitored and access-controlled at all times (24x7).

D. Access shall be controlled through key card and/or appropriate sign-in procedures for facilities with systems Processing Protected Data. ThousandEyes must register personnel and require them to carry appropriate identification badges.

2. **Physical Access to Equipment**. ThousandEyes equipment used to process or store Protected Data shall be protected using industry standard processes and technologies to limit access to authorized individuals.

3. **Protection from Disruptions**. ThousandEyes shall implement appropriate measures designed to protect against loss of data due to power supply failure or line interference.

4. **Clear Desk**. ThousandEyes shall have policies requiring a "clean desk/clear screen" to prevent inadvertent disclosure of Protected Data.

viii. **Operations Security**

1. **Operational Policy**. ThousandEyes shall maintain written policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Protected Data and to its systems and networks. ThousandEyes shall communicate its policies and requirements to all persons involved in the Processing of Protected Data. ThousandEyes shall implement the appropriate management structure and control designed to ensure compliance with such policies and with or applicable law concerning the protection and Processing of Protected Data.

2. **Security and Processing Controls**.

A. **Areas**. ThousandEyes shall maintain, document, and implement standards and procedures to address the configuration, operation, and management of systems, networks and services that store and/or Process Protected Data.

B. **Standards and Procedures.** Such standards and procedures shall include: security controls, identification and patching of security vulnerabilities, change control process and procedures, and incident prevention, detection, remediation, and management.

3. **Logging and Monitoring**. ThousandEyes shall maintain logs of administrator and operator activity and data recovery events related to Protected Data.

ix. **Communications Security and Data Transfer**

1. **Networks**. ThousandEyes shall, at a minimum, use the following controls to secure its networks that access or Process Protected Data:

A. Network traffic shall pass through firewalls, which are monitored at all times. ThousandEyes must implement intrusion prevention systems that allow traffic flowing through the firewalls and LAN to be logged and protected at all times.

B. Network devices used for administration must utilize industry standard cryptographic controls when Processing Protected Data.

C. Anti-spoofing filters and controls must be enabled on routers.

D. Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 8 characters with at least 3 of the following four classes: upper case, lower case, numeral, special character) and be changed at least every 180 days; or utilize other strong log-in credentials (e.g., biometrics).

E. Initial user passwords are required to be changed at first log-on. ThousandEyes shall have a policy prohibiting the sharing of user IDs, passwords, or other log-in credentials.

F. Firewalls must be deployed to protect the perimeter of ThousandEyes's networks.

2. **Virtual Private Networks ("VPN")**. When remote connectivity to the Customer's or ThousandEyes's network is required for Processing of Protected Data:

A. Connections must be encrypted using industry standard cryptography (i.e., a minimum of 256-bit encryption).

B. Connections shall only be established using VPN servers.

C. The use of multi-factor authentication is required.

3. **Data Transfer**. ThousandEyes shall have formal transfer policies in place to protect the transfer of information through the use of all types of communication facilities that adhere to the requirements of this ISA. Such policies shall be designed to protect transferred information from unauthorized interception, copying, modification, corruption, routing and destruction.

x. **System Acquisition, Development, and Maintenance**

1. **Security Requirements**. ThousandEyes shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.

2. **Development Requirements**. ThousandEyes shall have policies for secure development, system engineering, and support. ThousandEyes shall conduct appropriate tests for system security as part of acceptance testing processes. ThousandEyes shall supervise and monitor the activity of outsourced system development, if it utilizes any.

xi. **Penetration Testing and Vulnerability Scanning & Audit Reports**

1. **Testing.** ThousandEyes will perform periodic penetration tests on their internet perimeter network. Audits will be conducted by ThousandEyes's using industry recommended network security tools to identify vulnerability information. Upon written request from Customer, ThousandEyes shall provide a Vulnerability & Penetration testing report at the organization level which may include an executive summary of the results and not the details of actual findings.

2. **Audits.** ThousandEyes shall respond promptly to and cooperate with reasonable requests by Customer for security audit, scanning, discovery, and testing reports.

3. **Remedial Action.** If any audit or penetration testing exercise referred to in Section 4(b)(xi)(1) above reveals any deficiencies, weaknesses, or areas of non-compliance, ThousandEyes shall promptly take such steps as may be required, in ThousandEyes's reasonable discretion, to remedy those deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable given the circumstances and in any case within three (3) months of the findings from the audit and/or test.

4. **Status of Remedial Action.** Upon request, ThousandEyes shall keep Customer informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same, and shall certify to Customer as soon as may be practicable given the circumstances that all necessary remedial actions have been completed.

xii. **Contractor Relationships**

1. **Policies**. ThousandEyes shall have information security policies or procedures for its use of contractors that impose requirements consistent with this ISA. Such policies shall be reviewed at commercially reasonable planned intervals or if significant changes occur. Agreements with contractors shall include requirements that are consistent with, or analogous to, this MDPA.

2. **Monitoring**. ThousandEyes shall monitor and audit service delivery by its contractors and review its contractors' security practices against the security requirements set forth in ThousandEyes's agreements with such contractors. ThousandEyes shall manage changes in contractor services that may have an impact on security.

xiii. **Management of Information Security Incidents and Improvements**

1. **Responsibilities and Procedures**. ThousandEyes shall establish procedures to ensure a quick, effective, and orderly response to Information Security Incidents.

2. **Reporting Information Security Incident.** ThousandEyes shall implement procedures for Information Security Incidents to be reported through appropriate management channels as quickly as reasonably possible. All employees and contractors should be made aware of their responsibility to report Information Security Incidents as quickly as reasonably possible.

3. **Reporting Information Security Weaknesses.** ThousandEyes, employees, and contractors are required to note and report any observed or suspected information security weaknesses in systems or services.

4. **Assessment of and Decision on Information Security Events.** ThousandEyes shall have an incident classification scale in place in order to decide whether a security event should be classified as an Information Security Incident. The classification scale should be based on the impact and extent of an incident.

5. **Response Process.** ThousandEyes shall maintain a record of Information Security Incidents with a description of the incident, the effect of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to prevent future security incidents.

xiv. **Information Security Aspects of Business Continuity Management**

1. **Planning**. ThousandEyes shall maintain emergency and contingency plans for the facilities where ThousandEyes information systems that process Protected Data are located. ThousandEyes shall verify the established and implemented information security continuity controls at regular intervals.

2. **Data Recovery**. ThousandEyes shall design redundant storage and procedures for recovering data in a manner sufficient to reconstruct Protected Data in its original state as found on the last recorded backup provided by the Customer.

5. **Notification and Communication Obligations**

a. **Notification**. ThousandEyes shall without undue delay (i.e., within 72 hours from confirmation) notify Customer at such email address as is provided to ThousandEyes by Customer in writing if any of the following events occur:

A any compromise of Protected Data;

B any unmitigated, material security vulnerability, or weakness in (i) Customer's systems, or networks, of which ThousandEyes has actual knowledge, or (ii) ThousandEyes's systems or networks, that could allow an attacker to compromise the integrity, availability, or confidentiality of the Protected Data;

C an Information Security Incident that compromises or is likely to compromise the security of Protected Data and weaken or impair business operations of the Customer;

D an Information Security Incident that negatively impacts the confidentiality, integrity, and availability of Protected Data that is Processed, stored, and transmitted using a computer; or

E ThousandEyes's failure or inability to maintain compliance with the requirements of this ISA or applicable law.

Notwithstanding anything to the contrary in the Agreement, providing notice via email is sufficient for ThousandEyes to meet its notice obligations under this Section 5 (Notification and Communication Obligations).

b. **Cooperation**

i. ThousandEyes shall: (i) respond promptly to any Customer reasonable requests for information, cooperation, and assistance, including to a Customer designated response center.

c. **Information Security Communication**

i. Except as required by applicable law or by existing applicable contractual obligations, ThousandEyes agrees that it will not inform any third party of any of the events described above in this Section referencing, or identifying the Customer, without Customer's prior written consent. ThousandEyes shall fully cooperate with Customer and law enforcement authorities concerning any unauthorized access to Customer's systems or networks, or Protected Data. Such co-operation shall include the retention of all information and data within ThousandEyes's possession, custody, or control that is directly related to any Information Security Incident. If disclosure is required by law, ThousandEyes will work with Customer regarding the timing, content, and recipients of such disclosure. To the extent ThousandEyes was at fault, ThousandEyes will bear the cost of reproduction or any other remedial steps necessary to address the incident or compromise.

d. **Post-Incident**

i. ThousandEyes shall reasonably cooperate with Customer in any post-incident investigation, remediation, and communication efforts.

ARTICLE B

DATA PROTECTION ARTICLE

1. SCOPE

*This Data Protection Article ("**DPA**") outlines the terms and conditions with which the Parties must comply with respect to Processing Personal Data and applies to the extent that ThousandEyes Processes or has access to Personal Data in the Performance of its obligations to the Customer.*

2. DEFAULT STANDARDS

a. To the extent that ThousandEyes Processes Special Categories of Data, the security measures referred to in this DPA shall also include, at a minimum (i) routine risk assessments of ThousandEyes's information security program, (ii) regular testing and monitoring to measure and confirm the effectiveness of the information security program's key controls, systems, and procedures, and (iii) encryption of Special Categories of Data while "at rest" and during transmission (whether sent by e-mail, fax, or otherwise), and storage (including when stored on mobile devices, such as a portable computer, flash drive, PDA, or cellular telephone). If encryption is not feasible, ThousandEyes shall not store Special Categories of Data on any unencrypted storage devices. Further, ThousandEyes shall protect all Special Categories of Data stored on electronic databases, servers, or other forms of non-mobile devices against all reasonably anticipated forms of compromise by use of the safeguards contained in Attachment A (Information Security Exhibit).

b. If this DPA does not specifically address a particular data security or privacy standard or obligation, ThousandEyes will use appropriate, Generally Accepted Practices to protect the confidentiality, security, privacy, integrity, availability, and accuracy of Personal Data.

3. CERTIFICATIONS

a. ThousandEyes must maintain the certifications listed in an applicable agreement between the Parties, if any, and ThousandEyes shall recertify such certifications as reasonably required. If there is a material change in the requirements of a required certification or the nature of the Performance ThousandEyes is providing, such that ThousandEyes no longer wishes to maintain such certifications, the Parties will discuss alternatives and compensating controls in good faith.

b. Prior to Processing Personal Data and at Customer's request, ThousandEyes will provide Customer with copies of any certifications it maintains (along with relevant supporting documentation) that apply to the systems, policies, and procedures that govern the Processing of Personal Data. ThousandEyes will notify Customer if ThousandEyes has failed or no longer intends to adhere to such certifications or successor frameworks. This notification may be provided by posting or publication on ThousandEyes's public website.

4. DATA PROTECTION AND PRIVACY

a. The Parties agree that, for the Personal Data, Customer shall be the Data Controller and ThousandEyes shall be the Data Processor.

b. Customer shall:

i. in its use of the Services, comply with applicable law, including maintaining all relevant regulatory registrations and notifications as required under applicable law;

ii. ensure all instructions given by it to ThousandEyes in respect of Personal Data shall at all times be in accordance with applicable law;

iii. have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents or third parties to whom it extends the benefits of the Services; and

iv. keep the amount of Personal Data provided to ThousandEyes to the minimum necessary for the performance of the Services.

c. If ThousandEyes has access to or otherwise Processes Personal Data, then ThousandEyes shall:

i. implement and maintain commercially reasonable and appropriate physical, technical, and organizational security measures described in this DPA (including any appendices or attachments or referenced certifications) designed to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access; all other unlawful forms of Processing; and any Information Security Incident;

ii. take reasonable steps designed to ensure the reliability of its staff and that they are subject to a binding written contractual obligation with ThousandEyes to keep the Personal Data confidential (except where disclosure is required in accordance with applicable laws, in which case ThousandEyes shall, where practicable and not prohibited by applicable law, notify Customer of any such requirement before such disclosure) and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process Personal Data; and require that such personnel are aware of their responsibilities under this DPA and any applicable law (or ThousandEyes's own written binding policies that are at least as restrictive as this DPA);

iii. appoint data protection lead(s). Upon request, ThousandEyes will provide the contact details of the appointed person;

iv. assist Customer as reasonably needed to respond to requests from supervisor authorities, data subjects, customers, or others to provide information (including details of the Services provided by ThousandEyes) related to ThousandEyes's Processing of Personal Data;

v. not transfer Personal Data from the EEA or Switzerland to a jurisdiction which is not an Approved Jurisdiction, unless it first provides Customer advance notice and an opportunity to object; if Customer reasonably objects to the proposed cross border transfer the applicable Performance that is the subject matter of the objection shall terminate.

Where ThousandEyes Processes Personal Data from the EEA or Switzerland on behalf of Customer, ThousandEyes shall perform such Processing in a manner consistent with the Privacy Shield Principles (see www.commerce.gov/privacyshield) or its successor framework(s) to the extent the Principles are applicable to ThousandEyes's Processing of such data. If ThousandEyes is unable to provide the same level of protection as required by the Principles, ThousandEyes shall promptly notify Customer and cease Processing. In such event, Customer may terminate the applicable Performance of such Processing by written notice within thirty (30) days.

vi. for jurisdictions other than the EEA or Switzerland, not transfer Personal Data outside of the jurisdiction where the Personal Data is obtained unless permitted under applicable law and it first provides Customer advance notice and an opportunity to object; if Customer reasonably objects to the proposed cross border transfer the applicable Performance that is the subject matter of the objection shall terminate.

Where ThousandEyes Processes Personal Data from an APEC Member Economy on behalf of Customer, ThousandEyes shall perform such Processing in a manner consistent with the APEC Cross Border Privacy Rules Systems requirements ("**CBPRs**") (see www.cbprs.org) to the extent the requirements are applicable to ThousandEyes's Processing of such data. If ThousandEyes is unable to provide the same level of protection as required by the CBPRs, ThousandEyes shall promptly notify Customer and cease Processing. In such event, Customer may terminate the applicable Performance of such Processing by written notice within thirty (30) days.

d. In addition, if ThousandEyes Processes Personal Data in the course of Performance of its obligations to the Customer, then ThousandEyes shall also:

i. only Process the Personal Data in accordance with Customer's documented instructions, Appendix 1 of Attachment C and this DPA, but only to the extent that such instructions are consistent with applicable laws. If ThousandEyes reasonably believes that Customer's instructions are inconsistent with applicable law, ThousandEyes will promptly notify Customer of such;

ii. if required by applicable law, court order, warrant, subpoena, or other legal or judicial process to process Personal Data other than in accordance with Customer's instructions, notify Customer of any such requirement before Processing the Personal Data (unless applicable law prohibits such information on important grounds of public interest);

iii. only process or use Personal Data on its systems or facilities to the extent necessary to Perform its obligations solely on behalf of Customer and only for the purposes contemplated by the Parties;

iv. where applicable, act as a subprocessor of such Personal Data;

v. maintain reasonably accurate records of the Processing of any Personal Data received from Customer under the Agreement;

vi. make reasonable efforts to ensure that Personal Data are accurate and up to date at all times while in its custody or under its control, to the extent ThousandEyes has the ability to do so;

vii. disclose, at Customer's request, the categories and specific pieces of Personal Data collected; the source of Personal Data; and the categories of third parties with whom ThousandEyes discloses the Personal Data;

viii. not lease, sell, distribute, or otherwise encumber Personal Data unless mutually agreed to by separate signed, written agreement;

ix. provide reasonable cooperation and assistance to Customer in allowing the persons to whom Personal Data relate to have access to their data and to delete or correct such Personal Data if they are demonstrably incorrect (or, if Customer or Customer's customer does not agree that they are incorrect, to have recorded the fact that the relevant person considers the data to be incorrect);

x. provide such assistance as Customer reasonably requests (either on its own behalf or on behalf of its customers), and ThousandEyes or a Representative is reasonably able to provide, with a view to meeting any applicable filing, approval or similar requirements in relation to applicable law;

xi. promptly notify Customer of any investigation, litigation, arbitrated matter, or other dispute relating to ThousandEyes's information security or privacy practices as it relates to ThousandEyes's Performance of its obligations to Customer;

xii. provide such reasonable information and assistance as Customer reasonably requires (taking into account the nature of Processing and the information available to ThousandEyes) to Customer in ensuring compliance with Customer's obligations under applicable law with respect to:

i. security of Processing;

ii. data protection impact assessments (as such term is defined by applicable law;

iii. prior consultation with a supervisory authority regarding high risk Processing; and

iv. notifications to the supervisory authority and/or communications to Data Subjects by Customer in response to any Information Security Incident; and,

xiii. on termination of the MDPA for whatever reason, or upon written request at any time during the Term, ThousandEyes shall cease to Process any Personal Data received from Customer, and within a reasonable period will, at the request of Customer: 1) return all Personal Data; or 2) securely and completely destroy or erase (e.g. using a standard such as US Department of Defense 5220.22-M, NIST 800-53, or British HMG InfoSec Standard 5, Enhanced Standard) all Personal Data in its possession or control unless such return or destruction is not feasible or continued retention and Processing is required by applicable law. At Customer's request, ThousandEyes shall give Customer a certificate signed by one of its senior managers, confirming that it has fully complied with this Clause.

5. STANDARD CONTRACTUAL CLAUSES FOR THE PROCESSING OF PERSONAL DATA

If, and only with Customer's prior consent, ThousandEyes Processes Personal Data from the EEA or Switzerland in a jurisdiction that is not an Approved Jurisdiction, the Parties shall confirm there is a legally approved mechanism in place to allow for the international data transfer, which may include Standard Contractual Clauses.

6. SUBPROCESSING

a. Appointment of Subprocessors. Customer provides a general consent for ThousandEyes to engage onward subprocessors, conditional on ThousandEyes's compliance with the following requirements:

i. Any onward subprocessor must agree in writing to only process data in a country that the European Commission has declared to have an "adequate" level of protection; or to only process data on terms equivalent to the Standard Contractual Clauses, or pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities, or pursuant to a compliant US-EU Privacy Shield certification; and

ii. ThousandEyes will restrict the onward subprocessor's access to Personal Data only to what is strictly necessary to perform its services, and ThousandEyes will prohibit the subprocessor from processing the Personal Data for any other purpose.

b. List of Current Sub-processors and Notification of New Sub-processors**.** Customer hereby grants ThousandEyes general written authorization to engage the subprocessors listed at: www.thousandeyes.com/subprocessors ("**Subprocessor Lists**") subject to the requirements of this Section 6 (Subprocessing). Customer may receive notifications of new subprocessors by e-mailing dpa@thousandeyes.com with the subject "Subscribe", and if a Customer contact subscribes, ThousandEyes shall provide the subscriber with notification of new subprocessor(s) before authorizing such new subprocessor(s) to Process Personal Data in connection with the provision of the applicable Services. Notwithstanding anything to the contrary in the Agreement, providing notice via email is sufficient for ThousandEyes to meet its notice obligations under this Section 6 (Subprocessing).

c. Objection to Sub-processors**.** Customer may reasonably object to ThousandEyes's use of a new subprocessor (e.g., if making Personal Data available to the subprocessor may violate applicable law or weaken the protections for such Personal Data) by notifying ThousandEyes in writing within thirty (30) days after receipt of ThousandEyes's notice in accordance with the mechanism set out in Section 6(b). Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new subprocessor, as permitted in the preceding sentence, ThousandEyes will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new subprocessor without unreasonably burdening Customer. If ThousandEyes is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either Party may terminate without penalty the applicable Order Form(s) with respect only to those Services which cannot be provided by ThousandEyes without the use of the objected-to new subprocessor by providing written notice to the other Party. ThousandEyes will refund Customer any unused, prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

d. ThousandEyes shall have a documented security program and policies that provide (i) guidance to its subprocessors with respect to ensuring the security, confidentiality, integrity, and availability of personal data and systems maintained or processed by ThousandEyes; and (ii) express instructions regarding the steps to take in the event of a compromise or other anomalous event.

e. ThousandEyes will execute a written agreement with such approved subprocessors containing terms at least as protective as this DPA (provided that ThousandEyes shall not be entitled to permit the subprocessor to further subcontract or otherwise delegate all or any part of the subprocessor's Processing without ThousandEyes's prior notice and opportunity to object) and designating Customer as a third party beneficiary with rights to enforce such terms either by contract or operation of law. Further, if privity of contract is required by applicable law, ThousandEyes shall procure that any such subprocessors cooperates and enters into any necessary additional agreements directly with Customer.

f. ThousandEyes shall be liable and accountable for the acts or omissions of Representatives and its subprocessors to the same extent it is liable and accountable for its own actions or omissions under this DPA.

7. RIGHTS OF DATA SUBJECTS

a. **Data Subject Requests.** ThousandEyes shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, portability, or deletion of such Data Subject's Personal Data. Unless required by applicable law, ThousandEyes shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. In addition, ThousandEyes shall provide such information and cooperation and take such action as the Customer reasonably requests in relation to a Data Subject request.

b. **Complaints or Notices related to Personal Data.** In the event ThousandEyes receives any official complaint, notice, or communication that relates to ThousandEyes's Processing of Personal Data or either Party's compliance with applicable law in connection with Personal Data, to the extent legally permitted, ThousandEyes shall promptly notify Customer and, to the extent applicable, ThousandEyes shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Customer shall be responsible for any reasonable costs arising from ThousandEyes's provision of such assistance.

8. PERMITTED USE AND DISCLOSURE

Notwithstanding anything to the contrary in this MDPA, (i) ThousandEyes may disclose BGP Data and Support Data to third parties, provided such data has been aggregated and/or appropriately de-identified to reasonably prevent the identification of Customer; (ii) ThousandEyes may use BGP Data and Support Data for its own business purposes without attribution or compensation to Customer; and (iii) ThousandEyes may use Administrative Data for its own internal business purposes or to fulfill its obligations to Customer under an applicable agreement. ThousandEyes shall not be required to return or destroy Protected Data that constitutes Administrative Data, BGP Data or Support Data and shall continue to be permitted to use and disclose such Administrative Data, BGP Data, and Support Data as set forth in this Section 8 (Permitted Use and Disclosure) following the termination or expiration of this MDPA.

ARTICLE C

GLOSSARY OF TERMS

All capitalized terms not defined in this Glossary have the meanings set forth elsewhere in the MDPA.

a. "**Administrative Data**" means data related to employees or representatives of Customer that is collected and used by ThousandEyes in order to administer or manage ThousandEyes's Performance, or the Customer's account, for ThousandEyes's own business purposes. Administrative Data may include Personal Data and information about the contractual commitments between Customer and ThousandEyes, whether collected at the time of the initial registration or thereafter in connection with the delivery, management or Performance. Administrative Data is Protected Data.

b. **"Affiliates"** means any entity that directly or indirectly controls, is controlled by, or is under common control with, another entity, for so long as such control exists. In the case of companies and corporations, "control" and "controlled" mean beneficial ownership of more than fifty percent (50%) of the voting stock, shares, interest or equity in an entity. In the case of any other legal entity, "control" and "controlled" mean the ability to directly or indirectly control the management and/or business of the legal entity.

c. "**APEC**" means the Asia Pacific Economic Cooperation, a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. See www.apec.org for more information.

d. "**APEC Member Economy**" means the 21 members of APEC: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Vietnam.

e. "**Approved Jurisdiction**" means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

f. "**BGP**" or "**Border Gateway Protocol**" means a protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers. BGP directs packets between autonomous systems (AS) -- networks managed by a single enterprise or service provider.

g. "**BGP Data**" means information about a Party's BGP route tables.

h. "**Confidential Information**" means any confidential information or materials relating to the business, products, customers or employees of the Customer and includes, without limitation, trade secrets, know-how, inventions, techniques, processes, programs, schematics, software source documents, data, customer lists, financial information, pricing, product development, sales and marketing plans or information that ThousandEyes knows or has reason to know is confidential, proprietary or trade secret information obtained by ThousandEyes from the Customer or at the request or direction of the Customer in the course of Performing: (i) that has been marked as confidential; (ii) whose confidential nature has been made known by the Customer to ThousandEyes; or (iii) that due to their character and nature, a reasonable person under like circumstances would treat as confidential.

i. **"Customer Data"** means all data (including text, audio, video, or image files) that is provided by a customer in connection with the customer's use of services. Customer Data does not include Administrative Data, Support Data, BGP Data or ThousandEyes Technology.

j. "**Data Subject**" means the individual to whom Personal Data relates.

k. **"Customer"** means that party making available Protected Data (whether confidential or not) to the other party.

l. "**EEA**" or "**European Economic Area**" means those countries that are members of European Free Trade Association ("**EFTA**"), and the then-current, post-accession member states of the European Union.

m. "**EU Directives**" means the Data Protection Directive 95/46/EC and the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), any amendments or replacements to them (such as the EU General Data Protection Regulation). For clarity, the EU Directives are a subset of applicable law.

n. **"Generally Accepted Practices**" refer to the levels of accuracy, quality, care, prudence, completeness, timeliness, responsiveness, resource efficiency, productivity, and proactive monitoring of service performance that are at least equal to the then-current accepted industry standards of first-tier providers of the tasks contemplated in Performance of the Agreement.

o. "**Information Security Incident"** means a successful or imminent threat of unauthorized access, use, disclosure, breach, modification, theft, loss, corruption, or destruction of information; interference with information technology operations; or interference with system operations.

p. "**Order Form(s)**" means an order for the Services issued to ThousandEyes under the Agreement.

q. "**Parties**" means ThousandEyes and Customer.

r. "**Performance**" means any acts by either Party in the course of completing obligations contemplated under the Agreement, including the performance of services, providing deliverables and work product, access to Personal Data, or providing Software as a Service ("**SaaS**"), cloud platforms or hosted services. "**Perform**," "**Performs**," and "**Performing**" shall be construed accordingly.

s. "**Personal Data**" means any information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person, particular consumer, or household. Personal Data shall be considered Confidential Information regardless of the source. Personal Data is Protected Data.

t. "**Process**" means any operation or set of operations that is performed upon Personal Data, whether by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. "**Processes**" and "**Processing**" shall be construed accordingly.

u. "**Protected Data**" means Confidential Information, Customer Data, and all Personal Data. For clarity, ThousandEyes's Technology does not constitute Customer's Protected Data.

v. "**Representatives**" means either Party and its affiliates' officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.

w. "**Sensitive Personal Data**" or "**Special Categories of Data**" means personal information that requires an extra level of protection and a higher duty of care. These categories are defined by applicable law and include: information on medical or health conditions, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, precise geolocation over time, or information related to offenses or criminal convictions. Sensitive Personal Data and Special Categories of Data are each a category of Personal Data that are particularly sensitive and pose greater risk. Customer may require additional privacy responsibilities when dealing with such Personal Data, which will be appended to the Agreement or a statement of work, as applicable.

x. **"Service"** means a ThousandEyes service offering provided pursuant to the Agreement.

y. "**Standard Contractual Clauses**" means the standard model contractual clauses for data transfer approved by the European Commission is executed between the applicable parties (currently available at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en).

z. **"Support Data"** means information that ThousandEyes collects when Customer submits a request for support services or other troubleshooting, including information about the Services and other details related to the support incident.

aa. "**ThousandEyes Technology**" means the Service, performance metrics (including general measurements regarding application availability, performance, and security obtained through use of the Service), documentation, any deliverables or other materials created in the course of delivering the Service, any and all related and underlying technology and documentation, and any derivative works or modifications of the foregoing.