DATA PRIVACY ADDENDUM

This **Data Privacy Addendum** is made [ ] day of [ ]

BETWEEN:

(1) ***Qualys Inc.*** whose place of business is at 919 East Hillsdale Blvd, Foster City, CA 94404, USA ("**Qualys**"); and

(2) _____**.** whose place of business is at _____ ("**Customer**")

(together "**the parties**")

BACKGROUND:

(A) Qualys and Customer [signed/agreed to] a [*Master Cloud Services Agreement* on _____] (the "**Cloud Services Agreement**") which defines Qualys's obligations with respect to the provision of Cloud Services (defined below) to Customer.

(B) Since, as part of delivering the Cloud Services, Qualys will be processing personal data, the parties are required to enter into an appropriate data processing agreement which reflects the roles of the parties and their obligations under applicable data protection law.

(C) Accordingly, the parties hereby enter into this Qualys Data Privacy Addendum ("**Addendum**") in order to comply with the applicable obligations under data protection law.

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows.

OPERATIVE PROVISIONS

1. **DEFINITIONS**

1.1 All defined terms in this Addendum shall have the meanings set out in the Cloud Services Agreement unless specified to the contrary.

1.2 In this Addendum the words and phrases set out below shall have the meanings ascribed to them as set out below unless the context requires otherwise:

Applicable Law	shall mean all regional, national and international laws, rules, regulations and standards including those imposed by any governmental or regulatory authority that apply from time to time to the person or activity in the circumstances in question
Personal Data	means any personal data received, accessed or processed by Qualys in order to provide the Cloud Services.
Data Privacy Laws	the General Data Protection Regulation 2016/679, the implementation acts of the Directive by the Member States of the European Union; the California Privacy Rights Act of 2020, and its implementing regulations (as applicable); and/or any other Applicable Law or regulation relating to the protection of

	Personal Data.
Cloud Services	means the provision of Cloud Services as described and set out in the Cloud Services Agreement
Subprocessor	means a third party subprocessor (except for Qualys affiliates) engaged by Qualys to assist with the provision of the Cloud Services which involves the processing of Personal Data

2. **RELATIONSHIP WITH THE CLOUD SERVICES AGREEMENT**

2.1 For the avoidance of doubt, where there is any conflict or inconsistency, in relation to processing of Personal Data, between the provisions in the Cloud Services Agreement and this Addendum the provisions of this Addendum take precedence. Otherwise, all other provisions of the Cloud Services Agreement apply.

3. **STATUS OF PARTIES**

3.1 Customer is the controller of Personal Data; and Qualys is the processor of Personal Data under this Addendum.

3.2 The parties acknowledge that Qualys is entering into this Addendum on behalf of itself and its Affiliates located in and outside the European Union and where this Addendum refers to Qualys this may also include or refer to, where applicable, the local Affiliate of Qualys.

3.3 Qualys shall not assume any responsibility for determining the purposes for which Personal Data shall be processed. The purpose, nature and the details for processing of personal data are set forth in Schedule 1 of the Addendum.

3.4 Both parties shall comply with their applicable obligations under Data Privacy Laws.

3.5 The subject-matter of the data processing to be carried out by Qualys under this Addendum is: to provide the Cloud Services.

3.6 Customer bears the sole responsibility and liability for obtaining the required consents from the data subjects of any Personal Data to be processed or as anticipated under this Addendum.

4. **PROCESSOR OBLIGATIONS**

4.1 Qualys shall process Personal Data on behalf of Customer and only in accordance with lawful and documented instructions received from Customer, unless Qualys is required to otherwise process Personal Data under Data Privacy Laws. In the event that Qualys is subject to such an obligation, Qualys shall without undue delay notify Customer of this legal requirement before carrying out such processing, unless Qualys is prohibited from doing so under the Data Privacy Laws. Any processing required outside of the scope of the instructions from the Customer will require prior agreement between Qualys and the Customer, including agreement on any additional fees that Customer shall pay.

4.2 Qualys shall refer to Customer any requests from data subjects to rectify, amend, erase or port the Personal Data or to restrict or cease processing of such Personal Data.

4.3 Qualys shall promptly notify Customer and shall answer appropriately and without delay to all written inquiries from Customer regarding:

(a) Qualys's processing of Personal Data;

(b) any request it receives from a data subject regarding the Personal Data; Qualys shall not answer this request unless it has the specific prior written consent of Customer as well as documented instructions on how to respond; and

(c) any request, complaint or communication relating to Customer's obligations under Data Privacy Laws (including from supervisory authorities); Qualys shall not answer this request unless it has the specific prior written consent of Customer as well as documented instructions on how to respond.

5. **CUSTOMER COMPLIANCE**

5.1 Customer shall

(a) comply and will continue to comply with Data Privacy Laws

(b) ensure that the Personal Data will be and will continue to be collected, processed in accordance with notice, consent and other requirements of the Data Privacy Laws

(c) ensure that it has and will continue to have the right to transfer, or provide access to Personal Data to Qualys for processing and such processing by Qualys will not breach Data Privacy Laws.

(d) ensure that its instructions to Qualys in respect of the processing of the Personal Data are lawful and will not create legal or regulatory liability on part of Qualys, if followed.

(e) not disclose any special categories of Personal Data or Personal Data in relation to criminal convictions and offences.

6. **SCOPE MODIFICATIONS**

6.1 In the event that changes in Data Privacy Laws require modifications to the Cloud Services, the parties shall use commercially reasonable endeavours to comply with such requirements.

6.2 In the event that a party's (the "**first party**") compliance with Data Privacy Laws requires the imposition of certain contractual obligations under this Addendum, the first party shall notify the other party and both parties shall in good faith seek to amend this Addendum in order to address the requirements under Data Privacy Laws.

7. **SECURITY MEASURES**

7.1 Qualys shall implement appropriate technical and organizational security and confidentiality measures ("TOMs") which are designed to ensure a level of security appropriate to the Personal Data. The TOMs shall be designed to protect Personal Data, as processed by Qualys, against a breach of security leading to any accidental, unauthorised or unlawful destruction, loss, acquisition, alteration or unauthorized disclosure of or access to Personal Data ("**Breach**").

7.2 Such measures implemented in Section 7.1 shall require Qualys to take into regard the nature,

scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals that is presented by the processing, particularly from a Breach.

7.3 The TOMs implemented by Qualys are set out in Schedule 2 of this Addendum.

8. **CONFIDENTIALITY**

8.1 Qualys shall take reasonable steps to ensure that:

(a) All employees, agents or contractor who may have access to Personal Data shall undertake to maintain confidentiality of the Personal Date and use such Personal Data only for limited purposes of this Addendum. Qualys shall furthermore require its employees and contractors to adhere to the confidentiality obligations as set out in their respective agreement/arrangement with Qualys;

(b) All employees, agents or contractor who may have access to Personal Data undergone adequate training for handling of such Personal Data; and

(c) All employees, agents or contractor who may have access to Personal Data are informed of the confidential nature of the Personal Data and are aware of Qualys's data protection obligations under this Addendum.

9. **BREACH NOTIFICATION OBLIGATIONS**

9.1 In the event of a Breach resulting from a breach by Qualys of its obligations under this Addendum, the Qualys shall, at its own cost:

(a) notify Customer about the Breach, within seventy-two (72) hours of Qualys becoming aware of the Breach;

(b) provide Customer with reasonable assistance as required to take all such measures and actions as are necessary to remedy or mitigate the effects of Breach;

(c) if requested by Customer in writing, reasonably assist the Customer to fulfil its obligation to prepare and provide notification of the Breach to each data subject that may be affect by the Breach;

(d) after investigating the causes of such Breach, take such actions as may be necessary to minimize the effects of the Breach;

(e) take all actions as may be required by Data Privacy Laws;

10. **SUBPROCESSORS**

10.1 Where Qualys wishes to appoint a Subprocessor under this Addendum, Qualys will select Subprocessors with due diligence and will verify prior to engaging the Subprocessor that such Subprocessor is capable of complying with the obligations of the Qualys towards Customer, to the extent applicable to the Cloud Services assigned to that Subprocessor. Further Qualys will verify, prior to engaging the Subprocessor, that the Subprocessor has taken the appropriate technical and organisational measures to protect Personal Data.

10.2 The subcontracting under this Section 10 shall not release the Qualys from its responsibility for

its obligations under the Cloud Services Agreement. The Qualys shall be responsible for the work and activities of all Subprocessors.

11. **DATA TRANSFERS**

11.1 In the event of any transfer of Personal Data from a country in European Economic Area (the "EEA" and/or Switzerland) to a third country outside the EEA and/or Switzerland, that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data then the parties shall ensure an adequate level of protection by any of the recognized methods under the Data Privacy Laws, including but not limited to entering and/or procuring that the relevant Qualys affiliate enters into the standard contractual clauses, as set out under Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("**Standard Contractual Clauses**"), and Schedule 3 of this Addendum.

12. **RETURN AND DESTRUCTION**

12.1 Following termination or expiration of the Cloud Services Agreement for whatever reason, Qualys shall cease processing Personal Data and shall provide Customer with the opportunity to retrieve Personal Data in accordance with the data retention or portability provisions under the Cloud Services Agreement.

12.2 For the avoidance of doubt, Qualys may retain Personal Data where strictly required to store such data under Applicable Law and consequently must archive documentation that is evidence of the processing of Personal Data beyond termination or expiration of the Cloud Services Agreement.

13. **AMENDMENT**

13.1 This Addendum may not be amended or modified except in writing signed by authorised representatives of both parties.

14. **COUNTERPARTS**

14.1 This Addendum may be executed in any number of counterparts, each of which when executed and delivered shall constitute an original of this Addendum, but all the counterparts shall together constitute the same Addendum.

15. **GOVERNING LAW**

15.1 This Addendum shall be governed by and construed in accordance with the laws of state of California, USA without regards to conflicts of law provisions.

The parties' authorised signatories have duly executed this Addendum as of [_____]:

Customer	***Qualys Inc.***
By:	**By:**
Print Name:	**Print Name:**
Title:	**Title:**
Date:	**Date:**

Schedule 1

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]*

1. Name:

……

Address:

……

Contact person's name, position and contact details:

……

Activities relevant to the data transferred under these Clauses:

……

Signature and date: ……

Role (controller/processor): *Controller*

2. ……

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

Name: . ***Qualys Inc.***

……

Address: ***919 East Hillsdale Blvd, Foster City, CA 94404, USA***

……

Contact person's name, position and contact details: ***Ali Asgar Pancha, DPO, privacy@qualys.com***

……

Activities relevant to the data transferred under these Clauses: ***For provisioning of cloud services and providing related support***

……

Signature and date:

……

Role (controller/processor): *Processor*

……

2. ……

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees, contractors, co-workers and Personal Data shared by the Data exporter through use of Cloud Services

.

Categories of personal data transferred

Names, emails address, business contact information, IP addresses, job title

.

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).

Continuous

.

Nature of the processing

For providing cloud services and related support services

.

Purpose(s) of the data transfer and further processing

For providing cloud services and related support services

.

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

Throughout the term of the Cloud Services Agreement

.

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

For providing cloud services and related support services

.

Schedule 2 – Technical and Organisational Data Security Measures

Security Datasheet

Qualys shall maintain appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity and availability of the Cloud Service and the Customer Data. Qualys services operate under practices which are aligned with various frameworks and standards which are available at https://success.qualys.com/support/s/standards, as updated from time to time by Qualys.

Qualys shall take a holistic approach to information security, implementing a multilayered defense-in-depth security strategy where network, operating system, database, and software security practices and procedures complement one another with strong internal controls, governance, and oversight.

Qualys retains the right to make specific changes to the below security obligations provided that such changes shall not materially degrade the security controls provided to Customer Data under this Security Datasheet. Any capitalized terms that are not defined herein shall have the meaning given to such term in the Master Cloud Services Agreement ("Agreement").

Physical Security

Qualys shall;

1. employ measures designed to prevent unauthorized person from gaining access to computing facilities including facility building and designated datacenters.
2. restrict access to physical facilities that contain Qualys technical resources to authorized individuals only.
3. monitor and record, for audit purposes, access to the physical facilities containing Qualys technical resources.
4. provide additional safeguards for office locations and Qualys managed datacenters which include safeguards such as
   - Facilities shall be monitored and access-controlled at all times (24x7).
   - Qualys shall limit access to facilities to authorized individuals. Security perimeters shall be defined and used to protect information processing facilities.
   - Visitor management system, where visitors must sign into the visitor's register and be escorted and/or observed while at the location.
   - Areas containing teams who perform sensitive operations (e.g., security operations, site reliability and engineering) require a secondary, biometric authentication for access
   - Safeguards related to environmental hazards
   - Any physical movement of equipment is controlled and restricted to identified and authorized personal and other authorized change control procedures.

Personnel Security

1. All Qualys employees and contractor staff undergo pre-employment screening as permitted by applicable law and validation in accordance within the rules and regulations as applicable in the country of hiring.
2. Qualys performs standard background checks for all Qualys employees and contractor staff, including education, prior employment, criminal records, global sanctions, SSN, credit history etc., prior to their employment and access to Qualys information systems or Qualys' Customer Data. When a background check is not permitted by applicable law, Qualys will obtain alternate evidence to verify an employee's history and good standing.
3. All Qualys employees and contractor staff are required to complete security awareness training upon hire and thereafter annually, in accordance with the Qualys Information Security Awareness Program.
4. All Qualys employees and contractor staff enter into non-disclosure agreements prior to accessing Qualys

information systems or Qualys' Customer Data.

Access Control

1. With respect to Qualys employees and contractors accessing the production environment, Qualys enforces Role Based Access Controls (RBAC) and employs the access management principles of "need to know", "least privilege" and "segregation of duties.
2. System access control shall include system authentication, authorization, access approval, provisioning, and revocation for employees.
3. Qualys shall maintain and adhere to a documented User ID lifecycle management process that includes manual and/or automated processes for approved account creation, account removal within one (1) business day, and account modification for all Qualys technical resources and across all environments. Such process shall include review of access privileges and account validity to be performed at least each calendar year.
4. Qualys shall assign unique User IDs to Qualys authorized individual users. Qualys shall implement a multi-factor authentication solution to authenticate authorized personnel accessing its information systems used in production.
5. All Privileged access and access maintenance activities on Qualys cloud platform shall be centrally monitored.
6. Qualys shall enforce password policies on Qualys information systems used to operate the Cloud Services as per the industry standard requirements. When providing users with a new or reset password, use a secure method to provide this information and force password change at first login whenever a temporary credential is used.
7. Network and operating system accounts for Qualys employees shall be reviewed quarterly to ensure appropriate employee access levels.

System Security

1. Qualys shall maintain system hardening procedures and baseline configurations for systems that store or process Customer Data. This includes, at a minimum, restricting protocol access, removing or disabling unnecessary software, network ports and services, removing unnecessary files, user accounts, restricting file permissions, patch management and logging.
2. Qualys shall implement appropriate anti-virus/anti-malware software across all information systems processing Customer Data. Qualys keeps anti-virus/anti-malware software up to date with the most recent virus and malware signatures and definitions. On systems where anti-virus/anti-malware is not implemented, appropriate system hardening procedures are applied to minimize exposure.
3. Qualys shall prevent unauthorized access to Customer Data, Qualys implements technical controls to logically segment and segregate Customer Data from data belonging to other Qualys customers.
4. Qualys shall generate administrator and event logs for applications, system and infrastructure that store, or process Customer Data. Logs capture key security event types. Access to modify system logs is restricted.
5. Qualys shall protect information while at rest (including storage on any portable device, laptops, removable storage media, USB drives and backup tapes) using an encryption product/technology that meets or exceeds industry best practices.
6. Qualys shall protect Information during transmission using Transport Layer Security (TLS) 1.2 at a minimum.

Vulnerability & Patch Management

1. Qualys shall at least Weekly, scan Qualys information systems with industry-standard security vulnerability scanning software designed to detect security vulnerabilities, and remediate applicable critical, high, and medium risk security vulnerabilities identified.
2. Qualys shall implement or provide, as applicable, patches for vulnerabilities within the following time frames based upon the vulnerability classification described below.

Vulnerability classification	Time frame to implement/provide patch
Critical / High (or then-current equivalent classification)	Within thirty (30) days of discovery of the vulnerability
Medium (or then-current equivalent classification)	Within sixty to Ninety (60-90) days of discovery of the vulnerability
all others (or then-current equivalent classification)	Within one hundred and eighty days (180) days of discovery of the vulnerability

3. Qualys shall maintain and adhere to a documented process designed to identify and remediate security vulnerabilities.

Network Security

1. Qualys personnel and administrators shall connect to the Qualys Cloud Platform (QCP) environment via VPN into the Qualys corporate network and authentication through a bastion host, in order to gain access into the QCP Production environment.
2. Qualys shall employ industry standard communication security measures to protect Qualys' Customer Data from unauthorized access.
3. Qualys shall utilize security gateways (e.g., firewalls, routers, proxies, reverse proxies) to control access between the internet and Qualys Cloud Services.
4. Qualys shall perform security monitoring to reduce the risk of real time threats and prevent unauthorized access to QCP; this includes intrusion prevention system, intrusion detection systems, access controls, firewalls, and any other network monitoring tools.
5. Qualys shall employ Distributed Denial of Service protections services to ensure service availability to legitimate users.
6. Qualys shall protect Customer Data by segregating the production environment from development, testing and corporate environments with network and access level segmentation (e.g., networks, data, applications, etc.).
7. Qualys shall deploy resilient infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services.

Secure Coding Practice

1. Qualys shall comply with secure software development lifecycle program for managing the development and enhancement of any software or system to perform its Cloud Services.
2. Qualys shall follow secure coding practice as per OWASP and SANS security guidelines for building security into the design, build, test, and maintenance of its products and services.
3. Qualys development and test environment is logically segregated from its production and corporate environments. Production data is not used in test environment.
4. Qualys shall maintain and adhere to a documented change control process including back-out procedures for all production releases.

Monitoring and Auditing Controls

1. Qualys shall perform changes to cloud hardware infrastructure, operating software, product software, and supporting application software, to maintain operational stability, availability, security, performance, and product enhancement of QCP. Qualys follows formal change management procedures to review, test, and approve changes prior to application in the production environment.
2. Changes made through change management procedures include system and service maintenance activities, upgrades, and updates. Qualys change management procedures are designed to minimize service interruption during the implementation of changes.

3. For applications which utilize a database that allows modifications to Customer Data, logs for forensic analysis purposes shall be created and retained.
4. Qualys shall use a variety of software tools to monitor the availability and performance of the QCP and the operation of infrastructure and network components. Such as CPU, memory, storage, database, and other components.
5. Qualys operations staff shall monitor alerts associated with deviations to defined thresholds and follow standard operating procedures to investigate and resolve underlying issues
6. Qualys shall configure systems to log default security activities, access to information or programs, system events such as alerts, console messages, and system errors.
7. Security logs shall be stored within the security information and event management system (or equivalent system) in a native, unaltered format and retained in accordance with Qualys retention policies. Such logs are retained for 13 months, or as otherwise required by an applicable regulatory framework or applicable law.
8. Restrict access to security logs to authorized individuals and protect security logs from unauthorized modification.
9. Qualys shall periodically review anomalies from security and security-related audit logs. Thereafter they would be documented and resolved in a timely manner.

Contingency Planning

1. Qualys shall maintain a plan to ensure the continuation of the Cloud Services; should a Business Interruption occur. A "Business Interruption" means any event, that disrupts facilities, systems, personnel, or other business operations necessary for Qualys's performance of the Cloud Services in accordance with the Agreement or the Documentation.
2. Qualys Disaster Recovery (DR) plan for QCP is intended to provide service restoration capability in the event of a major disaster, as declared by Qualys.
3. Qualys shall determine whether an event constitutes a disaster requiring the execution of the DR plan for the affected Cloud Service.
4. Qualys shall set up and maintain a disaster recovery plan and ensure that it is tested at periodic Intervals.
5. Qualys shall deploy the QCP on resilient computing infrastructure designed to maintain service availability and continuity in the case of an incident or a disaster affecting the Cloud Services.
6. Qualys computing facilities including facility building and designated datacenters have component and power redundancy with backup generators in place, and Qualys shall incorporate redundancy in one or more layers, including network infrastructure, servers, database servers, cloud infrastructure and/or storage.
7. Qualys shall periodically make backups of the production data to minimize data loss in the event of an incident.
8. As part of the recovery efforts, Qualys shall maintain the Recovery Time Objective of 42 Hrs. and Recovery Point Objective of 8 hrs.

Security Breach

1. Qualys shall maintain and adhere to a documented Incident response plan against any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data ("Security Breach").
2. In the event that Qualys confirms that a Security Breach has occurred, and which has a material impact to Customer Data, Qualys shall notify Customer of such Security Breach, no later than seventy-two (72) hours from such confirmation.
3. Qualys shall provide Customer with regular status updates about the actions taken to resolve such Security Breach.
4. Qualys shall include the following information in a notification of a Security Breach to the extent such information is available with Qualys and are permitted to be shared:
    a. the date and time of the Security Breach occurrence (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known).
    b. type of Security Breach (i.e., data breach, malware, ransomware, etc.).

c. extent of the Security Breach and its known impact to Customer.
d. a summary of the facts and circumstances of the Security Breach and the impact or vulnerabilities caused by the Security Breach, including an identification of Cloud Services known or reasonably believed to have been impacted.
e. a description of response actions being undertaken. (Immediate, intermediate, and long-term).
f. recommendations for actions that may be undertaken by Qualys to mitigate, isolate, or eliminate any risks posed by the Security Breach.

5. Qualys acknowledges that where a Security Breach involves Customer Personal Data; then Qualys may be required to report such Security Breach to applicable regulatory authorities or law enforcement, without obtaining prior consent from the Customer.
6. Qualys shall inform Customer of any law enforcement agency or regulatory authority to which Qualys has reported the Security Breach and shall keep Customer abreast of any developments relating to any investigation or other involvement of any such agency or authority.

Audit Rights.

1. Customer shall have the right to request for information regarding Qualys' security program prior to the commencement of the Agreement and once annually thereafter during the term of the Agreement.
2. No more than once every twelve (12) months, Customer may submit a security assessment questionnaire to Qualys and may request summaries of third party's assessment reports about Qualys.
3. Qualys shall respond to such security assessment questionnaire and shall provide Customer with the requested report summaries within thirty (30) days after receipt of the request.
4. After reviewing Qualys' responses and reports, Customer may submit follow-up questions or request an online meeting with a Qualys representative. Qualys and Customer shall meet and discuss any remaining issues or Customer concerns.

Testing and Audits

1. Qualys at its expense, shall engage in security audits on an annual basis to validate the security measures in place as well as their sufficiency, and of the systems and the business processes by engaging a qualified, independent, and reliable third-party security professional to regularly (at least once per year) audit.
2. Qualys conforms to SOC 2 Type 2 which demonstrates the adequacy of Qualys controls under the Trust Services Principles and Criteria of the American Institute of CPAs,
3. Penetration Tests. At least once every year, Qualys undertakes an application penetration test by an independent third-party. Qualys remediates all critical and high vulnerabilities identified in the penetration test within 30 days of the date of identification. All other findings are remediated in a timeframe that is commensurate with the identified risks.
4. Vulnerability Scanning. Qualys performs regular vulnerability scanning on its infrastructure and services utilizing industry standard tools. Internal and external scans are performed at least weekly.
5. Upon Request, Qualys will provide a copy of its then most recent third-party audits or certifications, as applicable, or any summaries thereof.

Third Parties

1. Prior to engaging new third-party service providers and vendors, Qualys shall conduct risk assessment of the security practices of each third-party. Qualys also conducts periodic reviews of third-party vendors to verify their security practices continue to meet the necessary requirements as agreed between such third-party vendor and Qualys.

Privacy

1. Qualys shall at all times maintain appropriate information-security measures with respect to personally identifiable information/personal data in a manner consistent with applicable privacy laws including but not limited to, European Union (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)
2. In some jurisdictions, business contact information (a natural Person's name, job title, business address, business telephone number or email address) is considered personal information. For any business contact information that is Personal Information, Qualys shall: (a) use such information only as necessary to perform the Cloud Services; (b) access, use or process such personal information in accordance with applicable data protection and privacy laws; and (c) implement and maintain appropriate technical and organizational security measures to protect such personal information against unauthorized or unlawful access, loss, corruption or disclosure.
3. Qualys Privacy statement is accessible through https://www.qualys.com/company/privacy/.

Schedule 3 – Standard Contractual Clauses set out in European Commission Implementing Decision (EU) 2021/914 of 4 June 2021

For the purposes of Article 1(1) of Decision (EU) 2021/914 for the adoption of provisions of appropriate safeguards for the transfer by a controller or processor of personal data processed subject to that Regulation (data exporter) to a controller or (sub-) processor whose processing of the data is not subject to that Regulation (data importer).

Name of the data exporting organisation: **[Customer]**

Address:

Tel.: ……. ; fax:…… ; e-mail:…….

Other information needed to identify the organisation ……

(the data exporter)

And

Name of the data importing organisation: ***Qualys Inc.***

Address: 919 East Hillsdale Blvd, Foster City, CA 94404, USA

Other information needed to identify the organisation ……

(the data importer)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data.

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 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)([1]) for the transfer of personal 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

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(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 Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

(iv) Clause 12 –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).

(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.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of 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 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([2]) (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.

(2) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(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) GENERAL WRITTEN AUTHORISATION 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 30 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.([3])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 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

(3) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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.

[OPTION: deleted]

(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

(4) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

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 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, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter 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, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter 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, as indicated in Annex I.C, 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([5]);

(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

(5) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time- frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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.

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.

(b) 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.).

(c) 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.

(d) 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) [For Modules One, Two and Three: 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

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of Germany.]

[OPTION 2 (for Modules Two and Three): deleted]

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) The Parties agree that those shall be the courts of Germany.

(c) 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.

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

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *same as stated in Schedule 1 of the Addendum*

Data importer(s): *same as stated in Schedule 1 of the Addendum*

B. DESCRIPTION OF TRANSFER – *same as stated in Schedule 1 of the Addendum*

C. COMPETENT SUPERVISORY AUTHORITY – *The German Federal Data Protection Authority*

ANNEX II

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

In accordance with Schedule 2 of this Addendum

ANNEX III

LIST OF SUB-PROCESSORS

Subprocessors	**Address**	**Purpose of Processing**
Qualys Inc.	**USA** 919 East Hillsdale Blvd, Foster City, CA 94404, USA	To provide remote support services
Qualys Security TechServices Private Ltd.	**India** 10th to 16th Floor, Tower B, Panchshil Business Park, Survey No 20, Balewadi, Pune -4111045, Maharashtra	To provide remote support services
Oracle America Inc.	**USA** 500 Oracle Parkway Redwood Shores, CA 94065	Oracle public cloud for storage and datacentre services
Sify Technologies/OCI	**India** II Floor, TIDEL Park, No.4, Rajiv Gandhi Salai, Taramani, Chennai – 600113	Colocation datacentre
Cyxtera Technologies Inc./Centresquare	**USA** 2403 Walsh Ave Santa Clara, CA 95051	Co-location datacentres

ANNEX IV

UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Start date of this Addendum is the same date as the EU Standard Contractual Clauses ("SCCs") in Appendix 2 of the Agreement. **Parties** shall be incorporated into this document as listed in Annex I(A): List of Parties of the SCCs.

Table 2: Selected SCCs, Modules and Selected Clauses shall be incorporated as described in the EU SCCs in Appendix 2 to the Agreement. In particular, Module 2 Controller-to-Processor transfers apply.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

- Annex IA: List of Parties: see Annex I(A) to the EU SCCs: List of Parties
- Annex IB: Description of Transfer: see Annex I(B) to the EU SCCs: Description of Transfer and Appendix 1 to the Agreement
- Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: see Annex II to the EU SCCs
- Annex III: List of Sub processors (Modules 2 and 3 only): see Annex III to the EU SCCs

Table 4: Ending this Addendum when the Approved Addendum Changes

Which Parties may end this Addendum as set out in Section 0:

☐ Importer
☐ Exporter
☒ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

(A) **"Addendum"** means this International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.

(B) **"Addendum EU SCCs"** means the version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.

(C) **"Appendix Information"** is as set out in Table 3.

(D) **"Appropriate Safeguards"** means the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

(E) **"Approved Addendum"** means the template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 0.

(F) **"Approved EU SCCs"** means the Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

(G) **"ICO"** means the Information Commissioner.

(H) **"Restricted Transfer"** means a transfer which is covered by Chapter V of the UK GDPR.

(I) **"UK"** means the United Kingdom of Great Britain and Northern Ireland.

(J) **"UK Data Protection Laws"** means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

(K) **"UK GDPR"** is as defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 0 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 0 to 0 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 0, the provisions of Section 0 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 0 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 0) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 0, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a. its direct costs of performing its obligations under the Addendum; and/or

b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 0 of those Mandatory Clauses.

ANNEX V

CALIFORNIA PRIVACY RIGHTS ACT ADDENDUM

The California Privacy Rights Act ("**CPRA**"), codified at Cal. Civ. Code §1798.100 et seq., effective January 1, 2023, imposes on Customer (hereinafter also known "**Business**") certain obligations with respect to Consumers' Personal Information. Qualys (hereinafter also known as "**Service Provider**") seeks to comply with the CPRA and ensure that it will (a) Process Personal Information consistent with Business' obligations under the CPRA, and (b) cooperate with Business in its efforts to respond to requests by Consumers to exercise their rights under the CPRA and to otherwise comply with the CPRA.

Accordingly, commencing January 1, 2023, the following provisions apply to Service Provider's Processing of Consumers' Personal Information.

a. Definitions: Unless otherwise indicated in the Addendum, the capitalized terms used in this section shall have the meaning assigned to them in the CPRA.

   i. "Business" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that Collects Consumers' Personal Information, or on the behalf of which such information is Collected and that alone, or jointly with others, determines the purposes and means of the Processing of Consumers' Personal Information, that does business in the State of California, and that satisfies one or more of the following thresholds:

      A. As of January 1, of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant Cal. Civ. Code §1798.185(a)(5).
      B. Alone or in combination, annually buys, sells, or shares the Personal Information of 100,000 or more Consumers or, households.
      C. Derives 50 percent or more of its annual revenues from selling or sharing Consumers' Personal Information.

   ii. "Business Purpose" means the use of Personal Information for the Business' operational purposes, or other notified purposes, or for the Service Provider or contractor's operational purposes, as defined by regulations adopted pursuant to Cal. Civ. Code §Section 1798.185(a)(11), provided that the use of Personal Information shall be reasonably necessary and proportionate to achieve the purpose for which the Personal Information was Collected or Processed or for another purpose that is compatible with the context in which the Personal Information was Collected.

   iii. "Categories of Personal Information" or "Category of Personal Information" means the categories or category, as applicable, of Personal Information listed in Cal. Civ. Code §1798.140(v)(1).

   iv. "Collects," Collected," or "Collecting" means gathering, obtaining, receiving, or accessing any Personal Information pertaining to a Consumer by any means. This includes receiving information from the Consumer, either actively or passively, or by observing the Consumer's behavior.

   v. "Consumer" means a California resident (a) who is a natural person, and (b) whose Personal Information is Processed by Service Provider on Business' behalf for the purposes stated in the Addendum.

   vi. "CPRA Regulations" shall mean final regulations implementing the CPRA after those

regulations go into effect.

vii. "Personal Information" shall have the meaning set forth in the CPRA but shall be limited to Personal Information of California Consumers which Service Provider Processes on Business' behalf pursuant to the Addendum.

viii. "Process," "Processes," "Processed," or "Processing" means any operation or set of operations that are performed on Personal Information or on sets of Personal Information, whether or not by automated means.

ix. "Selling" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Consumer's Personal Information by the Business to a third party for monetary or other valuable consideration.

x. "Service Provider" means an entity that Processes Personal Information on behalf of a Business and that receives from or on behalf of the Business a Consumer's Personal Information for a Business Purpose pursuant to a written contract.

b. Compliance With Applicable Law: Service Provider shall Process Personal Information only (i) in accordance with the CPRA, the CPRA Regulations, and all other applicable laws and regulations; and (ii) in a manner that provides the same level of privacy protection for Personal Information as the CPRA and the CPRA Regulations require Business to provide. Business may take reasonable and appropriate steps to help ensure that Service Provider uses Personal Information consistent with the Business' obligations under the CPRA and the CPRA Regulations, and to stop and remediate unauthorized use of Personal Information.

c. Permissible Processing Of Personal Information: Service Provider shall Process Personal Information only (i) on Business' behalf; (ii) for Business' Business Purposes as set out below; (iii) to help Business respond, pursuant to subparagraph (g), below, to a request by a Consumer to exercise rights under the CPRA; and (iv) for any other purpose explicitly permitted by the CPRA or the CPRA Regulations.

i. The specific services for which Service Provider may Process Personal Information are as follows: See Schedule 1 to Data Privacy Addendum, Section B.
ii. Business is disclosing Personal Information to Service Provider only for the following specific Business Purposes: See Schedule 1 to Data Privacy Addendum, Section B.

d. Restrictions On Processing Personal Information: Service Provider is prohibited from (i) Processing Personal Information for any purposes but to provide the Services for the Business Purposes (as specified in Section (c), above), or as otherwise permitted by the CPRA or the CPRA Regulations; (ii) Processing the Personal Information for any commercial purpose other than the Business Purposes specified in this Addendum, including in the servicing of a different business unless expressly permitted by the CPRA Regulations; (iii) Processing Personal Information outside the direct business relationship between Business and Service Provider unless expressly permitted by the CPRA Regulations; (iv) Selling Personal Information; (v) combining Personal Information with personal information that it receives from, or on behalf of, another person or persons, or Collects from its own interaction with a Consumer (except as permitted by the CPRA Regulations); or (vi) Processing the Personal Information for any other purpose except as permitted by this Addendum.

e. Restrictions On Disclosure Of Personal Information To Subcontractors: Service Provider shall not disclose any Personal Information to any subcontractor, or permit any subcontractor to Process Personal Information on Service Provider's behalf, unless and until the subcontractor agrees, by contract, to the substantially the same restrictions and prohibitions on the Processing of Personal Information that this Addendum imposes on Service Provider.

f. Requests By a Consumer Directed To Service Provider: Service Provider shall refer to Business, within three (3) business days of receipt, any request received by Service Provider directly from a Consumer to exercise any of the consumers rights under the CPRA. Service Provider shall await instructions from Business before acting upon any request received directly from a Consumer.

g. Cooperation With Business' Response To Requests From Consumers: Business will inform Service Provider of any Consumer request made pursuant to the CPRA with which Service Provider must comply and will provide the information necessary for Service Provider to comply with the request. Within ten (10) business days of receiving a request from Business for assistance in responding to a request by a Consumer to exercise one or more of the rights provided by the CPRA, Service Provider shall do the following, as applicable:

   i. (A) delete the Consumer's Personal Information from the Service Provider's records; (B) direct any of its subcontractors and any Third Parties with which Service Provider shared the Consumer's Personal Information to delete the Consumer's Personal Information; and (C) confirm, in writing, that such deletion has been made unless an exception specified in the CPRA to the Consumer's right of deletion is applicable, in which case, Service Provider will identify the exception in writing to Business;

   ii. correct inaccurate Personal Information obtained by Service Provider pursuant to the Addendum and cause any subcontractor that maintains such inaccurate Personal Information to correct it as required by the Consumer;

   iii. identify for each relevant Consumer:

      A. the Categories of Personal Information Collected about the Consumer;
      B. the Business Purpose for Collecting the Personal Information;
      C. the categories of sources from which the Personal Information is Collected;
      D. the categories of persons or entities to which the Service Provider disclosed the Personal Information, the categories of Personal Information disclosed, and the Business Purpose(s) for the disclosure; and
      E. the Categories of Personal Information Shared, and for each Category of Personal Information Shared, the Third Parties to which that Category of Personal Information was Sold or Shared.

   iv. provide Business with a copy of the specific pieces of Personal Information Collected about the Consumer; and/or

   v. follow the Business' instructions regarding any limitations on the use or disclosure of the Consumer's Sensitive Personal Information.

Inability To Comply With CPRA: Service Provider will notify Business no later than five business days after Service Provider determines that it no longer can meet its obligations under this Addendum or the CPRA or CPRA Regulations. Upon receipt of any such notice, Business may take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information, or terminate the Service Agreement.