**EXHIBIT C**

**Data Processing Addendum**

This Data Processing Addendum ("DPA") is entered into as of the date of the License and Service Agreement ("Effective Date") and is made by and between Customer in the main Agreement above ("Data Controller") and QOMPLX, Inc. ("QOMPLX") (a "Data Processor"). The Data Controller and the Data Processor are collectively referred to as the "Parties."

**WHEREAS** this DPA is entered into to provide adequate safeguards with respect to the protection of Personal Data (as defined below) passed from the Data Controller to the Data Processor on the authority of the Data Controller for processing of such Personal Data by the Data Processor in connection with the provision of Services (as defined below),

**NOW THEREFORE,** the parties agree as follows:

1. **General**
    a. The above and foregoing recitals are true and correct and are incorporated herein by references.
    b. Any capitalized terms used in this DPA and not otherwise defined in this DPA shall have the same meanings such terms are given in the License and Services Agreement between the parties ("Agreement").
    c. This DPA shall be subject to the terms and conditions of the Services Agreement. To the extent this DPA, only as it relates to the processing of Personal Data, is inconsistent with the terms of the Services Agreement, this DPA shall govern. All terms of the Services Agreement remain in full force and effect.

2. **Subject Matter of this DPA**
    a. This DPA applies exclusively to the following: (i) processing of Personal Data by Data Processor on behalf of Data Controller that is subject to Regulation (EU) 2016/679 of the European Parliament and 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 repealing Directive 95/46/EC, the General Data Protection Regulation ("GDPR"), and any laws passed by the member states of the European Union to implement GDPR ("EU Data Protection Law") in connection with the Services under the Agreement; and (ii) the collection, use, retention, or disclosure of Personal Data by Data Processor on behalf of Data Controller that is subject to the California Consumer Privacy Act of 2018, as amended, Cal. Civ. Code §§ 1798.100-199 (the "CCPA"), in connection with the Services under the Agreement.
    b. The terms "Personal Data" (subject to the further clarification by the Data Processor on its processing of IP addresses set out in the Data Processor's documentation relating to its data collection, storage and use), "personal data

 

breach", "processing", "process", "Data Controller" and "Data Processor" shall have the meanings ascribed to them in the EU Data Protection Law.

c. Insofar as the Data Processor will be processing Personal Data subject to EU Data Protection Law or the CCPA on behalf of the Data Controller in the course of performing the Services under the Agreement, the terms of this DPA shall apply.
d. Processing of Personal Data by the Data Processor under this DPA shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in Schedule 2 of this DPA.

3. **The Data Controller and the Data Processor**
   a. The Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor. The Data Processor will process the Personal Data in accordance with the terms and conditions of the Agreement, this DPA, and any other written instructions from the Data Controller to which the Data Processor has agreed. The Data Processor will limit Personal Data collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the contracted business purposes.
   b. The Data Processor will only process the Personal Data on documented instructions of the Data Controller in such manner as, and to the extent that, is necessary for the provision of Services, except as may be otherwise required for compliance with applicable laws, including, but not limited to, EU Data Protection Law and the CCPA, save that the Data Processor may process Personal Data in anonymised form to evaluate the effectiveness of or means of improving its products and services. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction from the Data Controller violates EU Data Protection Law or the CCPA.
   c. The Data Processor will not collect, use, retain, disclose or otherwise make Personal Data available for its own commercial purposes or in a way that does not comply with the CCPA. The Data Processor will not sell the Personal Data.
   d. The Data Processor will promptly comply with any Data Controller request or instruction requiring Data Processor to provide, amend, transfer, or delete the Personal Data, or to stop, mitigate, or remedy any unauthorized processing.
   e. The Data Controller represents and warrants that it has all necessary rights to provide the Personal Data to Data Processor for the processing to be performed in relation to the Services. To the extent required, Data Controller is responsible for ensuring that any necessary data subject consents to the processing of Personal Data by Data Processor are obtained and for ensuring that a record of such consents is maintained by the Data Controller.
   f. If the contracted business purposes of the Agreement require the collection of Personal Data from individuals on Data Controller's behalf, Data Processor will, with regard to any Personal Data collected from residents of California,

 

provide a CCPA-compliant, Data Controller-approved notice addressing use and collection methods.

g. The Data Processor shall provide that all persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
h. Both Parties will comply with all applicable requirements of the CCPA when collecting, using, retaining, or disclosing personal information collected from residents of California.

4. **Security**
   a. Taking into account generally accepted industry standards, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Data Processor shall implement reasonably appropriate technical and organizational measures to ensure a level of security of processing of Personal Data appropriate to the risk. These measures shall include as appropriate:
      i. Measures to ensure that Personal Data can be accessed only by authorized personnel for the purposes of providing the Services;
      ii. In assessing the appropriate level of security, shall account for the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed;
      iii. The pseudonymization and encryption of Personal Data;
      iv. The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
      v. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
      vi. Measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide Services to the Data Controller;

   b. At the request of the Data Controller, the Data Processor shall demonstrate the measures it has taken pursuant to this Section 4 and shall allow the Data Controller to audit such measures no more than once annually, with reasonable notice to the Data Processor and at the Data Controller's own cost. The Data Processor shall provide reasonable assistance to the Data Controller with respect to such audits.

5. **Data Transfers**
   a. The Parties agree that the Processing of Personal Data by the Data Processor (or its sub-processors) may take place in any country outside of the European Economic Area ("EEA"). The Parties agree that where Processing takes place in connection with the provision of Services under the Agreement the standard

contractual clauses approved by the EU authorities under EU Data Protection Laws at Schedule 3 of this DPA apply in respect of that Processing.

b. The Data Processor agrees to enter into the standard contractual clauses referenced at 5a. with any sub-processor which it appoints to Process Personal Data in connection with the provision of Services by the Data Processor (and that in such circumstances it will be the data controller and the sub-processor will be the data processor).

6. **Information Obligations and Incident Management**
   a. The Data Processor shall notify the Data Controller promptly of becoming aware of a personal data breach involving Data Controller Personal Data information relevant to reasonably assist the Data Controller with its own notification obligations as applicable to Data Controller under EU Data Protection Law which may include the following: (i) a description of the nature of the personal data breach; (ii) the categories and approximate number of data subjects impacted; (iii) a description of the measures taken or proposed to be taken by the Data Processor to address the personal data breach.

7. **Sub-processors**
   a. The Data Controller authorizes the Data Processor to utilize sub-processors to process Personal Data, provided that such sub-processors enter into written terms consistent with the terms of this DPA. As of the Effective Date of this DPA, Data Processor's current sub-processors are those listed in Schedule 1 to this DPA attached hereto and incorporated herein. The Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of sub-processors, thereby giving the Data Controller the opportunity to object to such changes.

8. **Return or Destruction of Personal Data**
   a. Upon termination of the Agreement, and provided there is no applicable retention requirement in place to the contrary, the Data Processor shall, at the election of the Data Controller, either delete, destroy, or return all Personal Data of the Data Controller.

9. **Assistance to Data Controller**
   a. The Data Processor shall, taking into account the nature of the processing, assist the Data Controller by reasonably appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Data Controller's obligation to respond to request for exercising the data subject's rights, if any, under GDPR and the CCPA.
   b. The Data Processor must notify the Data Controller immediately if the Data Processor receives any complaint, notice, or communication that directly or indirectly relates to either Party's compliance with the CCPA. Specifically, the

Data Processor must notify the Data Controller within five (5) working days if the Data Processor receives a verifiable consumer request under the CCPA.

**IN WITNESS WHEREOF** the Parties have caused this Agreement to be executed by their duly authorized representatives as set forth below.

**QOMPLX, INC.**

_____
SIGNATURE

_____
PRINTED NAME

_____
TITLE

_____
DATE

_____
CUSTOMER

_____
SIGNATURE

_____
PRINTED NAME

_____
TITLE

_____
DATE

ADDRESS: _____

_____

_____

## Schedule 1

## Sub-processors

Amazon Web Services

## Schedule 2
## Data Processing Details

Processing of the Personal Data by the Data Processor under this DPA shall be for the subject-matter, duration, nature, and purposes and involve the types of Personal Data and categories of Data Subjects set out in this Schedule 2. The Data Controller is responsible for providing to the Data Processor the following information.

1. **Subject-matter of processing:**

   Provision of CMMC Pre-assessment services

2. **Duration of the processing:**

   QOMPLX retains processed information for three years, unless Customer specifies a different retention period in its Master Service and License Agreement or in Statements of Work.

3. **Nature and purpose of the processing:**

   Q:CYBER products collect a range of information from customers to help them detect and reduce the impact of potential security incidents. As part of those collection activities, Q:CYBER collects personal data. The products that process Personal Data are the following:

   - **Identity Assurance** analyzes Kerberos authentication exchanges to ensure the protocol is working as designed and has not been subverted, thereby safeguarding the integrity of customers' authentication controls. To fulfill this purpose, Identify Assurance collects and processes all Kerberos Authentication Service (V5) messages and Directory Services Replication (DRS) protocol messages. The QOMLINK software appliance can also optionally collect Windows event logs from customer premises, which are used for heuristically detecting Kerberoasting and other attacks.

   - **Privilege Assurance** analyzes Active Directory data to identify security risks associated with privileged user accounts, stale or outdated user accounts and machines, weaknesses in policy, and other risks. To fulfill this purpose, Privilege Assurance extracts and processes Active Directory data.

   - **Q:Scan** analyzes publicly information to identify an organization's weaknesses and exposures, using either an internet domain or D-U-N-S® number to identify the target organization.

- **CMMC Pre-assessment** assists customers in documenting their conformance with the United States Department of Defense's Cybersecurity Maturity Model Certification ("CMMC"). It combines customer-supplied survey answers with information connected by QOMPLX's Scan product. Scan analyzes publicly information to identify an organization's weaknesses and exposures, using either an internet domain or D-U-N-S® number to identify the target organization. The results of the customer-supplied survey responses are combined with Scan data to generate a final score.

4. **Type of Personal Data:**

Identifiers:

- email address of the individual registering accounts with QOMPLX
- email Addresses related to the domains, when scanned by Q:Scan
- email addresses of employees, when collected by Privilege Assurance
- names of employees, when collected by Privilege Assurance
- names of employees considered to be High-Value Personnel and Management Team members, when collected by Q:Scan on a discretionary basis
- IP addresses[1]

5. **Categories of Data Subjects:**

Employees
Customers

6. **Specific processing instructions:**

Personal Data is processed by QOMPLX products, and are not disclosed to third parties.

[1] IP addresses have been classified as "personal data" by some Data Protection Authorities on the grounds that publicly routable IP addresses could be hypothetically linked with internet service provider (ISP) subscriber records to identify data subjects. We do not agree in QOMPLX's specific case. QOMPLX does not collect or process ISP records, or any other data, that could plausibly identify a data subject solely from an IP address.

**Schedule 3**

**COMMISSION IMPLEMENTING DECISION (EU) 2021/914**

**of 4 June 2021**

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

---

**STANDARD CONTRACTUAL CLAUSES**

**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 Appendix 1 (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 Appendix 2 (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 Appendix 4.

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

***Clause 2***

**Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses

pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

***Clause 3***

**Third-party beneficiaries**

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

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

(ii) Clause 8 –Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

(iv) Clause 12 –Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – 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 Schedule 2 of the Data Processing Agreement between the Parties ("Agreement") and Appendix 4 of these Clauses.

***Clause 7 – Optional***

**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 Appendix 1 or 2 as applicable.

(b) Once it has completed the Appendix and signed Appendix 1 or 2 as applicable, 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 Appendix 1 or 2 as applicable.

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

**SECTION II – OBLIGATIONS OF THE PARTIES**

***Clause 8***

**Data protection safeguards**

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

**8.1 Instructions**

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

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

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Schedule 2 of the Agreement and Appendix 4 of these Clauses 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 Appendix 5 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 Schedule 2 of this Agreement and Appendix 4 of these Clauses. 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 Schedule 2 of this Agreement and Appendix 4 of these Clauses.

**8.8 Onward transfers**

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

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

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

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

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

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

**8.9 Documentation and compliance**

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

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

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing

activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

***Clause 9***

**Use of sub-processors**

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list as set out in Schedule 1 of this Agreement. 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. 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***

**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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

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

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

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

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

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

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

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

***Clause 12***

**Liability**

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

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

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

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

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

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

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

### *Clause 13*

### Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, is the supervisory authority located in the jurisdiction stated at Clause 15 of this Agreement shall act as competent supervisory authority.

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

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

### *Clause 14*

### Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

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

***Clause 15***

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

### 15.1 Notification

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

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

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

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

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

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

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

### 15.2 Review of legality and data minimisation

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

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

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

## SECTION IV – FINAL PROVISIONS

### *Clause 16*

### Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

### *Clause 17*

### Governing law

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

governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ **(*specify Member State*).**

***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** _____ **(*specify Member State*).**

(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 1

## DATA EXPORTERS

| Name | Place of Incorporation | Company Number | Registered Office / Principal place of business |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## APPENDIX 2

## POTENTIAL DATA IMPORTERS

| Name | Place of Incorporation | Company Number or Federal Employer Identification Number | Registered Office / Principal place of business |
|---|---|---|---|
| QOMPLX, Inc. | Delaware, USA | 47-4091518 | 1775 Tysons Blvd, Suite 800 Tysons, VA 22102-4284 |
| QOMPLX Limited | England | 10893355 | Clarendon House, 52 Cornmarket Street, Oxford OX1 3HJ United Kingdom |
| QOMPLX Underwriting Limited | England | 11538456 | Clarendon House, 52 Cornmarket Street, Oxford OX1 3HJ, United Kingdom |
| QOMPLX Government Solutions, LLC | Delaware, USA | 84-3675432 | 1775 Tysons Blvd, Suite 800 Tysons, VA 22102-4284 |
| RubiQon Holdings LLC | Delaware, USA | 85-0530180 | Tysons, VA 22102-4284 |
| RubiQon Risk and Insurance, LLC | Delaware, USA | 85-0557801 | 1775 Tysons Blvd, Suite 800 |

# APPENDIX 3

## DATA PROCESSING PRINCIPLES

### 1. PURPOSE LIMITATION

Personal data may be processed and subsequently used or further communicated only for purposes described in Appendix 3 or subsequently authorized by the data subject.

### 2. DATA QUALITY AND PROPORTIONALITY

Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

### 3. TRANSPARENCY

Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the Data Exporter.

### 4. SECURITY AND CONFIDENTIALITY

Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

### 5. RIGHTS OF ACCESS, RECTIFICATION, DELETION AND OBJECTION

As provided in Article 15 of GDPR, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the Data Exporter. Provided that the Authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the Data Importer or other organisations dealing with the Data Importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation

may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the Data Importer, and the data subject may always challenge a refusal before the Authority.

**6. SENSITIVE DATA**

The Data Importer shall take such additional measures (e.g., relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause 2.

**7. DATA USED FOR MARKETING PURPOSES**

Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

**8. AUTOMATED DECISIONS**

For purposes hereof "automated decision" shall mean a decision by the Data Exporter or the Data Importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The Data Importer shall not make any automated decisions concerning data subjects, except when:

(a) such decisions are made by the Data Importer in entering into or performing a contract with the data subject; and

(b) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that party.

or

(c) where otherwise provided by the law of the Data Exporter.

# APPENDIX 4

## DESCRIPTION OF THE TRANSFER

### Data subjects

Identifiers:

- email addresses of employees
- names of employees
- IP addresses[2]

### Purposes of the transfer(s)

Q:CYBER products collect a range of information from customers to help them detect and reduce the impact of potential security incidents. As part of those collection activities, Q:CYBER collects personal data. The products that process Personal Data are Identity Assurance, Privilege Assurance, Q:Scan and CMMC Pre-assessment. See *Schedule C, Data Processing Addendum*, Schedule 2 for additional details.

### Categories of data

Customers
Employees

### Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

1. Data Importers;
2. Data processors of the data importer, subject to the terms of this agreement and applicable law;

The contact point for all data protection enquiries relating to any group Company is:

| | |
|---|---|
| Contact Name: | John Ferrari |
| Company: | QOMPLX, Inc. |
| Position: | DPO, CAO |
| Email: | John.ferrari@qomplx.com with a copy to privacy@qomplx.com |
| Telephone: | 571.835.0645 |

[2] IP addresses have been classified as "personal data" by some Data Protection Authorities on the grounds that publicly routable IP addresses could be hypothetically linked with internet service provider (ISP) subscriber records to identify data subjects. We do not agree in QOMPLX's specific case. QOMPLX does not collect or process ISP records, or any other data, that could plausibly identify a data subject solely from an IP address.

# APPENDIX 5

## TECHNICAL AND ORGANISATIONAL MEASURES APPLICABLE TO THE TRANSFER

Description of the technical and organisational measures implemented by the data importer(s) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

**Examples of possible measures**:

Measures of pseudonymisation and encryption of personal data.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing.

Measures for user identification and authorization.

Measures for the protection of data during transmission.

Measures for the protection of data during storage.

Measures for ensuring physical security of locations at which personal data are processed.

Measures for ensuring events logging.

Measures for ensuring system configuration, including default configuration.

Measures for internal IT and IT security governance and management.

Measures for certification/assurance of processes and products.

Measures for ensuring data minimisation.

Measures for ensuring data quality.

Measures for ensuring limited data retention.

Measures for ensuring accountability.

Measures for allowing data portability and ensuring erasure.