DATA PROCESSING AGREEMENT

This data processing agreement ("***DPA***") is executed upon the date of the last signature ("***DPA Effective Date***") by **Coupa Software, Inc.** ("***Coupa***") and the customer identified below ("***Customer***") to amend the master subscription agreement governing the use of the Coupa Platform and Hosted Applications by Customer ("***Agreement***").

This DPA is incorporated into and subject to the Agreement and reflects the parties' agreement with respect to the processing of personal data within Customer Data under the Agreement. If there is a conflict between this DPA and the Agreement, this DPA shall control. To the extent applicable and required by applicable data protection laws, the Standard Contractual Clauses, set forth as Exhibit A, form an integral part of this DPA. Capitalized terms used but not defined in this DPA will have the meaning provided in the Agreement.

0. **Definitions**. Except as stated otherwise herein, the terms "*personal data*", "*data subject*", "*processing*", "*controller*" and "*processor*" will have the meanings ascribed to them in Article 4 of Regulation (EU) 2016/679 ("***GDPR***"). The term "***Data Protection Law(s)***" shall include Regulation (EU) 2016/679 ("***GDPR***") and the UK Data Protection Act 2018 ("***UK GDPR***"), as applicable. Where a specific reference is made to GDPR it shall be understood to be referring to the equivalent requirement under the UK GDPR, *mutatis mutandis*.

1. **Term**. This DPA will take effect on the DPA Effective Date and automatically terminate following the expiry or termination of the Agreement.

2. **Information Security Program and Related Matters**. Coupa has implemented an information security program consisting of policies and procedures that define how system information is entered, managed, and protected. Coupa's current security program is further specified in Appendix 2 to Exhibit A. Coupa shall monitor, analyze and respond to security incidents in a timely manner in accordance with Coupa's standard operating procedure, which sets forth the steps that Coupa employees must take in response to a threat or security incident. Customer shall promptly apply any subscription service upgrade that Coupa determines is necessary to maintain the security, performance or availability of the subscription service and shall in general comply with Coupa's upgrade policy.

3. **Affected Persons/Categories of Data**. Users and business partner personnel designated by Customer are affected by the collection, processing or use of personal data. The categories of personal data processed hereunder are specified in Appendix 1 to Exhibit A. Unless otherwise agreed by the parties in writing, no Restricted Information as defined in the Agreement, shall be processed under the Agreement.

4. **Personnel.** Coupa will ensure (a) that its personnel with access to Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and (b) that such personnel are adequately instructed in the appropriate handling of personal data. Coupa shall implement measures to restrict access to personal data as set out in Appendix 2 to Exhibit A.

5. **Audit Rights.** Coupa makes available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR, in particular, by making available annual compliance reports for download at https://get.coupa.com/Compliance-Reports_Request-Report.html (or another successor site as designated by Coupa). In the event Customer wishes to carry out further audit activities, Customer shall provide Coupa and its subprocessors with as much notice as possible if it exercises any of its audit rights under the DPA or, as applicable, according to the Standard Contractual Clauses and shall pay Coupa and its subprocessors reasonable administrative costs and expenses for engaging and complying with any on-site audit, unless such audit shows that Coupa is in material breach with its obligations under this DPA.

6. **Subprocessing**. Coupa uses subprocessors listed under https://success.coupa.com/subprocessors (or another successor site as designated by Coupa). Customer hereby consents to Coupa engaging new subprocessors subject to Clause 11 of Exhibit A and the following terms.

   Coupa shall provide Customer in due time with prior notice (written or email) of any new subprocessor. Customer shall notify Coupa promptly in writing within 10 business days after receipt of such notice, if the Customer has a reasonable basis to object to the use of new subprocessor. For the avoidance of doubt, the Customer hereby acknowledges that the use of a new subprocessor shall be deemed acceptable if Coupa has procured: (i) the same level of protection of personal data by imposing the same obligations as set out in this DPA on each new subprocessor by way of a written contract; and (ii) that the relevant subprocessor will implement and use appropriate technical and organizational measures which meet the requirements of applicable Data Protection Law. Notwithstanding the foregoing, if Customer reasonably objects to the appointment of another subprocessor, the parties will come together in good faith to discuss an appropriate solution. Coupa may in particular choose: (a) not to use the intended subprocessor or (b) take corrective steps and/or measures reasonably requested by the Customer and engage the subprocessor.

7. **Processing of Customer Data**. With respect to personal data within Customer Data under this DPA, the parties agree that Customer is the controller and Coupa is a processor. Customer will comply with its obligations as a controller and Coupa will comply with its obligations as a processor under the Agreement and this DPA. Coupa will only process Customer Data in fulfilling its obligations under the Agreement, such as, without limitation, providing and supporting Customer's usage of the subscription service, detecting and addressing security and technical issues, and responding to support requests. The processing of Customer Data only takes place within the framework of the Agreement and according to the instructions of Customer. In particular, the collected, processed or used data may only be corrected, deleted or blocked on instructions of Customer. Backup copies are created, if they are necessary to ensure proper data processing, or reproduction processes that are necessary in order to ensure compliance with regulatory retention requirements. All instructions must be issued in writing. Coupa shall immediately inform the Customer if, in its opinion, an instruction violates the GDPR or other applicable data protection regulations.

8. **Data Subject Access Requests**. Coupa will provide reasonable assistance to Customer in the fulfillment of Customer's obligation to respond to data subject requests, referred to in Chapter 3 (Rights of the data subject) of the GDPR, for personal data stored on the Coupa Platform used to provide the services. If a data subject raises a request directly with Coupa, Coupa will promptly pass this request to Customer.

9. **Assistance, Reporting and Impact Assessments**. Coupa will provide reasonable assistance to Customer in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of Regulation (EU) 2016/679.

10. **Breach Notification**. Coupa shall report to Customer's support contacts designated in Coupa's customer support portal the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data within Customer Data ("***Breach***") within 24 hours, after Coupa determines that a Breach has occurred, unless restricted by law. Accordingly, Coupa shall share information about the nature and consequences of the Breach that is reasonably requested by Customer to enable it to notify affected individuals, government agencies and/or credit bureaus. Customer has sole control over the content of Customer Data that it enters into the subscription service and is solely responsible for determining whether to notify impacted Data Subjects (defined below) and the applicable regulatory bodies or enforcement commissions and for providing such notice. Customer shall ensure that the support contacts designated in Coupa's customer support portal be current and ready to receive any breach notification from Coupa.

11. **Return and Deletion of Customer Data.** The return and deletion of Customer Data after the termination of the Agreement shall be in accordance with Clause 12 of Exhibit A.

12. **International Data Transfers**.

a) **Lawful Transfers**. As part of providing the Hosted Applications or Coupa Platform, Coupa may transfer personal data to a jurisdiction different from the hosting region as necessary for the purposes of complying with its obligations under the Agreement. The transfer of personal data regulated by the GDPR to a jurisdiction outside the EEA, or the European Commission-approved countries providing 'adequate' data protection, shall be governed by the Standard Contractual Clauses, attached to this DPA as Exhibit A, to enable the lawful transfer of personal data.

In the event that, for any reason whatsoever, the Standard Contractual Clauses no longer constitute an adequate safeguard, the parties shall, acting reasonably, promptly negotiate in good faith an alternative lawful method to facilitate such transfers of Customer Data, taking into consideration what other similarly situated business partners have done in respect of such issue.

In case the EU Commission adopts a new set of standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection (Chapter V GDPR), the parties shall mutually agree on the incorporation of the new set of standard data protection clauses upon request.

b) **"Schrems II" clause**. Coupa shall promptly notify the Customer if it: (i) receives a legally binding request by a public authority under the laws of the country of destination for disclosure of personal data transferred pursuant to this DPA; 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 this DPA in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

If Coupa is prohibited from notifying the Customer, Coupa agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicate as much information and as soon as possible. Coupa agrees to document its best efforts in order to be able to demonstrate them upon request of the Customer.

To the extent permissible under the laws of the country of destination, Coupa agrees to provide or make available to the Customer, in regular intervals for the duration of the contract, the greatest possible amount of relevant information on the requests received in relation to this DPA (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.).

ACKNOWLEDGED AND AGREED TO:

"**Customer**"		**Coupa Software, Inc.,** on its own behalf and as agent for and on behalf of Coupa Affiliates who are processing Customer Data.
Address	____________________________________	1855 S. Grant Street., San Mateo, CA 94402, USA
Signature	____________________________________	DocuSigned by: Jon Stueve 128BCF74AAF2405...
Name	____________________________________	Jon Stueve
Title	____________________________________	SVP & General Counsel
Date	____________________________________	

<u>Exhibit A</u>

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC[1] for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization:	Customer
Address:	see signature section above

(the data **exporter**)

and

Name of the data importing organization:	**Coupa Software, Inc.,** on its own behalf and as agent for and on behalf of Coupa Affiliates who are processing Customer Data.
Address:	1855 S. Grant Street., San Mateo, CA 94402, USA
Telephone:	+1 650.931.3200
E-mail	legalnotices@coupa.com
Other information needed to identify the organization:	Attention: Coupa Legal Department

(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 specified in **<u>Appendix 1</u>**.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

[1] References to the repealed Directive 95/46/EC shall be construed as references to the GDPR, see Art. 94 GDPR.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case, the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[2]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

***

[2] *This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.*

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The "Customer" in the applicable subscription service for the use of the Coupa Platform and Hosted Applications.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

The data importer will provide a business spend management cloud solution to the data exporter to support the optimization of transactional and operational processes of the data exporter. The data that is provided and created by the data exporter will be housed in a 3rd party data center. The data importer provides 24x7x365 support and has support centers in the EEA, United States of America, and India. In the course of the aforementioned activities, Coupa and its Subprocessors may require access to Customer Data to fulfill their obligations under the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Users and contacts at Customer's business partners (e.g. suppliers or similar third parties) of the data exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

a) Data exporter's User data:
- Email address
- First and last name
- Optional: nick name, picture, employee ID, phone and/or fax number, legal entity and cost center

b) Data exporter's business partner contact data:
- Contact email address
- Contact first and last name
- Optional: phone and/or fax number

c) Such other personal data as the data exporter may configure the Hosted Application to collect and to process

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

No special categories of data will be transferred by the data exporter.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The data exporter's Coupa instance will be hosted in a data center in the region specified on the applicable Order Form. The data exporter's supplier contact data will be hosted centrally on the Coupa Supplier Portal (https://supplier.coupahost.com/).

In the scope of providing the Coupa Platform and Hosted Applications, including technical support, Coupa and its Subprocessors may need access to or process the personal data that is entered by data exporter into Coupa's database in order to provide the subscription service. For more details around Subprocessors used by Coupa in the provision of the service please go to https://success.coupa.com/subprocessors.

***

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

(1) Coupa shall collect, process, and use data related to data subjects only within the scope of the Agreement and the processing instructions issued by the data exporter.

(2) Coupa shall implement and maintain technical and organizational measures to adequately protect the data exporter's data as further described below:

(a) ORGANIZATIONAL ACCESS CONTROL

(i) ***Control Environment***. Coupa employees are required to sign a written acknowledgement form documenting their receipt and understanding of the employee handbook and their responsibility for adhering to the policies and procedures therein. Employees are also required to sign a confidentiality agreement agreeing not to disclose proprietary or confidential information, including customer information, to unauthorized parties.

(ii) ***Access Administration***. Coupa employees do not have direct access to Customer Data, except where necessary for Technical Support, system management, maintenance, backups and other purposes separately authorized by Customer in writing. Access to Customer Data is further restricted to technical and customer support staff on a need-to-know basis. When an employee or contractor no longer has a business need for these privileges, his or her access is revoked in a timely manner, even if he or she continues to be an employee or contractor of Coupa. Coupa's policies require Coupa personnel to report any known security incidents to Coupa management for investigation and action.

(iii) ***Personnel Screening***. Criminal background checks are performed for employees with access to Customer Data as part of the hiring process.

(iv) ***Security Awareness and Training***. Coupa maintains a security awareness program that includes training of Coupa personnel on Coupa's security program. Training is conducted at the time of hire and periodically in accordance with Coupa's information security policies.

(v) ***Subprocessors and Data Transfer***. Coupa may engage Subprocessors and other Third-Party Suppliers (each as defined below) to perform some of its obligations under the Agreement. Coupa shall require that Subprocessors only access and use Customer Data in a manner consistent with the terms of the Agreement and bind Subprocessors to written obligations to protect Customer Data. At the written request of Customer, Coupa shall provide additional information regarding Subprocessors and their locations. Customer may send such requests to Coupa's Data Privacy Officer at gdpr@coupa.com. "***Third-Party Suppliers***" means third-party contractors and suppliers engaged by Coupa in the context of the provision of the Hosted Applications or Coupa Platform. "***Subprocessors***" means those Coupa Affiliates and Third-Party Suppliers that have access to, and process, personal data within Customer Data. As part of providing the Hosted Applications or Coupa Platform, Coupa and its Subprocessors may transfer, store and process Customer Data in the European Economic Area, United States of America, India or any other country in which Coupa and its Subprocessors maintain facilities.

(vi) ***Business Continuity Management Process***. Coupa shall maintain a business continuity plan (BCP) that defines the processes and procedures for the company to follow in the event of a disaster and shall review and shall regularly test Coupa's disaster recovery plan to ensure that it is capable of recovering Coupa assets and continuing key Coupa business processes in a timely manner.

(b) PHYSICAL ACCESS CONTROL

(i) ***Physical Protection of the Data Centers***. Physical access to data centers is strictly controlled by the cloud infrastructure provider ("***IaaS Provider***") both at the perimeter and at building ingress points by security staff. The IaaS Provider only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee or contractor no longer has a business need for these privileges, his or her access is immediately revoked, even if he or she continues to be an employee or contractor of the IaaS Provider. All physical access to data centers is logged and audited routinely.

(ii) ***Availability***. Data centers are built in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move Customer Data traffic away from the affected area. The datacenters have backup power and environmental protection systems, which are regularly maintained and tested.

(iii) ***Disaster Recovery***. Coupa shall create a disaster recovery plan designed to provide appropriate technical and operational controls to deliver a recovery time objective (RTO) of no more than one day and a recovery point objective (RPO) of availability with data loss of no more than one hour for the Hosted Applications.

(iv) ***Fire Detection and Suppression***. Automatic fire detection and suppression equipment has been installed to reduce risk and damage to data center environments.

(v) ***Power.*** The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Data center facilities have power backup and environmental protection systems in the event of an electrical failure for critical and essential loads in the facility.

(vi) ***Climate and Temperature***. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

(vii) ***Monitoring***. The IaaS Provider monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

(c) **TECHNICAL SECURITY MEASURES**

(i) ***Database Protection***. Database infrastructure is segregated from the application servers and the Internet via firewalls.

(ii) ***Encryption***. All communications are encrypted between the data exporter and the data centers using high-grade encryption (AES-256). Access to Coupa's on-demand applications and services is only available through secure sessions (https) and only available with an authenticated login and password. Passwords are never transmitted or stored in their original form.

(iii) ***Intrusion Protection***. The application infrastructure is protected against intrusion by industry standard firewalls and application levels, and intrusion detection systems across all servers. Unless otherwise agreed by Coupa in writing, Customer is prohibited from performing its own penetration on any system of Coupa.

(iv) ***Instance Isolation***. Different IaaS instances are hosted on the same physical machine and are isolated from each other through the hypervisor layer. All packets pass through this layer, so that another instance has no more access to Customer's instance than any other host on the Internet (i.e. the instances look like they are on separate physical hosts). Customer instances in the IaaS Provider infrastructure have no access to raw disk devices, but instead are presented with virtualized disks.

(v) ***Malicious Software Protection***. The Hosted Applications and the Coupa Platform shall include reasonably up-to-date versions of system security agent software which shall include reasonably current and tested malware protection, patches and anti-virus protection.

(d) **RETURN OF CUSTOMER DATA.** Customer will have a period of 60 days after the effective date of termination of the Agreement ("**Transition Period**") to download any Customer Data. Customer may seek assistance from Coupa during the Transition Period to download large files. Upon such request, Coupa will promptly make available for download the data in comma separated value (.csv) format along with attachments in their native format (e.g. PDF, JPEG, etc.). For clarity, such data will not include system generated log files or Coupa specific configuration data. After the Transition Period, Coupa shall have no obligation to maintain or provide any Customer Data and may thereafter, unless legally prohibited, delete all Customer Data in its systems or otherwise in its possession or under its control. Backup copies of Customer Data will be managed subject to Coupa's data backup process.

(e) **EXCLUSIONS**. If Customer installs, uses, or enables third party services that interoperate with the Hosted Applications, then the Hosted Applications may allow such third-party services to access, use, or otherwise process and transmit Customer Data. Coupa's Security Program does not apply to any processing, storage, or transmission of data outside the Coupa Platform, and Coupa is not responsible for the security practices (or any acts or omissions) of any third-party service providers engaged by or on behalf of Customer. The Coupa Security Program excludes: (i) data or information shared with Coupa that is not stored in the Coupa Platform; or (ii) data in Customer's virtual private network (VPN) or a third-party network other than one that is under a subcontract with Coupa to assist Coupa in fulfilling its obligations in the Agreement. Additionally, Coupa shall not be liable for any data used, processed, stored or transmitted by Customer or Users in violation of this Agreement.

***