coupa

WHITEPAPER

EU GENERAL DATA PROTECTION REGULATION

December 2017

COUPA'S COMMITMENT TO DATA PRIVACY

Coupa Software, Inc. ("Coupa"; "we"; "our") is committed to providing our Coupa Spend Management Solutions to our Customers in compliance with applicable laws and regulations in general and data privacy laws such as the EU General Data Protection Regulation (**"GDPR"**) in particular.

We shall comply with these laws and regulations as they apply to Coupa as a cloud powered B2B Spend Management provider and likewise expect our Customers to comply with all applicable laws and regulations in connection with using our services.

We seek to partner with our customers and their users to help them understand how we achieve data privacy compliance as processor and how the Coupa Platform enables our customers to achieve data privacy compliance in their role as a data controller.

The terms *"personal data"*, *"data subject"*, *"processing"* and *"processor"* will have the meanings ascribed to them in the Article 2 of EU Directive 95/46/EC (**"Data Protection Directive"**) or Article 4 of Regulation (EU) 2016/679 (aka GDPR), as applicable.

PURPOSE AND SCOPE OF THIS WHITE PAPER

Effective May 25, 2018, the GDPR will replace the currently applicable Data Privacy Directive. The Data Protection Directive has been applied in all EU member states through local implementation laws. Unlike the Data Protection Directive however, the GDPR will have direct effect in all EU member states without local implementing legislation and it will override existing national privacy laws (i.e. such local laws will not automatically be voided by the GDPR but the GDPR supersedes conflicting provisions in local laws). The GDPR will eventually lead to a greater degree of data protection harmonization across EU nations which in turn shall help controllers and processors with broad geographical reach to following a consistent data privacy regime.

In this document, we focus on Coupa's Spend Management platform delivered in a Software-as-a-Service model (**"Coupa Platform"**). We will outline key components of our compliance program and our data security model within the Coupa Platform. In light of the aforesaid purpose, we focus on general EU privacy law aspects coming from the Data Protection Directive and the upcoming GDPR. Any general references, such as "legal compliance", refer to either the Data Protection Directive or the GDPR only unless we expressly refer to other legal regimes.

OUR PLATFORM AND ITS FEATURES

Coupa is a leading cloud platform for business spend, helping our customers maximize the value of every dollar they spend. Through the Coupa Platform, we offer a unique cloud based spend management solution that simplifies and unifies business processes across the many ways our customers spend money.

In summary, our Coupa Platform includes the following principal features (**"Hosted Applications"**):

- **Coupa Procurement:** Coupa Procurement provides capabilities for an organization to create a consumer-like shopping experience for their employees, allowing them to requisition and purchase products and services using the company's pre-negotiated prices.
- **Coupa Invoicing:** Coupa Invoicing provides organizations with a solution for managing their accounts payable (AP) processes.
- **Coupa Expenses:** Coupa Expenses provides capabilities for organizations to capture, manage and process expenses.
- **Coupa Sourcing:** Coupa Sourcing allows organizations to create, host and manage sourcing events.
- **Coupa Inventory:** Coupa Inventory provides organizations with real time visibility into inventory availability right as an item is being ordered via procurement.
- **Coupa Contracts:** Coupa Contracts provides capabilities to make contracts in an organization centralized, and enforceable.
- **Coupa Analytics:** Coupa Analytics provides drag-and-drop analytics dashboards that allows users to setup and configure their own analytics dashboard and reports.
- **Coupa Supplier** Information Management: Coupa Supplier Information Management (SIM) provides capabilities that allows organizations to receive additional information from their supplier.
- **Coupa Risk Aware:** Risk Aware lets customers monitor risk on their eligible suppliers* and provides the ability to take real-time action on that risk.

These features are surrounded by our Open Business Network, connecting more than three million suppliers worldwide. Combined, our cloud platform delivers amplified visibility, improved control and compliance, and ultimately increased value from every dollar they spend, allowing our customers to be more operationally fit.

EXECUTIVE SUMMARY

We carefully designed our services, as well as our legal, organizational and technical infrastructure, to meet applicable privacy requirements and to support our customers in using our Coupa Platform in compliance with the same principles.

We process only the information necessary to deliver our services in line with the instructions received from our customers. To this end, Coupa processes our customer's data (including the personal data provided therein) as necessary to serve the business-to-business (B2B) spend management needs of our customers and their end users. As a consequence, all customer data, including customer personal data, remains under full control of our customers.

Within our contractual framework, comprising a master subscription agreement (**"MSA"**) with one or more attached order forms (**"OF"**) and an accompanying data processing agreement that is compliant with GDPR (**"DPA"**), we commit to:

- **comply** with applicable laws and government regulations, including data privacy legislation, in connection with providing the Hosted Applications and/or Coupa Platform,
- **protect** the confidentiality of the customer's data in the same manner that Coupa protects the confidentiality of its own proprietary and confidential information,
- **maintain** a written information security program of policies, procedures and controls ("Security Program") governing the processing, storage, transmission and security of a customer's data,
- **engage** at our expense, an independent accounting firm to conduct an audit of Coupa's operations with respect to the Hosted Applications in accordance with the Statement on Standards for Attestation Engagements No. 18 (the "SSAE 18"), and have such accounting firm issue SSAE 18, SOC 1 Type 2 and SOC 2 Type 2[1] reports (or substantially similar report of a successor auditing standard in the event the SSAE 18 auditing standard is no longer an industry standard) (the "Auditor's Report"),
- **provide** customer and its external auditors with a current copy of such Auditor's Report, and
- **comply** with our obligations as a processor of customer data according to the instructions of our customer.

Our Security Program includes industry leading practices designed to protect customer data from unauthorized access, acquisition, use, disclosure, or destruction. Coupa periodically reviews and updates the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats. When entering into our GDPR-compliant DPA, we enclose and execute the EU Model Clauses to create a recognized compliance framework. Moreover, we comply with necessary organizational and technical measures and we have implemented additional security measures that go beyond the legal requirements (as further described in the Coupa DPA).

[1]The SOC 2 report includes the Security, Confidentiality, and Availability Trust Principles.

DATA PRIVACY COMPLIANCE FRAMEWORK

CONTROLLER VS. PROCESSOR

Coupa will generally qualify as the processor with regard to all personal data coming from the customer. According to Article 2 (e) of the Data Protection Directive, a data processor (Coupa) is an entity that processes personal data on behalf of the controller (our customer). The role of Coupa as the processor of personal data on behalf of our customers will not change under the GDPR. Under the GDPR a processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Thus, Coupa will continue to qualify as processor with regard to personal data coming from our customer.

COUPA AS A COMPLIANT PROCESSOR VIS-À-VIS OUR CUSTOMERS

Article 17 of the Data Protection Directive and Article 28 of the GDPR detail the compliance requirements when a controller engages a processor. Such requirements include - amongst other obligations - the execution of a contract that (i) sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller, (ii) the processor processes the personal data only on instructions from the controller, including with regard to transfers of personal data to a third country, and (iii) the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Coupa documents all of the foregoing requirements in its MSA and DPA including through the use of the EU Model Clauses. We define requirements for adequate technical and organizational measures in our MSA and DPA. Within the DPA we specify the hosting location of the customer (within the EU, US or in another location currently serviced by Coupa) and also list Coupa supplier's that qualify as a sub-processor.

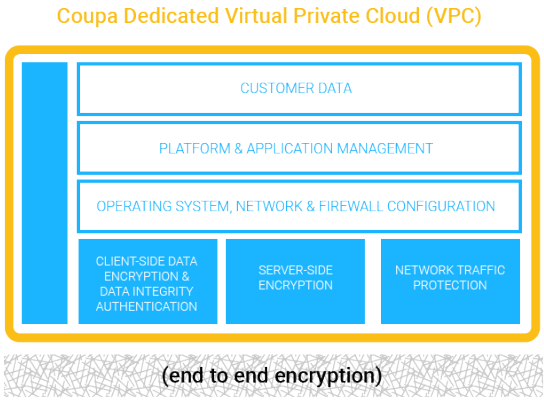
As part of our services, we may compile aggregated content and usage information that has removed all personally identifiable information for statistical or analytics purposes. This does not impact our role as a processor. The aggregated data is purely anonymous and does not qualify as personal data under European privacy law.

Information Security

Coupa is committed to providing customers with reliable, secure applications that allow them to manage their spend management processes from anywhere, at any time, through a compatible website browser. To this end, Coupa has partnered with Amazon Web Services Inc. (**"AWS"**) to provide the hardware and infrastructure to facilitate our services. Coupa uses state-of-the-art and highly-available AWS Data Centres within the EU and worldwide. The following tables provide an overview of the Coupa Platform architecture based on AWS:

Table A - Overview

Coupa operates the services and manages the platform which is hosted in a dedicated Virtual Private Cloud (VPC)

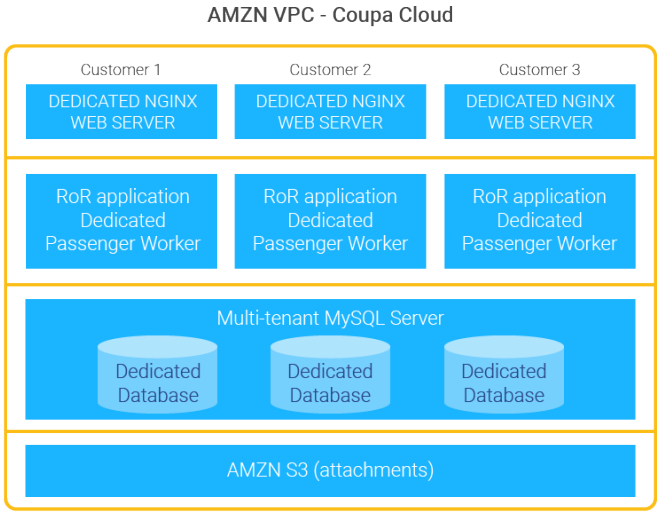


Coupa standards:
SSAE 18 SOC1 Type I
SSAE 18 SOC2 Type II
ISO 27001
TUV Rheinland Cloud Certification
PCI
HIPAA

Amazon provides secure infastructure and services

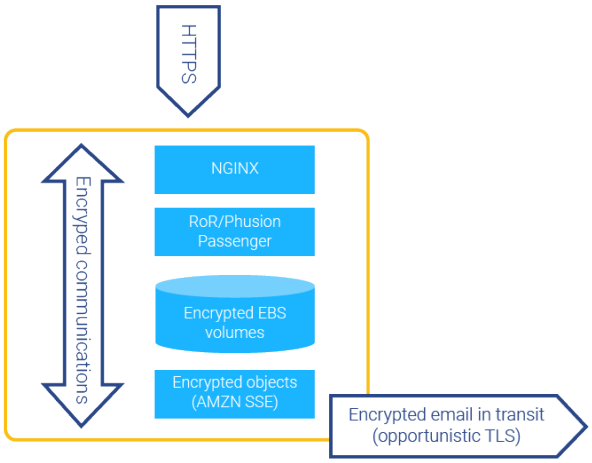
Amazon standards:
SOC1, SOC2, SOC3 FISMA, DIACAP, FedRAMP, DOD CSM Levels 1-5, PCI DSS Level 1, ISO 27001, ITAR, FIPS 140-2, MTCS Level 3

Table B – Coupa Multi-tenant architecture



- Everyone running the same version of the code
- Customers fully segregated
- No shared app servers
- No co-mingling of customer data
- Each DB with a customer specific password

Table C – Coupa Virtual Private Cloud



- Encryption keys managed by AMZN KMS
- AES 256 encrypted file systems using EBS encryption
- Encrypted Communications (outside & inside)
- Each file encrypted on AMZN S3 with its own encryption key
- Encrypted email channel if supported by the customer

EU Model Clauses

Within our DPA we use the Standard Contractual Clauses (processors) adapted by the EU Commission under Commission Decision C(2010)593 (**"EU Model Clauses"**). The EU Model Clauses are typically used in agreements between service providers (such as Coupa) and our customers to ensure that access to personal data from outside the EEA and any transfer of personal data outside the EEA meet the requirements of the Data Protection Directive. The use of EU Model Clauses is also valid under the GDPR.

The EU Model Clauses allow the commission of sub-processing and in addition provide for a certain degree of flexibility, as the parties may add individual business-related clauses as well as further amendments as requested by EU data protection authorities.

We believe that the use of the EU Model Clauses in connection with our DPA and MSA is the most robust way to structure the transfer of personal data to a processor such as Coupa. Additionally, data protection authorities recommend the use of EU Model Clauses for data transfers from an EU-based controller to a processor in a third country. Correspondingly, Coupa strives to do everything possible to help our customers implement a compliant contractual structure.

Coupa's Sub-Processors

Coupa generally limits the number of sub-processors that need to or may have access to customer personal data to an absolute minimum. Consequently, Coupa uses only a small number of sub-processors to provide its services to our customers on the Coupa Platform. The primary sub-processors used in the Coupa Platform are (1) our host provider AWS with worldwide hosting locations, (2) our network operations center provider IndMax IT Services Private Limited, India and (3) certain Coupa group companies with support services locations in the EEA and India.

We selected AWS as our primary hosting provider because AWS has implemented advanced additional security measures which go beyond the legal requirements in order to keep our customers' data as safe as possible.

When we acquire other companies and organizations with a different IT infrastructure setup we may continue using other sub-processors for an interim period until full architectural transition to the Coupa Platform has occurred. Such exceptions are detailed in our contracts if and when applicable.

We have taken great care in building our sub-processing structures transparently and in compliance with applicable EU privacy law. We maintain an up-to-date list of sub-processors for our customers and conduct due diligence and sign appropriate terms with those sub-processors.

OUR CUSTOMERS AS CONTROLLERS

Our customers are the controller of the personal data populated on the Coupa Platform and therefore have to comply with their obligations under the Data Privacy Directive and the GDPR. One side of these obligations relates to the controller-processor relationship we refer to in this white paper (see Sections above), while the other side relates to the controller obligations vis-à-vis the data subject (i.e. employees, contractors, partners and suppliers, etc. of our customers).

As a user of the Coupa Platform, we expect our customers to comply with all applicable laws and regulation in connection with the use of the Coupa Platform, in particular making sure, that our customers have all rights and consents necessary to allow Coupa to use and process such data on the Coupa Platform.

As the service provider of the Coupa Platform, we are committed to support you in your compliance activities and in meeting your obligations vis-à-vis the data subject as outlined in GDPR Chapter III (Rights of the data subject), most notably the rights of access and rectification (Art. 15 + 16 GDPR), right to erasure or 'right to be forgotten' (Art. 17 GDPR), right to data portability (Art. 20 GDPR), right not to be subject to automated decision-making, including profiling (Art. 22 GDPR). Coupa provides its services with the aim to enable our customers to be compliant. In particular, we can support our customers by making certificates and mandatory documentation available (including third-party certifications and audit reports). Of course, as a Coupa customer you will remain in control of the data provided to us on the Coupa Platform at all times.

ACTIONS THAT COUPA UNDERTAKES TO COMPLY WITH THE GDPR

Many of the main concepts and principles of GDPR are similar to existing EU data privacy laws. Therefore, much of our current approach will remain valid under the GDPR. However, the GDPR introduces new elements and important enhancements that require detailed consideration by all organisations involved in processing personal data.

To that end, Coupa has been carrying out a "GDPR readiness" project that comprises a "review and enhance" analysis of current or envisaged data processing in line with GDPR. The "GDPR readiness" project will help ensure that Coupa has adequate procedures in place to address the improved transparency, accountability and individuals' rights provisions, as well as optimising our approach to governance and how to manage data protection under the GDPR.

In 2017 Coupa received the TÜV Rheinland "Certified Cloud Service" certificate which is based on essential information security standards such as ISO 27001, as well as additional standards issued by the German Federal Office for Information Technology and ITIL. This certification demonstrates Coupa's commitment to a robust quality and security program that has been independently tested.

Coupa is thus keenly aware of the GDPR requirements that our customers and prospects, and for that matter Coupa itself, will face come May 2018. To that end, Coupa has taken the following steps to ensure that we will be in compliance before the May 2018 deadline:

- Kicked off internal "GDPR readiness" project in the beginning of 2017
- Achieved ISO 27001 certification in June of 2017
- Added a Germany based and German law qualified senior IT lawyer with extensive industry and data privacy experience to our legal staff in June of 2017
- Achieved TÜV Rheinland Certified Cloud Service certification in September of 2017
- Updated our DPA to be GDPR-compliant in October 2017
- Providing awareness and training to the Coupa village
- Providing public guidance and position papers to our prospects and customers

GDPR & "FUD" (AKA FEAR, UNCERTAINTY AND DOUBT)

The GDPR rightfully draws a lot of attention in the market. And, in the words of the European Commission this means:

> *"The Regulation is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. A single law will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year."*

Coupa fully supports this goal and strives to partner with prospects and customers in their compliance activities, every day. We trust that the GDPR brings about an effective and efficient way to support data privacy compliance in what Coupa and our customers do.

On the other hand, the GDPR is also drumming up lots of uncertainty ahead of the May 2018 deadline. If you're unsure about all the commentary around GDPR, we recommend you follow the GDPR myth buster blog series of the UK ICO and perhaps start with the following post "GDPR – sorting the fact from the fiction".

STAYING CURRENT

Ensuring the privacy and security of our customer's data is an ongoing commitment for Coupa. As we continue to approach the May 2018 GDPR deadline we will update this white paper to reflect any GDPR-related developments.

Please consult www.coupa.com/gdpr for the latest version of this document.

Of course, Coupa is happy to discuss any privacy aspect with you at any time!
If you have any questions, please contact us via e-mail (gdpr@coupa.com).

LEGAL DISCLAIMER -

This white paper is provided for informational purposes only and should not be considered as a contractual commitment or legal advice and does not discuss other privacy-related laws or regulations that may also be relevant to our customers and prospects, including any industry specific requirements. The relevant privacy and data protection laws and regulations applicable to individual companies will depend on several factors, including but not limited to where a company conducts its business, the industry in which it operates, the type of content it wishes to store, where or from whom the content originates, and where the content will be stored.

ABOUT COUPA

Coupa Software (NASDAQ:COUP) is the cloud platform for business spend. We deliver “Value as a Service” by helping our customers maximize their spend under management, achieve significant cost savings, and drive profitability. Coupa provides a unified, cloud-based spend management platform that connects hundreds of organizations representing the Americas, EMEA, and APAC with millions of suppliers globally.
The Coupa platform provides greater visibility into and control over how companies spend money.
Customers – small, medium, and large – have used the Coupa platform to bring billions of dollars in cumulative spend under management. Learn more at www.coupa.com.

CONNECT WITH US ON SOCIAL:
Facebook: https://www.facebook.com/coupasoftware
Twitter: https://twitter.com/Coupa
Linkedin: https://www.linkedin.com/company/coupa-software