Quick Guide: Coupa's Privacy Program

Overview

We designed our privacy program with the following objectives in mind:

- To support our customers' compliance efforts and to reflect the international footprint of our customers' and of our own operations;
- To align with trusted and tested data privacy and governance frameworks to ensure robustness of our privacy efforts;
- To go beyond the legal obligations and to meet the expectations of broader groups of stakeholders.

In this document you can find out more about our privacy program.

The Global Scope of Our Privacy Program

Coupa's privacy program is mapped to the GDPR, CCPA, CPRA, VCDPA, CPA, UCPA, CTDPA, FedRAMP, HIPAA, PIPEDA, and the privacy laws of Mexico, Brazil, Colombia, South Africa, Australia, Singapore, Japan, China, India, and the United Kingdom.

We analyzed from which countries our customers' users access our platform, and these jurisdictions account for more than 90% of our users. We monitor regulatory developments globally and evaluate their impact on our own and our customers' operations.

Our privacy program is reviewed and updated on a regular basis to maintain its relevance. All changes to our products go through a rigorous review process to ensure privacy requirements are embedded.

Trusted and Tested Data Privacy and Governance Frameworks

Coupa's privacy program is ISO 27701 and Global PRP [1] certified, and it is integrated into our Enterprise Risk Management process together with all other significant compliance domains. In this way all compliance efforts are coordinated, and there is both a top-to-bottom and bottom-to-top information flow cross-functionally to manage compliance requirements and expectations.

Additionally, we follow a holistic approach to have a risk-based privacy program which addresses more than just regulatory risks. To achieve this, we adopted practices of mature governance frameworks such as the Sarbanes-Oxley Act to create a comprehensive risk and control matrix for our privacy activities. This approach ensures accountability and design and operating effectiveness of our privacy program on a continuous basis where privacy controls are documented with the same rigor as for financial reporting purposes.

---

[1] The Global PRP System Certification Mark™ is a trademark of the International Trade Administration/ Office of Global Data Policy and Privacy, used with permission.

Meeting Stakeholders' Expectations Beyond Legal Obligations

Coupa's privacy program is aligned with the GRI and SASB sustainability standards as we believe data privacy is more than just regulatory compliance. We view privacy as a fundamental human right which impacts both data subjects and our society.

We anticipate ESG standards becoming part of mandatory external reporting practices, and we designed our privacy program accordingly to meet such requirements.

We regularly benchmark our privacy program using various maturity models and best practices to keep it up-to-date and best in class. The ComplOrg model, presented below, describes how compliance domains typically mature over time within organizations:

	Maturity levels	Brief description
01	Sporadic and ad-hoc	The focus is on the most apparent/critical areas but this may leave the organization exposed to a lot of compliance vulnerabilities
02	Planned but not comprehensive/ documented	There is a deliberate focus on the most important areas but the compliance program may not be comprehensive and/or the organization may not be able to demonstrate compliance in the absence of appropriate documentation
03	Comprehensive and documented	The compliance program is comprehensive and the compliance activities are documented
04	Aligned with voluntary ESG	Compliance can support voluntary ESG reporting with the relevant data and metrics to satisfy key stakeholders' expectations
05	Integrated compliance function	All compliance domains are considered, and a formal risk assessment is conducted to justify why any individual domains are not viewed as significant and why they are excluded from the integrated compliance function's scope
06	Integrated into ERM	Compliance domains are linked to the organization's ERM function
07	Integrated into external reporting	Compliance domains provide input into the organization's mandatory external reports

As demonstrated above, our privacy program is comprehensive, documented, aligned with key ESG standards, integrated with all significant compliance domains and into ERM, and it is ISO 27701 and APEC PRP certified.

Publications

We prepared a number of documents on specific privacy-related topics which you may find helpful for your compliance efforts:

- GDPR Transfer Risk Assessment
- FISA Statement
- Data Subject Requests and Enquiries Policy
- China Privacy and Security Whitepaper

These documents are available upon request. Please reach out to your Coupa contact to obtain them.

***