Cisco Privacy Insights

Privacy Data Sheets—Proactive Answers

Transparency builds trust and avoids sales delays

Data privacy: growing concern for people, customers—and our company

At Cisco, we're committed to openly sharing how our products and services process customer data. "Privacy is a fundamental human right," says Chuck Robbins, Cisco CEO, "We need security and transparency to protect it."

Before purchasing our products and services offerings—especially cloud services—customers are asking important questions about how we govern, protect, and manage their data. What do we collect and why? Where is data stored and for how long? Is it transferred, especially across countries or continents? If so, what is the legal transfer mechanism?

Today's heightened awareness of data privacy comes from several fronts:

- Recent highly publicized data breaches that had a direct impact on people. "Privacy is a boardroom issue now. Companies won't do business with a company that can't explain how it uses and stores data," says Robert Waitman, Cisco director of data valuation and privacy.
- Privacy legislation is growing worldwide. More than 80 countries have privacy regulations, including Europe's General Data Protection Regulation (GDPR), whose 4% fines got everyone's attention; Canada's Personal Information Protection and Electronic Documents Act (PIPEDA); and Singapore's Personal Data Protection Act (PDPA). Federal legislation is also widely expected in the U.S.
- Increasing awareness by vendors that privacy concerns are not just a regulatory concern but also a business matter. In the 2019 Cisco Data Privacy Benchmark Study, 87% of respondents (up from 65% in 2018) said that customer questions about data privacy cause sales delays—an average of 3.4 weeks for organizations meeting all or most GDPR requirements, 4.5 weeks for organizations that aren't yet ready but to expect to be within a year, and 5.4 weeks for organizations that are over a year away from being GDPR-ready.

Cisco's focus on data privacy has grown since we expanded our product portfolio from products that move data (like switches and routers) to services that process data (like cloud-based services for collaboration, security, and analytics). "Customers increasingly need to know the who, what, where, when, and how of what we do with their data," says Lisa Bobbitt, Cisco privacy architect.

> "Privacy is a boardroom issue now. Companies won't do business with a company that can't explain how it uses and stores data."
>
> - Robert Waitman, Director of Data Valuation and Privacy, Cisco

Before, finding answers delayed sales and tied up legal teams

Questions about data protection and privacy crop up all along the sales cycle, escalating at the end, when customers review terms and conditions. "Our contract says data can be used in any ways legally permissible and can be shared with third parties," says Jennifer Mann, contracts negotiator in our Legal Global Center of Excellence (GCOE). "Before finalizing the sale, customers say they want more clarity."

Responsibility for answering these questions falls to our contract negotiators and privacy team. Fast, accurate answers avoid sales delays and show our commitment to transparency. But in a company as large as ours, with as many products and services, tracking down the answer to even one question can easily take 2–3 days.

Take Webex Meetings, for example. Frequently asked questions include: What kind of data do you collect? How long do you keep the call recording? Do you store anything else? Why do you need that information? In which country is the data stored, and will it be transferred? Similarly, customers considering our Cloud Email Security service want to know what we do with emails after they're scanned. (Answer: either send it on to the destination or delete it.)

Until recently, our contract negotiators contacted the business unit's lawyer for answers to customers' privacy questions. A lawyer who didn't know the answer asked engineers or product teams. But this one-off approach didn't scale. In some cases the back and forth took months—delaying sales and tying up product managers, legal or compliance team, and local engineers. Another problem: different engineers sometimes gave different answers depending on the depth of their knowledge.

We wanted to be more proactive. "Providing data privacy-related information quickly and accurately isn't just a GDPR requirement, it's a business necessity," says Jonathan Fox, director of privacy engineering for the Cisco Security and Trust Organization. "Answering questions before they are asked makes it easier for customers to engage with us."

> "Providing data privacy-related information quickly and accurately isn't just a GDPR requirement, it's a business necessity."
>
> - Jonathan Fox, Director of Privacy Engineering, Cisco Security and Trust Organization

Solution: privacy data sheets for our data-rich products and services

Rather than keeping engineers and lawyers tied up in conversations, we decided to get out in front of the challenge by creating a privacy data sheet for products and services that collect or store data. "Our goals for the privacy data sheets were to help customers with compliance, strengthen our trusted relationship, and avoid sales delays by providing information customers need without their having to ask," says Lorena Marciano, EMEAR data protection officer.

We published the first privacy data sheet in January 2018. As of April 2019 we have more than 30, available for download here.

The team

We formed a cross-functional team to create the privacy data sheets:

- Data privacy team and their lawyers
- Product teams and their lawyers
- Product or service technical leads
- Sales teams and contract negotiators—to provide the privacy-related questions that customers ask

The content: it starts with privacy engineering

The Cisco Secure Development Lifecycle (SDL) has always included data requirements, and we added privacy engineering in 2016. "Privacy engineering starts with scoping business objectives, privacy policies, the market, and the data needed," says Bobbitt. When product design begins, the privacy engineering team conducts a data impact assessment, noting the

data content, classification, context, and controls for meeting the appropriate data policies. Some of the questions we ask: How confidential is the data? Does it include personally identifiable information (PII), which identifies an individual or could reasonably linked to the individual's laptop or mobile device? Where is the data processed? What's the location of the person the data could identify? How long will we keep the data and how will we delete it?

We map the answers to controls that enforce our policies for governance, protection, and privacy. The data sheets explain the processes and technology we use to put the controls in place.

The first privacy data sheet we developed was for Webex Teams. Built the Agile way, with more than 100 microservices, Webex Teams has especially complex data privacy controls. We frequently add new features, many of which have privacy implications. For example, in early 2019 we integrated Webex Teams with People Insights, which provides business and professional profiles of meeting participants. Therefore, we conduct a privacy impact assessment at every software development milestone to address potential privacy risks and implement the appropriate controls.

Webex Teams Privacy Data Sheet

Identifying the information to include

Our goal is to answer the questions that the majority of our customers ask, in sufficient detail. (Some customers require specialized information.) We started with the most common questions that we receive, which involve:

- PII processing
- Cross-border data transfers
- Access control
- Data portability
- Data deletion and retention
- PII security
- Third-party service providers
- Information security incident management
- Certifications and compliance with privacy laws
- Controls for processing personal data

Business value for the company—and our customers

"Customers say that privacy data sheets are the gold standard—providing the right information in the right level of detail for them to complete a purchase," Fox says. Bearing out this observation, privacy data sheets are one of the top downloads from our Trust Center website: well over 1000 monthly downloads on average during the second half of 2018. In the second quarter of 2019, our Legal Global Center of Excellence sent out privacy data sheets for half of all privacy cases—and for more than 70% of requests that required a quick answer. "The sales force considers the privacy data sheets fantastic assets for helping them close deals much faster," says Thomas Flambeaux, Webex privacy consultant.

Privacy data sheets benefit our companies in the following ways:

Building trust and transparency

Anticipating the information customers need makes it easier for them to do business with us. “Now there’s one less friction point for customers,” adds Miguel Rostagno, contracts negotiator. “They don’t have to wait while we research the answers to their privacy-related questions.”

Helping us close deals sooner so customers can start benefiting from the solution

“Finding answers to customers’ privacy questions used to take at least 2-3 days,” says Sofia Gonzalez, contract negotiator. “Now when a customer asks about privacy matters, I just send the privacy data sheet. In many cases they don’t come back with follow-up questions, and they even want the data sheet to be part of the contract.” Flambeaux adds, “Customers appreciate that we now make this information public. It shows we’re trustworthy.”

> “Finding answers to customers’ privacy questions used to take at least 2-3 days. Now when a customer asks about privacy matters, I just send the privacy data sheet. In many cases they don’t come back with follow-up questions, and they even want the data sheet to be part of the contract.”
>
> - Sofia Gonzalez, Contract Negotiator, Cisco Legal Global Center of Excellence

Simplifying business

When customers advise the contract negotiator that they will be redlining a contract, the negotiator asks if any of the concerns are privacy or data-protection related. If so, the negotiator can often preempt the changes by sending the privacy data sheet. “Customers typically say ‘this is great,’ and most often don’t redline the contract,” Mann says.

Conclusion

We have always responded promptly to customer inquiries about data privacy. “The sea change is that we’re now sharing information before the question is even asked,” Waitman says. “The privacy data sheets are simplifying the business, reducing sales friction, and reinforcing that we are a trustworthy partner.”

For more information

Privacy data sheets

Cisco 2019 Data Privacy Benchmark Study

Data map infographics

Note

This publication describes how Cisco has benefited from the deployment of its own products, processes, and policies. Many factors may have contributed to the results and benefits described. Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties; therefore, this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**