Compliance

slack

Table of contents

Introduction

Slack complies with applicable privacy and security mandates to meet global industry standards. In order to assist your team in understanding Slack's compliance measures we've gathered key compliance resources for your convenience.

While Slack has developed and cultivated tools, policies and certifications necessary to help our customers meet their regulatory obligations, customers are ultimately responsible for ensuring their use of the Slack Service meets their legal and compliance obligations.

Data collection

Slack understands that your organization may need to comply with complex international, regional, and industry-specific requirements governing the collection and use of data. For a detailed list of what data Slack collects, uses and discloses, and how Slack categorizes that data please see Slack's Privacy Policy section: "**Information we collect and receive**."

Slack uses "Other Information" in furtherance of our legitimate interests in operating our Services, Websites and business. For more information please visit the slack **Privacy Policy**.

Compliance certifications and regulations

Slack meets and exceeds some of the most broadly recognized security standards and offers solutions to help you address your compliance requirements. To download many of these certificates and for more details please visit us **here**. For additional support, please contact yoursales representative.

Key topics

Please review the highlighted key topics in the following Q&A which address many of the most commonly asked questions:

Do you have a Data Protection Officer (DPO)?

Yes. To communicate with our Data Protection Officer, please email dpo@slack.com.

Can I control where my data is stored?

Yes. We provide the option to store certain categories of **customer data** at rest (including messages, posts, files and search index) in a variety of countries and regions

Do you perform privacy impact assessments?

Yes. We have a formal privacy risk assessment process that incorporates the principles relating to processing of personal data. More information regarding data

Slack certifications and attestations

	ISO IEC 27001		ISO/IEC 27017
	SOC 2		SOC 3
	ISO IEC 27018		FedRAMP Moderate
	CSA		APEC Privacy
	APEC Processor		

processing can be found in the '**Information we collect and receive**' and the '**How we use information**' sections of our Privacy Policy.

Do you use a third party to provide the required services?

Yes. Slack currently uses third party subprocessors to provide infrastructure services, and to help us provide customer support and email notifications. You can see a list of the vendors and their data hosting locations **here**.

Do you transfer data to third countries?

Please refer to the **International Data Transfer** section of our Privacy Policy, the entities listed on our **Affiliates page** and vendors listed on our **Subprocessors** page.

Slack offers European Union Model Clauses, also known as Standard Contractual Clauses, to meet the adequacy and security requirements for our customers that operate in the European Union and the United Kingdom. A copy of our standard data processing addendum, incorporating Model Clauses, is **available here**.

What is your data retention policy?

Customers determine the data retention for their messages and files. For more information, see **here**.

Customers on paid plans can set specific retention settings for their workspace. For more information see **here**.

Within 24 hours of customer initiated deletion, Slack hard deletes all information from currently-running production systems. Slack services backups are destroyed within 14 days. Refer to our **security practices** page for more information.

Is there a destruction schedule or a process in place to return data to the customer?

Yes. Customer Data is removed immediately upon deletion by the end user or upon expiration of message retention as configured by the customer.

You can read more about data destruction in our **Security Whitepaper** for more details.

Slack does provide data portability options to our customers and you can learn more information about our data management tools **here**.

Does Slack require its employees to receive security and privacy training?

Yes. Every Slack employee receives mandatory privacy, confidentiality and security training at the time of hiring and is required to take annual follow-up training. Employees also receive regular awareness training via informational talks and presentations.

Does Slack assist its customers in responding to data subjects seeking to exercise their rights?

Yes. Slack forwards requests for Customer Data (message and file information), as well as requests for personal data deletion or erasure to the workspace primary owner. The primary owner has ultimate control over the workspace, can assist with access and deletion requests, and generally acts on behalf of the company they represent.

Additionally, Slack has implemented a process for responding to data subject access requests for personal data it controls. As a data processor, Slack controls only "Other Information" as described in the Privacy Policy.

How does Slack accommodate educational customers' privacy requirements?

For information on our Slack for Education Program please visit our **help center**. Please note that per our **Terms of Service**, anyone under the age of 16 may not use Slack.

Also see our **Customer-Specific Supplement** and our **FERPA Policy** for more information on compliance with the U.S. Family Educational Rights and Privacy Act.

For more information, we encourage you to review our extensive privacy and security content that's available in our **Trust Center** and to review the following **security documentation:**

- **Slack Security overview including 3rd partyand ISO certifications**

- **Slack Security practices**

- **Slack Security Whitepaper**

- **Downloadable Slack datasheet**