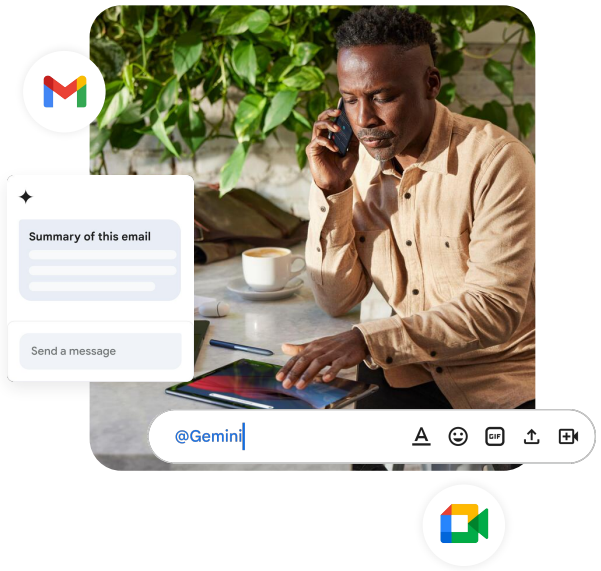
Google Workspace

Safeguarding your organization's data with Gemini



Building helpful, secure, and safe products that give users and customers choice and control over their data has been a bedrock principle for us for 25 years. With Google Workspace, we've long shared robust privacy commitments that outline how we protect user data and prioritize privacy. Generative AI doesn't change these commitments — it reaffirms their importance. Here are some key facts about how your organization's data in Google Workspace is handled[1]:

Data confidentiality

Your data is your data, and it does not belong to Google. We don't use your data, user prompts, or generated responses to train Gemini models outside of your domain without permission. We don't sell your data or use it for ads targeting. You can delete or export your data at any time.

Compliance

Gemini is one of the first generative AI solutions to attain a comprehensive set of safety, privacy, and security certifications, such as SOC 1/2/3, ISO 27701/17/18, 9001, and 42001, to help you address regulatory requirements. Gemini can help you meet HIPAA compliance and was also submitted for FedRAMP High authorization.

Data protection

Gemini respects existing data access and security controls in place, and only retrieves relevant data that the user has the permission to access. You can use built-in Workspace controls, such as AI classification, DLP, IRM, and client-side encryption, to help identify, classify, and protect sensitive data from oversharing risks.

IT controls

You can decide how to roll out Gemini across your organization. You can turn off/on access to Gemini in Workspace apps (for example, Gmail), the Gemini app, and NotebookLM for specific organizational units (OUs) or groups such as the legal or finance departments, to educate users and help meet regulatory requirements.

[1] Generative AI in Google Workspace Privacy Hub, Google, March 2025

Gemini in practice

	Gemini DOES NOT	Gemini DOES
Data access	Retrieve content in Google Workspace that you don't have the permission to access. For example, if you don't have access to a document in Google Drive, Gemini will not retrieve it.	Retrieve relevant content in Google Workspace based on your prompt and what you have the permission to access.
Data security	Retrieve content in Google Workspace that is protected with IRM or CSE controls. For example, if you can't download, print, or copy files based on the IRM policy, Gemini will not retrieve those files or their content on your behalf.	Automatically apply existing data security and residency controls, when you insert the generated response into an email in Gmail or a document in Google Drive.
Data privacy	Use your data, your prompts, or the generated responses to train Gemini models outside of your domain without permission.	Use your prompt and relevant content to generate a more personalized response, unique to you.

[1] Generative AI in Google Workspace Privacy Hub, Google, March 2025

Protecting customers with generative AI indemnification[2]

"If you are challenged on copyright grounds, we will assume responsibility for the potential legal risks involved."

Indemnity 1

Training data

Your company is protected against third parties claiming copyright infringement as a result of Google's use of training data. Put simply, regardless of the training data underlying all our services, Google indemnifies you.

Indemnity 2

Generated output

Your company can use content generated with Google Workspace knowing Google will indemnify you for third-party IP claims, including copyright – assuming your company is following responsible AI practices.

[2] Protecting customers with generative AI indemnification, Google, October 2023

©2025 Google LLC. All rights reserved. Google and the Google logo are trademarks of Google LLC.

Ready to get started?

Check out the Privacy Hub or sign up for a trial, available at no cost.