



# Data Privacy and Security in Google Gemini for Enterprise

## Gemini in Google Workspace (Generative AI in Gmail, Docs, etc.)

**Overview:** Gemini for Google Workspace refers to generative AI features embedded in Workspace apps (e.g. "Help me write" in Gmail, AI assistance in Docs/Sheets/Slides) as well as the standalone Gemini app. These AI capabilities are built with enterprise-grade security and privacy protections identical to core Workspace services [support.google.com](https://support.google.com). In essence, using Gemini within Workspace does **not** weaken Google's existing data protection commitments.

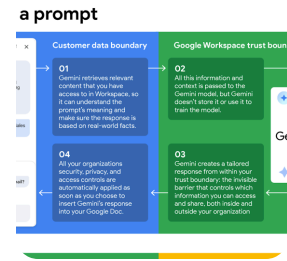
## Use of Enterprise Data and Model Training

**Data stays within your organization:** Content that your users provide to Gemini (prompts, documents, emails, etc.) **is not shared outside your organization** by the service [support.google.com](https://support.google.com/gemini/answer/12345678) . Gemini abides by all your existing Workspace access controls, meaning it can only access data that the user already has permission to view [support.google.com](https://support.google.com/gemini/answer/12345678) . For example, if you ask Gemini to summarize a Google Doc, it will only retrieve that doc's content if you have access rights.

**Not used to train Google's models:** Google explicitly commits that **your enterprise's Workspace data and prompts are not used to train or improve Gemini's models** (or any other Google models) unless you give prior permission [support.google.com](https://support.google.com/gemini/answer/12345678) [support.google.com](https://support.google.com/gemini/answer/12345678) . The Workspace Service Specific Terms include a *"Training Restriction"* guaranteeing that customer data will not be used for AI model training outside your domain without your instruction [support.google.com](https://support.google.com/gemini/answer/12345678) . In practical terms, this means internal emails or documents you process with Gemini **will not end up in Google's training corpus** for future AI model updates. Data from one customer is never used to benefit other customers [support.google.com](https://support.google.com/gemini/answer/12345678) . Additionally, **no human reviewers at Google see your prompts or outputs** by default [support.google.com](https://support.google.com/gemini/answer/12345678) , so your content isn't manually inspected.

*"The life of a prompt" in Google Workspace Gemini: enterprise data stays within a trusted boundary. The model retrieves relevant content the user has access to (Step 1), processes it **without storing or learning from it** (Step 2), and generates a response within the organization's trust boundary (Step 3). All of the organization's existing security and privacy controls apply when the AI-generated content is inserted back into a document or email (Step 4)*

[support.google.com](https://support.google.com) [support.google.com](https://support.google.com) .



**Ephemeral processing:** When using Gemini features inside Workspace, prompts and responses are **not permanently stored** by Google. They persist only for the duration of the user's session and are then discarded [support.google.com](https://support.google.com) . In other words, if an employee uses "Help me write" in Gmail, the prompt and draft output are not saved on Google's servers once that session ends. (If your organization enables the separate **Gemini web app**, which functions like a chat assistant, those chat histories are saved to the user's account for up to 18 months **but still are not used for model training or human review** [support.google.com](https://support.google.com) [support.google.com](https://support.google.com) . Admins can disable the Gemini app or adjust how long such chat data is retained once Google provides that setting.)

## Data Residency and Storage

**Processing location:** Gemini's generative AI processing in Workspace is performed in Google's global infrastructure for optimal speed, rather than a customer-specified region [support.google.com](https://support.google.com) . In practice, the service will route requests to Google data centers nearest to the user for low latency. (Google provides transparency about its data center locations and subprocessors used for Gemini [support.google.com](https://support.google.com) .) While the *computation* may happen globally, any **resulting content that you choose to keep** (e.g. an email draft or a document with AI-generated text) becomes part of your Workspace data. That resulting content **follows your data residency settings** just like other Workspace data [support.google.com](https://support.google.com) . For example, if you have a Data Region policy to store Drive files in Europe, and Gemini inserts text into a Google Doc, that doc is stored in Europe per your policy.

**Storage of prompts/responses:** As noted, prompts and responses are transient for Workspace's built-in AI features [support.google.com](https://support.google.com) . Nothing is written permanently to disk except the final user-accepted output in a document/email. The only exception is the optional Gemini chat app (if used), which stores conversation history in the user's Google account (similar to Chat history) — and even that data stays within Google's cloud and under your admin control.

## Encryption and Security

**Encryption in transit:** All data exchanged with Gemini is encrypted in transit. When a user's prompt and context are sent to the Gemini model and when the AI's response is returned, it is transmitted over secure TLS encryption [cloud.google.com](https://cloud.google.com) . This is consistent with Google's standard practice that all data within Google Workspace is protected in transit between the user and Google's servers.

**Encryption at rest:** Any customer data handled by Google Workspace (including any Gemini-related processing) is also encrypted at rest on Google's systems. Google Workspace applies the same encryption standards (e.g. AES-256) to generative AI data as it does to emails, docs, and other content [revolgy.com](https://revolgy.com) [services.google.com](https://services.google.com) . In short, whether data is temporarily cached or finally stored as part of a document, it is encrypted on disk in Google's data centers. For customers with extra requirements, Workspace also offers **Client-side encryption (CSE)** for certain data: if a document or email is CSE-encrypted such that Google cannot decrypt it, then **Gemini cannot read it either** [support.google.com](https://support.google.com) . (This provides an additional safeguard: highly sensitive content protected by your own encryption keys simply won't be accessible to the AI or Google.)

**Secure design:** Google emphasizes that Gemini brings *"the same enterprise-grade security as the rest of Google Workspace."* [support.google.com](https://support.google.com) This includes not only encryption but also protection against unauthorized access, spam/malware checks on content, and reliability features inherited from Workspace's infrastructure. The generative AI models run within a **Workspace trust boundary** that prevents data from leaking between users or organizations [support.google.com](https://support.google.com) . For example, one user's prompt or result will never be shown to another user, and the model will only retrieve data the requesting user is allowed to see, enforcing document permissions [support.google.com](https://support.google.com) . Google also filters Gemini's outputs for sensitive or disallowed content, and users can employ a "Double Check" feature (which uses Google Search) to verify AI responses – all handled under the same privacy commitments [support.google.com](https://support.google.com) [support.google.com](https://support.google.com) .

## Google Personnel Access and Privacy

Google's policies ensure that **Google employees or systems do not access your enterprise data arbitrarily**. Data handled by Gemini in Workspace is treated as **Customer Data** under Google's Cloud Data Processing Addendum [support.google.com](https://support.google.com/a/answer/9119132) , meaning Google acts as a data processor and will only access/process it according to your instructions and the agreement. **No human at Google sees your prompts or generated outputs**, unless you explicitly request support that involves accessing specific data. In normal operations, Gemini's processing is fully automated and **content is not sent to human reviewers** [support.google.com](https://support.google.com/a/answer/9119132) .

Even within the AI systems, Google maintains strict logical separation: your prompts and session data are isolated to your account. There is an "invisible barrier" (as shown above) that keeps each user's session private even from other users in the same company [support.google.com](https://support.google.com/a/answer/9119132) . In effect, your data remains confined to your domain's environment. For additional assurance, if you use **Client-side Encryption**, not even Google's servers (and by extension, not even the AI model) can decrypt or read that content [support.google.com](https://support.google.com/a/answer/9119132) . Google employees similarly **have no technical means to access CSE-protected data** [support.google.com](https://support.google.com/a/answer/9119132) , so highly confidential material can be kept completely opaque to Google while still using other Workspace features.

## Admin Controls and Data Loss Prevention

Enterprise administrators have several controls to manage Gemini's use and prevent data exposure:

- **Enable/disable AI features:** Admins can turn the generative AI features on or off for their organization or specific groups [support.google.com](https://support.google.com/a/answer/9119132) . If a company is not comfortable with these features, they can be disabled via the admin console. Likewise, the standalone *Gemini app* (chat interface) can be enabled or disabled for users [support.google.com](https://support.google.com/a/answer/9119132) .

- **Data Loss Prevention (DLP):** Existing DLP rules in Google Workspace still apply to content **generated or inserted by Gemini**. For example, if your DLP policy forbids certain sensitive data from being shared via email or Drive, and Gemini produces text that violates that policy, Workspace will treat it just as if a user typed it. The DLP system can flag or prevent the email or document containing the AI-generated text from being sent or shared, per your rules [support.google.com](https://support.google.com/workspace/answer/1258828) [support.google.com](https://support.google.com/workspace/answer/1258828) . This ensures AI suggestions don't accidentally leak sensitive info outside allowed bounds.
- **Restricting AI access to data:** Admins can use **Information Rights Management (IRM)** and classification labels on documents to prevent Gemini from accessing certain files [support.google.com](https://support.google.com/workspace/answer/1258828) . For instance, if a Drive file is marked "Confidential" and IRM prevents downloading or copying it, then Gemini will *not* use that file's content in its responses for any user who has that restriction [support.google.com](https://support.google.com/workspace/answer/1258828) . By labeling and protecting highly sensitive documents, you ensure Gemini won't include them in its analysis, even for the document owner.
- **Audit logs:** Google is rolling out **Gemini audit logging** in Workspace, so admins can monitor usage (e.g. which users are using generative AI features) similar to other Workspace audit logs [support.google.com](https://support.google.com/workspace/answer/1258828) . This transparency helps with oversight and compliance reporting.
- **Opt-outs:** As mentioned, by default Google does not use Workspace customer data for its own model training, so there is no need to "opt out" of data sharing – it's already off. If Google ever introduces any optional data sharing (for example, a program to send anonymized feedback to improve the product), those would be strictly opt-in. Admins always maintain control over whether their users' data can be used beyond the immediate AI query.

In summary, **all existing Workspace admin governance tools extend to Gemini**. Your policies for data access, sharing, and retention continue to apply. And you have full control to restrict or allow the generative AI functionality and its access as appropriate for your organization's risk profile.

## Compliance and Certifications

Google has extended its compliance programs to cover Gemini's generative AI services in Workspace. The platform has undergone independent audits and attained a broad set of certifications and attestations:

- **SOC 1/2/3:** System and Organization Controls reports for security, availability, processing integrity, confidentiality, and privacy [support.google.com](#) .
- **ISO/IEC Certifications:** Including ISO 9001 (quality management), 27001 (information security management), 27701 (privacy information management), 27017 (cloud security), 27018 (cloud privacy), and even the new **ISO/IEC 42001** for AI management systems [support.google.com](#) . Attaining ISO 42001 indicates that Google has been audited for responsible AI development and data governance practices [support.google.com](#) .
- **FedRAMP High:** Gemini in Workspace has FedRAMP High authorization [support.google.com](#) [support.google.com](#) , meaning U.S. government agencies can use it for sensitive (up to high-impact level) data, as it meets stringent federal security standards.
- **HIPAA Support:** Google has updated its HIPAA implementation guide to include Gemini, indicating it can be used in compliance with U.S. healthcare data regulations when the workspace is properly configured [support.google.com](#) .
- **GDPR and global privacy laws:** Google Workspace, including Gemini features, is covered by the Google Cloud *Data Processing Addendum* (CDPA) which addresses GDPR requirements for data processors [support.google.com](#) . Google affirms that introducing generative AI doesn't change its obligations to handle personal data in compliance with GDPR and other laws [support.google.com](#) . Customer data remains under your control and is processed according to your contract.
- **Other:** Compliance support for COPPA (children's privacy) and FERPA (education records privacy) is noted for educational usage of Gemini [support.google.com](#) . Google is also actively preparing for requirements in the forthcoming EU AI Act [support.google.com](#) .

These certifications and measures demonstrate that **Gemini for Workspace undergoes rigorous oversight for security and privacy**. In short, enterprises can use these AI features while remaining in compliance with industry standards and regulations

[support.google.com](#) .



# Gemini Advanced via API (Embedding Gemini in Enterprise Applications)

**Overview:** Gemini “Advanced” typically refers to the most powerful version of Google’s next-generation AI model, which enterprises can access via Google Cloud (e.g. through Vertex AI or an API). In this scenario, an organization might integrate Gemini’s text-generation or chat capabilities into their own internal apps, services, or chatbots. The **privacy and security model** here is governed by Google Cloud’s policies for enterprise AI services. In many respects it is similar to the Workspace scenario (no data sharing or training use by default), but it offers more customer control. Below, we cover how data is handled when using Gemini via the Google Cloud API.

## Use of Enterprise Data and Model Training

**No data exposure to model training:** Just like Workspace, Google Cloud's **Gemini API** does not use your prompts, inputs, or outputs to train the underlying AI model

cloud.google.com . Your data remains your data – it's considered Customer Data under Google's agreements, and Google will not add it to its model's learning set without permission. In Google's words, *"We do not use data that you provide us to train our own models without your permission."* services.google.com . This applies to both the content you send in (prompts) and the responses generated. The only exception would be if you explicitly opt in to a program (such as a Trusted Tester program or a fine-tuning service) that involves Google using your data – and even then it would be for product improvement or a custom model for you, **not to update the base Gemini model** cloud.google.com . By default, **enterprise API calls are isolated** – your data is processed only to generate the result and not retained for other purposes.

**Customer-controlled fine-tuning:** If your enterprise uses features like fine-tuning or code customization with Gemini (where you provide your own data to tailor the model's responses), that data and the derived model artifacts are kept within your cloud project's scope. Google notes that in the enterprise GenAI implementation, their large language model remains fixed ("frozen") and any learning from your data is stored in an *adaptive layer* attached to your instance services.google.com services.google.com . This means the base model isn't altered globally; the customization lives in your tenant. Your fine-tuning data and results are **considered your confidential data** – Google doesn't use that for others, and you can delete it when you want.

## Data Residency and Storage

**Regional processing options:** When calling Gemini via API, enterprises have **control over where data is processed and stored at rest**. Google Cloud allows you to choose regional or multi-regional endpoints for generative AI services [services.google.com](https://cloud.google.com/gemini). For example, you might choose an EU region endpoint to ensure prompts are handled in Europe. According to Google, customers can *“control what regions customer data is stored at-rest when using Generative AI and Vertex AI... by using the corresponding regional or multi-regional APIs.”* [services.google.com](https://cloud.google.com/gemini). In other words, if data residency is a concern, you can pick an endpoint in a geography that meets your compliance needs, and Google will confine data storage to that location. (As of now, Google’s Gemini models may be hosted in specific Google Cloud regions – you would select one of those available regions when making API calls.)

**Data storage and retention:** By default, Google does not persistently store your prompts or outputs from the Gemini API **beyond the processing needed to serve your request** [services.google.com](https://cloud.google.com/gemini). Google Cloud services generally might log request metadata or brief traces for reliability, but they *“do not persistently store, read, or use customer data outside your cloud tenant.”* [services.google.com](https://cloud.google.com/gemini). This means once the response is delivered, your input and the model’s answer are not saved by Google for reuse. (They are, of course, available to you to store in your own systems as you see fit.) Enterprise customers also have the ability to delete any data that might be retained through configurable settings. If any optional data logging or sampling for product improvement is in effect, it would be disclosed and under your control.

## Encryption and Data Security

**In-transit encryption:** All communications with the Gemini API occur over HTTPS with TLS encryption. When your application sends a prompt to the Google Cloud AI endpoint, the data is encrypted in transit to Google's servers and likewise encrypted when the response is sent back to you [cloud.google.com](https://cloud.google.com) . This ensures that no eavesdropper can intercept the data while it's moving between your environment and Google Cloud.

**Encryption at rest:** Any data stored on Google's side (even temporarily in memory or on disk caches during processing) is encrypted at rest by default. Google Cloud encrypts all customer data on storage media using strong encryption (AES-256) [services.google.com](https://services.google.com) . In practice, if the Gemini service writes your prompt to disk (for instance, as a temporary file or in logs stored in a secure service), that storage is encrypted. You also have the option in many Google Cloud services to use **Customer-Managed Encryption Keys (CMEK)** if needed for additional control, though for a transient AI request this may not be applicable beyond any logging you explicitly direct to persistent storage. The bottom line is that enterprise data handled by Gemini via API is protected by multiple layers of encryption by default – both as it travels and at rest in Google's infrastructure

[services.google.com](https://services.google.com) .

**Secure environment:** Running on Google Cloud means Gemini operates within Google's hardened data centers and leverages the platform's security features. Network security, physical security, and software integrity protections are the same that Google uses for its own sensitive data. Additionally, Google Cloud's **IAM (Identity and Access Management)** allows you to tightly control who in your organization or which applications can call the Gemini API, adding another layer of internal security. You may also integrate Google Cloud's **Sensitive Data Protection** tools – for example, you could use Cloud DLP (Data Loss Prevention) to redact or tokenize sensitive identifiers *before* sending prompts to Gemini, if you choose, ensuring that only necessary data is sent to the model. All these measures help enterprises use Gemini in a way that meets their security policies.

## Access by Google Personnel and Systems

**No unwarranted access:** Google's enterprise privacy commitments state that **Google personnel will not access customer content without a legitimate need** (e.g. you initiating a support request) [services.google.com](https://services.google.com/fh/files/misc/enterprise_privacy_commitments.pdf) . They have implemented *Access Transparency* logs for many cloud services, which means if any Google administrator or engineer ever does access your content, that action is recorded and visible to you. For the generative AI API, Google is extending this practice to ensure any such access is tracked [services.google.com](https://services.google.com/fh/files/misc/enterprise_privacy_commitments.pdf) . Routine operations do not involve human access at all — data processing is automated. Internally, Google's systems have strict controls and oversight to prevent misuse of customer data.

**Isolation:** Each customer's data is logically separated. When your enterprise uses Gemini via API, the requests are tied to your Google Cloud project/tenant. Google does not intermingle your data with other customers'. Furthermore, Google confirms it *"does not persistently store, read, or use customer data outside your cloud tenant."* [services.google.com](https://services.google.com/fh/files/misc/enterprise_privacy_commitments.pdf) . That means Google isn't mining your data behind the scenes; it stays within the scope of your account and the purpose of fulfilling your API calls.

**Support and troubleshooting:** In the rare case that you need Google to investigate an issue that requires looking at the data (for example, a technical support case where an AI response needs debugging), this would be done only with your consent. Google's Cloud Support procedures and the CDPA contract ensure customer authorization is obtained for any access beyond automatic processing. Any access is limited to the needed scope and is audited. This ensures that even Google employees follow a *need-to-know principle* with your Gemini API data.

## Enterprise Controls and Customization

Using Gemini via API gives enterprises flexibility in how the service is implemented and what controls to apply:

- **API/Service configuration:** You choose how and where to integrate the model. For instance, you might restrict usage to certain business applications or limit the length or nature of prompts sent. You can enforce that only specific datasets are used as context (by your application logic) and that sensitive data is filtered out. Essentially, you have full control over the **input** given to the model and can programmatically enforce your own policies (e.g., refusing to send any prompt that contains certain keywords or customer identifiers).
- **Admin governance:** If your organization uses Google Cloud, you can manage who has access to the Gemini API via Cloud IAM roles. For example, you might allow only the R&D team to use the generative AI endpoints. This prevents unauthorized or accidental use of the AI by others in the company.
- **Data loss prevention & masking:** As noted, you can integrate Google Cloud DLP to preprocess data. This is an optional enterprise-driven control: e.g., before your app calls Gemini, you run the input through DLP to mask out phone numbers or credit card numbers. This way, even though Google wouldn't store that info, you add an extra layer of assurance that certain sensitive fields never leave your environment in the first place.
- **Opt-outs and data usage settings:** There is generally no need to opt out of data sharing since none is done by default. Google Cloud does not use your content for any purpose other than to provide the service [cloud.google.com](https://cloud.google.com). In some cases, Google might offer an *opt-in* program (for example, a feedback pipeline where your app can send ratings or logs of model outputs to help Google improve the service). Participation in these is voluntary and configurable. By default, your data isn't retained for improvement, as already discussed.
- **Logging and monitoring:** You have access to logs for API calls (which can include timestamps, sizes, etc., though not full prompt content unless you choose to log it) via Cloud Logging. This allows you to monitor usage of the Gemini API and detect any anomalies or misuse on your side. You can set up alerts if usage exceeds certain thresholds, etc. Combined with Google's forthcoming **Access Transparency** for AI, you have visibility both into your usage and any Google-side access.

- **Customization:** If you use features like **Vertex AI's model tuning or prompt templates**, those give you control over how the model operates with your data. Any tuned model (even if based on Gemini) that is created for you is kept within your account. You can also delete or retrain such models as needed, ensuring you control the lifecycle of derived data. Google's contracts make clear that even when an AI model is customized with your data, Google handles that under your instructions and doesn't use it to improve their base models or share it with others without consent [services.google.com](#) [services.google.com](#) .

In summary, when embedding Gemini via the API, **the enterprise is in the driver's seat** in terms of what data is sent and how the AI is used. Google provides the secure service and honoring of data boundaries, and you layer any additional controls required by your internal policies.

## Compliance and Certifications

Enterprises using Gemini via Google Cloud benefit from Google Cloud's robust compliance stance:

- **Contractual compliance (GDPR, etc.):** Google Cloud's *Customer Data Processing Addendum (CDPA)* covers generative AI services, meaning Google is contractually bound to GDPR principles as a processor of your data [support.google.com](#) . The commitments like data usage limitations and security measures are part of this agreement. Google Cloud also has strict **data privacy commitments** published for AI, reinforcing that generative AI doesn't change their obligations [cloud.google.com](#) . Your data remains under your control, and you can execute Data Subject Requests or other compliance actions just as with any cloud data.
- **Certifications:** The same set of certifications mentioned earlier for Gemini apply to the Cloud offering as well. Systems supporting Gemini's API have been audited for SOC 2 and ISO 27001, 27701, etc., compliance [support.google.com](#) . This means the controls in place for security and privacy meet the industry standards for enterprise cloud services. If your organization requires evidence of compliance for your regulators or customers, you can refer to Google's compliance reports covering the AI services.


- **FedRAMP and government use:** Since Gemini has FedRAMP High authorization [support.google.com](https://support.google.com/fedramp) , U.S. government agencies and contractors can use the API in regulated environments. Google Cloud also supports various other public sector standards which would extend to the AI service under the hood.
- **HIPAA:** If you sign a Business Associate Agreement (BAA) with Google for Cloud, you can use the Gemini API with protected health information in a HIPAA-compliant manner. Google's documentation indicates that Gemini can support HIPAA compliance when appropriately configured [support.google.com](https://support.google.com/cloud/answer/9171493) .
- **Auditability:** Google Cloud provides audit logs and is subject to independent audits. They have stated that *"independent auditors validate our practices against international standards"* for Gemini [support.google.com](https://support.google.com/cloud/answer/9171493) . This external validation (e.g. auditors checking that Google truly isn't using customer data for training, etc.) gives extra assurance that the stated policies are actually followed in practice.
- **Regulatory compliance:** Whether it's GDPR in Europe, CCPA in California, or other data protection laws, Google Cloud's services are designed with compliance in mind. Data residency options, customer control over data deletion, and comprehensive security controls help you meet regulatory requirements. Google is also actively tracking upcoming regulations (like the EU AI Act) to ensure their services (including Gemini) will comply when those rules come into effect [support.google.com](https://support.google.com/cloud/answer/9171493) .


Overall, **Gemini (both in Workspace and via API) is built with enterprise privacy in mind**, ensuring that your internal data remains confidential and under your control. Google contractually commits that your data will not be used to improve their models or be accessible to others without permission [support.google.com](https://support.google.com/cloud/answer/9171493) [cloud.google.com](https://cloud.google.com/ai/gemini/privacy) . All data is secured through strong encryption and modern cloud security practices. And you have administrative tools and legal assurances to confidently deploy these AI capabilities while meeting your organization's compliance requirements. **In short, your enterprise data stays private and secure when using Google's Gemini AI solutions** [support.google.com](https://support.google.com/cloud/answer/9171493) [services.google.com](https://services.google.com/fh/articles/enterprise_privacy) .


**Sources:** Official Google Workspace and Google Cloud documentation on Gemini's privacy and security [support.google.com](https://support.google.com/cloud/answer/9171493) [support.google.com](https://support.google.com/cloud/answer/9171493) [cloud.google.com](https://cloud.google.com/ai/gemini/privacy) [services.google.com](https://services.google.com/fh/articles/enterprise_privacy) , Google Cloud privacy whitepapers [services.google.com](https://services.google.com/fh/articles/enterprise_privacy) [services.google.com](https://services.google.com/fh/articles/enterprise_privacy) , and Google Workspace blog posts on generative AI protections [support.google.com](https://support.google.com/cloud/answer/9171493) [support.google.com](https://support.google.com/cloud/answer/9171493) .





## Citations


 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**  
<https://support.google.com/a/answer/15706919?hl=en>


 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**  
<https://support.google.com/a/answer/15706919?hl=en>


 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**  
<https://support.google.com/a/answer/15706919?hl=en>


 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**  
<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**  
<https://support.google.com/a/answer/15706919?hl=en>


 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**  
<https://support.google.com/a/answer/15706919?hl=en>


 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**  
<https://support.google.com/a/answer/15706919?hl=en>


 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**  
<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**  
<https://support.google.com/a/answer/15706919?hl=en>

 **How Gemini for Google Cloud uses your data**  
<https://cloud.google.com/gemini/docs/discover/data-governance>

 **How Google Workspace keeps your data safe when using ... - Revolgy**  
<https://www.revolgy.com/insights/blog/how-google-workspace-keeps-your-data-safe-when-using-generative-ai>

 **Google Cloud - Delivering trusted and secure AI**  
[https://services.google.com/fh/files/misc/google\\_cloud\\_delivering\\_trusted\\_and\\_secure\\_ai.pdf](https://services.google.com/fh/files/misc/google_cloud_delivering_trusted_and_secure_ai.pdf)

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**  
<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

 **How Gemini for Google Cloud uses your data**

<https://cloud.google.com/gemini/docs/discover/data-governance>

 **genai\_privacy\_google\_cloud**

[https://services.google.com/fh/files/misc/genai\\_privacy\\_google\\_cloud\\_202308.pdf](https://services.google.com/fh/files/misc/genai_privacy_google_cloud_202308.pdf)

 **genai\_privacy\_google\_cloud**

[https://services.google.com/fh/files/misc/genai\\_privacy\\_google\\_cloud\\_202308.pdf](https://services.google.com/fh/files/misc/genai_privacy_google_cloud_202308.pdf)

 **genai\_privacy\_google\_cloud**

[https://services.google.com/fh/files/misc/genai\\_privacy\\_google\\_cloud\\_202308.pdf](https://services.google.com/fh/files/misc/genai_privacy_google_cloud_202308.pdf)

 **genai\_privacy\_google\_cloud**

[https://services.google.com/fh/files/misc/genai\\_privacy\\_google\\_cloud\\_202308.pdf](https://services.google.com/fh/files/misc/genai_privacy_google_cloud_202308.pdf)

 **genai\_privacy\_google\_cloud**

[https://services.google.com/fh/files/misc/genai\\_privacy\\_google\\_cloud\\_202308.pdf](https://services.google.com/fh/files/misc/genai_privacy_google_cloud_202308.pdf)

 **genai\_privacy\_google\_cloud**

[https://services.google.com/fh/files/misc/genai\\_privacy\\_google\\_cloud\\_202308.pdf](https://services.google.com/fh/files/misc/genai_privacy_google_cloud_202308.pdf)

 **How Gemini for Google Cloud uses your data**


<https://cloud.google.com/gemini/docs/discover/data-governance>

 **Generative AI in Google Workspace Privacy Hub - Google Workspace Admin Help**

<https://support.google.com/a/answer/15706919?hl=en>

## All Sources

 support.google

 cloud.google

 revolgy

 services.google

