SCANEE

SECURITY OVERVIEW

Security and privacy: where your data lives and who processes it

Scanee's hosting, AI processing, isolation, encryption, access, retention and vendors, in brief

PUBLISHED BY

Scanee (scanee.ai)

© 2026 Scanee.ai — All rights reserved.

DOCUMENT STRUCTURE

Contents

	In brief	03
01	Where your data lives	03
02	Where your documents are processed	04
03	Isolation and encryption	04
04	Access and roles	05
05	Retention and deletion	05
06	Vendors	06
07	Reporting a problem	06
	Going further	06

© 2026 Scanee.ai — All rights reserved.

In brief

- The files and data of your documents are hosted in Canada.
- To extract their data, Google's AI (Gemini) reads your documents in the United States. We say so plainly because it matters for your assessment.
- The AI does not train on your documents, neither at Scanee nor at Google.
- Each workspace is isolated from the others, and access is managed by role and by project.
- Traffic is encrypted in transit and data at rest.
- You set how long your documents are kept, project by project.

This overview describes Scanee as it works on October 28, 2026. **The full security brief**, with the details of each point and a table of answers to security questionnaires, is sent on request: write to us at support@scanee.ai.

01 Where your data lives

In Canada. The files you upload and your projects' data are hosted in Canada, at Google Cloud and MongoDB Atlas. Receiving emails and sending notifications go through Amazon Web Services' Canada region.

Sign-in accounts are the exception. Your users' identity (name, email address, encrypted password) is managed by a global Google service, outside Canada.

Your own storage. Scanee can archive your files in storage you own: Google Drive, OneDrive, Dropbox, SharePoint, Amazon S3, Google Cloud Storage, Azure Blob Storage or an SFTP server. You then control the location, the access and how long your documents are kept.

© 2026 Scanee.ai — All rights reserved.

02 Where your documents are processed

By Google, in the United States. To read a document and extract its data, Scanee sends it to Google's AI (Gemini), in the United States. The same goes for Scanee's other AI features: batch splitting, coding suggestions, search by meaning, the assistant. The extracted data then comes back to Canada.

No training. Your documents and data are not used to train AI models, neither at Scanee nor at Google. Under Google's terms for the Gemini API, Google keeps requests and responses for 55 days, only to detect abuse and meet its legal obligations.

> For a Quebec business, this processing is a disclosure of personal information outside Quebec. It belongs in your privacy impact assessment. Our white paper "Law 25: entrusting your invoices to Scanee" gives you the answers to prepare it.

A person reviews. The document is shown next to the extracted data, and your team corrects it as needed. The AI suggests; it never approves a document and never exports anything to your ERP without an action or rule on your part.

03 Isolation and encryption

Each customer is isolated. All data carries the identifier of its workspace, and every request is checked against it. Download links generated by Scanee are signed: a modified or made-up link is refused.

Where	What is in place
In transit	Traffic between your browser, your systems and Scanee goes over HTTPS (TLS)
At rest	Files and the database are encrypted by our hosting providers

© 2026 Scanee.ai — All rights reserved.

Where	What is in place
Your integration secrets	ERP access tokens, your storage keys, your webhook tokens: also encrypted by the application before they are stored
Scanee API keys	Stored as a non-reversible hash; the full key is shown only once

04 Access and roles

Sign-in. Your users sign in with email and password, or with their Google or Microsoft account. Two-factor authentication and enterprise single sign-on (SSO) are planned.

Roles. In the workspace, an administrator invites and removes users, changes roles and manages billing and integrations. In each project, a member is Admin, Editor or Reader. A user only sees the projects they created or are a member of.

No one signs in as you. The application has no super-administrator account and no feature that lets a Scanee employee sign in as a customer.

A log for every document. Creation, every field change with the old and new value, the author and the date, every status change, every export and the deletion. It answers your auditors' questions: who changed this amount, when, and what the original value was.

05 Retention and deletion

By default, nothing is deleted automatically. You turn on automatic deletion project by project, with a period in days and a mode: delete files only, or purge everything.

Your data goes with you. You can export it at any time as CSV or Excel, or to your ERP. Ending the subscription deletes no data: the workspace stays accessible so you can export or delete your data.

© 2026 Scanee.ai — All rights reserved.

06 Vendors

Vendor	Role for Scanee	Location
Google Cloud	Hosting the application and files	Canada
Google	User sign-in	Global service
Google (Gemini)	AI processing of documents, assistant	United States
MongoDB Atlas	Database	Canada
Amazon Web Services	Receiving emails and sending notifications	Canada
Stripe	Subscription billing; card numbers never pass through Scanee	United States

If you connect your storage or your ERP, those services are your vendors, under your contracts; Scanee acts there with the access you give it.

07 Reporting a problem

As a service provider, Scanee is required by Law 25 to notify your privacy officer without delay of any breach of the confidentiality of your data. To report a security problem, write to support@scanee.ai.

Going further

Filling in a security questionnaire or a privacy impact assessment? Ask us for the full security brief at support@scanee.ai: it details each point of this overview and answers the usual questionnaire questions.

© 2026 Scanee.ai — All rights reserved.

SCANEE

scanee.ai

© 2026 Scanee.ai — All rights reserved.