SCANEE

WHITE PAPER

Law 25: entrusting your invoices to Scanee

What the law requires, Scanee's role, processing outside Quebec and the answers for your privacy impact assessment

PUBLISHED BY

Scanee (scanee.ai)

© 2026 Scanee.ai — All rights reserved.

DOCUMENT STRUCTURE

Contents

	In brief	03
01	Your invoices hold personal information	03
02	What the law requires of you	04
03	Scanee's role: a provider processing on your behalf	05
04	Processing outside Quebec	06
05	Ready answers for your PIA	08
06	Individuals' rights	09
07	Retention and destruction	10
08	Confidentiality incidents	11
09	Going further	11
	Conclusion	11

© 2026 Scanee.ai — All rights reserved.

In brief

- A vendor invoice often holds personal information: a freelancer's name and address, banking details, a signature. Quebec's law then governs how you hand it over to a tool.
- Scanee acts as a service provider: it processes your documents on your behalf, to deliver the service, and for nothing else. You remain responsible for the information.
- The files and data of your documents are hosted in Canada. AI processing takes place at Google, in the United States. That is a communication outside Quebec, which calls for a privacy impact assessment (PIA) and a written agreement.
- Section 5 gives you Scanee's answers to PIA questions, in a table.
- You set retention per project, you keep a record of every change, and you can archive your files in your own storage.

This document is not legal advice. It sums up the law and describes Scanee to help you carry out your own assessment. Before making a decision, consult your legal advisor.

01 Your invoices hold personal information

Personal information is any information about a natural person that allows them to be identified. A business-to-business invoice doesn't always contain any. But a stack of invoices, receipts and statements often includes:

- the name, address and phone number of a freelancer or subcontractor;
- banking details or a void cheque;
- a signature;
- an employee's name on an expense report or a receipt;
- the name and address of an individual customer.

© 2026 Scanee.ai — All rights reserved.

As soon as a document holds this kind of information, Quebec's Act respecting the protection of personal information in the private sector, modernized by Law 25, governs how your business collects, uses, communicates, keeps and destroys it. Handing these documents to an extraction tool is a communication to a service provider.

If you also operate elsewhere in Canada, the federal law (PIPEDA) may apply. This document covers the Quebec law.

02 What the law requires of you

The obligations that apply when you entrust invoices to a provider such as Scanee:

Obligation	Section	What it means here
A person in charge of the protection of personal information	3.1	By default, the person with the highest authority in the business. They can delegate the role in writing. Their title and contact details are published on your website
Governance policies	3.2	They cover, among other things, retention and destruction of information and staff roles. Detailed information about them is published on your website
A PIA for any project to acquire an information system	3.3	Adopting a tool that processes personal information is such a project. The assessment is proportionate to the sensitivity, purpose, quantity, distribution and medium of the information
A PIA and a written agreement before any communication outside Quebec	17	Also applies when you entrust a provider outside Quebec with using or keeping information on your behalf (section 4)
A written contract with your service provider	18.3	It sets out the protection measures, limits use to the mandate and rules out keeping the information after the contract ends (section 3)
Destruction or anonymization once the purposes are met	23	Subject to retention periods set by other laws, tax laws in particular (section 7)

© 2026 Scanee.ai — All rights reserved.

Obligation	Section	What it means here
Handling confidentiality incidents	3.5 to 3.8	Reduce the risk, notify the Commission d'accès à l'information and the people concerned when there is a risk of serious injury, keep a register (section 8)
Rights of access and rectification	27, 28, 32	Respond in writing within 30 days (section 6)

03 Scanee's role: a provider processing on your behalf

In your relationship with Scanee, your business holds the information and is responsible for it. Scanee, a product of Skillztank Inc., is the service provider you entrust with a task: receiving your documents, extracting their data, displaying it for review and exporting it according to your settings.

Section 18.3 allows you to communicate personal information to a provider without the consent of the people concerned, when it is necessary to carry out the service contract, on three conditions: a written contract; confidentiality protection measures set out in the contract; use limited to carrying out the contract, with no retention after it expires. The provider must also notify your person in charge, without delay, of any breach or attempted breach of confidentiality, and allow them to carry out any verification on the matter.

What Scanee does, in practice:

Requirement	At Scanee
Use limited to the service	Your documents are used to deliver the service. They are not used to train AI models, at Scanee or at Google
Protection measures	Hosting in Canada, workspace isolation, roles, encryption, change log: described in the security and privacy overview
Retention	You set it per project. Nothing is deleted automatically until you turn it on

© 2026 Scanee.ai — All rights reserved.

Requirement	At Scanee
End of contract	Today, ending the subscription deletes no data: the workspace stays accessible so you can export or delete your data.
Notice of a breach	Write to us at support@scanee.ai
Written contract	Write to us at support@scanee.ai

Scanee itself relies on vendors to deliver the service: Google (hosting, user sign-in and AI), MongoDB Atlas (database), Amazon Web Services (email) and Stripe (subscription billing). The list, with each vendor's role and location, is in the security and privacy overview.

04 Processing outside Quebec

What happens. The files and data of your documents are hosted in Canada; the application servers are in Google Cloud's Montréal region. To extract the data, Scanee sends each document to Google's AI services (Gemini), which process it in the United States, then saves the result in Canada. Google keeps prompts and responses for 55 days, solely to detect abuse, and does not use them to train its models. If a project turns on full-text reading, the document is also read by Google Cloud Vision, whose processing location is not guaranteed to be in Canada.

Two other communications outside Quebec belong in your assessment: your users' sign-in accounts (name, email address), managed by a global Google service that does not host them in Canada, and conversations with the AI assistant, whose thread Google keeps so that questions can follow on from each other.

© 2026 Scanee.ai — All rights reserved.

What it means. Under section 17, before communicating personal information outside Quebec, or entrusting someone outside Quebec with using or keeping it on your behalf, you must carry out a PIA. It takes into account, among other things, four factors:

Section 17 factor	What Scanee provides	What remains for your assessment
The sensitivity of the information	A description of the data processed (section 5)	What your documents contain: banking details, information about individuals
The purposes for which it will be used	Extracting data for your accounting, and nothing else	That this purpose is the one for which you hold the information
The protection measures, including contractual ones	Encryption, isolation, no training, configurable retention, change log	Whether these measures are enough for your documents
The legal framework of the destination State	The location: the United States, at Google	The US legal framework, including possible access by authorities, with your legal advisor

The communication may take place if the assessment shows that the information would receive adequate protection, in particular in light of generally recognized principles of personal information protection. It must then be covered by a written agreement that takes into account the results of the assessment and, where applicable, the terms agreed to mitigate the risks.

What you can do to reduce the risk.

- Define, in each project, only the fields you need.
- Turn on automatic deletion, in "files only" or "purge everything" mode, with a period that matches your policy.
- Archive files in your own storage, wherever you choose. AI processing still takes place in the United States; only where the files are kept changes.
- Keep more sensitive documents, such as employee expense reports, in a project with restricted access.

Scanee cannot carry out this assessment for you or tell you whether it is conclusive. Our role is to give you accurate answers.

© 2026 Scanee.ai — All rights reserved.

05 Ready answers for your PIA

PIA question	Scanee's answer
What is the service?	AI extraction of data from financial documents, review by your team, export to your ERP or your files
What is the purpose of the processing?	Entering, coding, reviewing and archiving your accounting documents
What information is processed?	The content of the documents you send (which may include names, addresses, banking details, signatures), the extracted data, a summary and a search fingerprint produced by the AI, conversations with the AI assistant, and your users' names, email addresses and roles (plus their photo, phone and company if they add them)
Who are the people concerned?	Your vendors and their representatives, freelancers, employees (expense reports), individual customers, your users
Where do the documents come from?	From you: uploads, the project's email address, files you pick in your cloud folders, the API
Where are they hosted?	In Canada. In your own storage, if you turn it on. Your users' sign-in accounts are managed by a global Google service, outside Canada
Where are they processed?	At Google, in the United States, for AI extraction; by Google Cloud Vision (global endpoint) if full-text reading is turned on
Which subprocessors?	Google, MongoDB Atlas, Amazon Web Services, Stripe; see the security and privacy overview
Are documents used to train the AI?	No
Who has access in your organization?	The members you invite, according to their role (admin or viewer in the workspace; admin, editor or reader in each project) and the projects they belong to
Who has access at Scanee?	The application has no super-administrator account and no feature for signing in as a customer.

© 2026 Scanee.ai — All rights reserved.

PIA question	Scanee's answer
How is the data protected?	HTTPS in transit, encryption at rest by the hosting providers, integration secrets encrypted by the application, logical isolation by workspace
Is activity logged?	Every change to a document is recorded with the old and new value, the author and the date; status changes, exports and deletions too. Views and sign-ins are not logged
How long is data kept?	Until you delete it, or according to the automatic deletion rule you set per project
How is it destroyed?	Automatic deletion per project (files only or full purge) or deleting the project
What happens to it at the end of the contract?	No data is deleted automatically when the subscription ends; you can export or delete your data.
Backups?	Write to us at support@scanee.ai
What happens in an incident?	Write to us at support@scanee.ai
Security testing, certifications, authentication?	Detailed answers in the full security brief, sent on request at support@scanee.ai
Can access and rectification requests be handled?	Yes: document search, field correction, export to CSV or Excel
Is there a written agreement?	Write to us at support@scanee.ai

06 Individuals' rights

A person can ask whether you hold information about them, get a copy of it and ask for it to be corrected (sections 27 and 28). Computerized information collected from them is, at their request, provided in a structured, commonly used technological format, unless that raises serious practical difficulties. You respond in writing within 30 days of receiving the request (section 32).

© 2026 Scanee.ai — All rights reserved.

Your business receives the request and responds to it. In Scanee, you can:

- find the documents about that person, project by project: with a text search (title, summary, extracted text, displayed columns) or a search by meaning;
- correct an extracted field, with the change recorded in the log;
- export the data to CSV or Excel;
- delete documents that no longer need to be kept, or let the automatic deletion rule handle it.

Deleting a document by hand removes its record and its data from your projects, but the original file stays stored until the project is deleted, and the log keeps a copy of the document's data. For complete erasure, use automatic deletion in "Purge everything" mode.

07 Retention and destruction

The law requires you to destroy or anonymize personal information once the purposes for which it was collected are met, subject to retention periods set by law (section 23). For accounting records, tax laws often require you to keep them for several years. Set your retention period with your accountant or advisor.

In Scanee, the rule is set per project, in the "Storage" tab, "Data Retention & Privacy" section:

Setting	Default	Options
Auto-deletion	Off	On or off
Retention period	7 days suggested when turned on	A number of days, counted from the document's arrival
Mode	"Files only"	"Delete files only (keep the data)" or "Purge everything (delete files and the data)"

Two ways to reconcile tax obligations and minimization:

- **Keep the records on your side, not in Scanee.** Archive files in your own storage or attach the PDF to the entry in your ERP, then set a short deletion period in Scanee.

© 2026 Scanee.ai — All rights reserved.

- **Keep the data, not the files.** "Files only" mode deletes the source document and keeps the extracted data for your reports.

08 Confidentiality incidents

A confidentiality incident is access, use or communication not authorized by law, or the loss of personal information (section 3.6). If you have reason to believe an incident has occurred, you must take reasonable measures to reduce the risk of injury (section 3.5). If the incident presents a risk of serious injury, you must promptly notify the Commission d'accès à l'information and the people concerned. To assess that risk, you consider in particular the sensitivity of the information, the anticipated consequences and the likelihood of harmful use (section 3.7). You keep a register of all incidents (section 3.8).

If the incident occurs at your provider, section 18.3 requires it to notify your person in charge without delay.

To report an issue or ask a question, write to support@scanee.ai.

09 Going further

Scanee's security and privacy overview sums up hosting, AI processing, isolation, encryption, roles, retention and vendors. The full security brief details each point and answers security questionnaires: it is sent on request at support@scanee.ai. Attach it to your PIA.

Conclusion

Entrusting your invoices to Scanee means entrusting a provider with documents that often hold personal information. The law asks you to assess that choice, frame it in writing and set retention. AI processing in the United States is the main point of your assessment; this document and the security brief give you the facts to address it.

© 2026 Scanee.ai — All rights reserved.

This document is not legal advice. It sums up the law as of October 28, 2026 and describes Scanee as of the same date.

Next step. Start your PIA with the table in section 5. For a question it doesn't cover, or for the written agreement, write to us at support@scanee.ai.

© 2026 Scanee.ai — All rights reserved.

SCANEE

scanee.ai

© 2026 Scanee.ai — All rights reserved.