

Document AI Security and Data Handling

How CloudFiles Document AI handles your documents, and how you control what gets written to Salesforce

What does a security review need to know about Document AI?

CloudFiles is Document Automation for Salesforce, and Document AI runs document processes inside Salesforce: a document arrives, is read, is classified and split, is matched against records, is written where it belongs, and is held for review where someone has to sign off. Security, IT and Salesforce admin teams reviewing Document AI tend to ask the same questions about AI data handling, storage, certification and control. This data sheet answers them in the words CloudFiles publishes, and then explains the Salesforce controls that decide what document processing is allowed to change.

Does CloudFiles train AI models on our documents?

CloudFiles does not train or fine-tune AI models on your documents.

This is the question buyers ask most often, and it has a one-sentence answer. It holds for every document Document AI reads, whichever Flow action, Mapper configuration or workflow reads it.

What technology reads our documents?

Document AI uses large language models and OCR.

OCR is the reading step for scanned and mixed pages, and native PDF text is read directly. Large language models then read, classify and answer questions about the content, using the field descriptions and prompts your admins write. Before anything goes into production, a Super Admin can try prompts on a sample document in the AI Playground to see how a document will be read.

How is our data protected in transit and at rest?

TLS 1.2 or higher in transit, AES-256 at rest.

Where are our files stored?

Your files are stored in the data-residency region you choose: United States, European Union, United Kingdom or Australia.

Where do the documents themselves live?

Documents live in Salesforce Files, and with CloudFiles Document Management also in SharePoint, OneDrive, Google Drive, AWS S3, Azure Blob, Box and Dropbox. A file dropped into a connected folder can trigger processing, and classified documents can be moved into the right folder with Document Management's Move Resource action. Split Document using AI saves its outputs as Salesforce Files.

Which certifications does CloudFiles hold?

CloudFiles is independently audited for SOC 2 Type II and certified to ISO 27001, and is GDPR compliant.

Security documents are available under NDA from the CloudFiles Trust Center.

Security and IT teams that need more than this data sheet can request the full set there as part of a vendor review, before or during a proof of concept.

Does Document AI respect Salesforce permissions?

Writes respect Salesforce validation rules and field-level security. Document Mapper writes through standard Salesforce DML, so the rules your admins already enforce on a record apply to every value Document AI writes to it. Document AI adds its own guards on top:

- **A blank value never wipes a field.** In Doc AI Workflows, a value the document does not contain leaves the existing field alone.
- **Existing values can be protected.** In Document Mapper, a per-field option stops a run from overwriting a value that is already on the record.
- **References are checked before a run.** The start card of a workflow checks every object and field the workflow references.
- **Published versions are frozen.** A published workflow version does not change, so the process that was reviewed is the process that runs.
- **Testing is gated.** The AI Playground needs Super Admin.

Who decides what is written without a person's sign-off?

Review queues and approval settings decide what is written without a person's sign-off. Your admins set them per configuration and per workflow.

Where	Setting	What happens
Document Mapper	"Auto approve"	Results are written when the run finishes
Document Mapper	"Send to review queue"	Runs show Pending Review until a reviewer acts
Doc AI Workflow	"Straight through"	Steps write as the workflow runs
Doc AI Workflow	A hold on the first write	The run pauses before it writes anything
Doc AI Workflow	Approval on every write	Each write waits for a person
Workflow step	"Require approval for this write"	Only that step waits for a person

In Document Mapper, a reviewer can edit cells and add rows, then choose "Approve & Write to Salesforce" or Reject. A lookup with no match or several matches forces review, whatever the configuration says, so a missing or ambiguous match always reaches a person. In workflows, runs waiting on a person show "Awaiting review".

How is each run recorded?

Each run is recorded in Salesforce as a CloudFiles DocAI Run record.

Every run record carries its status: Processing, Completed, Pending Review, Failed or Rejected. Reprocessing creates a new run and keeps the old one, so a second pass never overwrites the record of the first. Workflows keep a step-by-step history of every run, and every pause, approval and rejection is recorded. Because run records are Salesforce records, your admins review them in the same org where the documents and the written data already sit.

How is Document AI deployed?

Document AI is part of one CloudFiles managed package alongside Document Management and Document Generation, installed from AgentExchange. Document processing runs as Salesforce Flow actions and the same invocable actions are callable from Apex, so your admins build and test it in a sandbox the way they build any other Flow. Triggers are the ones admins already know, including record-triggered Flows on an asynchronous path, CloudFiles events such as a file attached or uploaded, screen Flows and Mapper buttons.

How can our team evaluate it?

A free sandbox proof of concept is offered, so your team can run Document AI against its own documents and its own validation rules before anything reaches production. A free 14-day AppExchange trial and a Test Drive are also available. CloudFiles is headquartered in California and provides 24x7 support, and implementation and support are included.

For the full security package, request the documents under NDA from the CloudFiles Trust Center.

Get started

Install CloudFiles Document AI from AgentExchange and start a free 14-day trial or a Test Drive, or book a demo at cloudfiles.io.

CloudFiles, Document Automation for Salesforce · cloudfiles.io · Install CloudFiles Document AI from AgentExchange