

SECURITY & COMPLIANCE BLUEPRINT

How Instafill.ai protects the information you put in your forms.

This blueprint is for organizations evaluating Instafill.ai. It covers where the data in your forms goes, who can see it, how it is protected, what happens if something goes wrong, and how our controls answer the questions a vendor security review asks.

Each statement here is backed by a written policy, a contract term, or independent testing, and the underlying documents are available for your file. If your compliance team, IT department or cyber carrier has a questionnaire of its own, send it over and we'll complete it.

WRITTEN FOR

Teams that fill forms with personal and business information

And the compliance, privacy and IT staff and cyber carriers who review their vendors

PREPARED BY

BOTMAKERS LLC d/b/a Instafill.ai

Oleksandr Gamaniuk, CEO & Security Officer
oleksandr@instafill.ai · Instafill.ai

01

At a glance

The short answer to “is my data safe with you?”

US-stored

MICROSOFT AZURE,
TEXAS

AES-256

AT REST · TLS 1.2+ IN
TRANSIT

48 hours

BREACH NOTICE TO
YOU

Stored in the United States. Documents and form data are stored in Microsoft Azure's South Central US region in Texas.

Encrypted twice. HTTPS on every connection and AES-256 at rest. On top of that, your uploaded files and field values are encrypted with keys unique to your workspace, held in Azure Key Vault.

Never sold, shared or used to train AI. Your content is used only to fill your forms. That's in our contract with you and in our AI provider's business terms.

Two-factor sign-in you can require. Your organization can require 2FA for every user, and your team can sign in with Google or Microsoft accounts.

Independently tested. White-box penetration test by Iterasec (November 2025), with remediation re-testing in December.

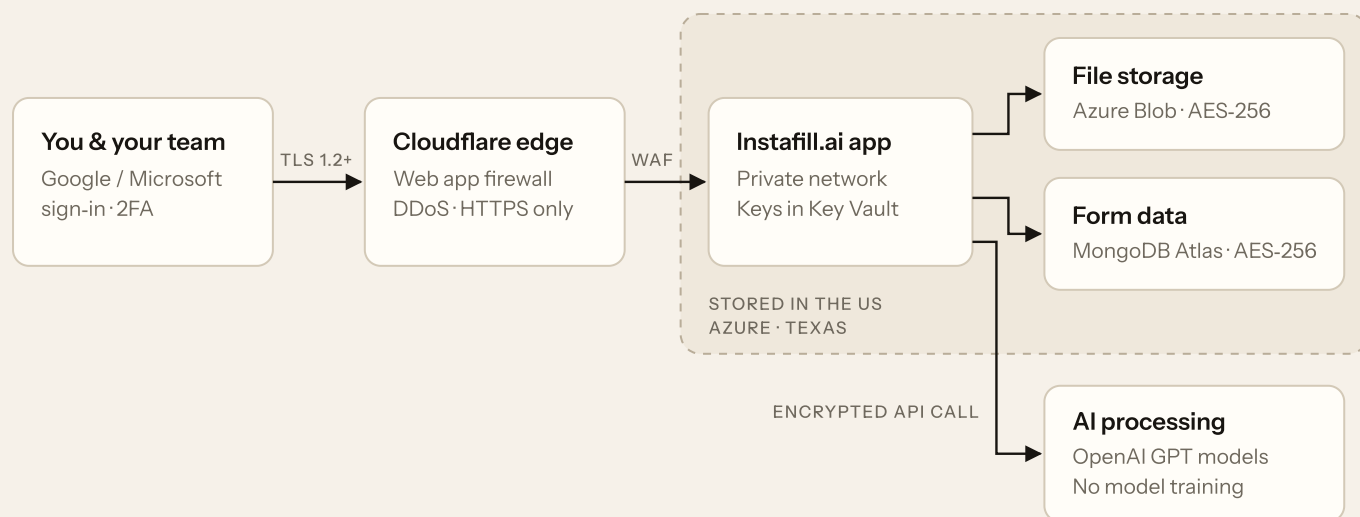
Committed in writing. A Data Processing Addendum covering our security measures, 48-hour breach notice, no AI training, and deletion when you leave.

02

Your data, end to end

What happens when you upload a form and the information that goes into it.

- 01 **You sign in and upload.** Sign in with Google, Microsoft, or email and password, with 2FA if your organization requires it. Upload a blank form (an application, an enrollment or credentialing form, a certificate) plus source data: an intake form, a prior application, a spreadsheet, or an export from the system you already use.
- 02 **It travels encrypted.** Traffic passes through Cloudflare's firewall and DDoS protection over HTTPS to our application in Microsoft Azure.
- 03 **It's stored encrypted, in the US.** Files go to Azure Blob Storage and field values to a MongoDB Atlas database in the same Azure region. Both are encrypted with your workspace's own keys.
- 04 **AI fills the form.** The form and the source data for that one fill go over an encrypted connection to OpenAI's API. They're processed to produce the fill and never used for training.
- 05 **You review and download.** Every value is editable before you download the completed PDF. Delete documents whenever you like, or have your workspace delete them automatically.



The shaded area is where your documents and form data are stored. AI requests leave it only as encrypted API calls, and nothing in them is used for training.

03

What we process

Only what you choose to upload, nothing more.

DATA	EXAMPLES	STORED IN
Forms & templates	Blank applications, enrollment and credentialing forms, certificates	Azure Blob Storage (US) · encrypted
Source data you attach	Intake forms, prior applications, system exports, spreadsheets	Azure Blob Storage (US) · encrypted
Filled values	Names, addresses, dates of birth, license and ID numbers, history entries	MongoDB Atlas (US) · encrypted
Account & activity	Your users' names, business emails, sign-in and activity logs	MongoDB Atlas (US) · application logs
Billing	Card details go straight to Stripe and never touch our servers	Stripe · PCI DSS Level 1

Data minimization tip: leave Social Security and bank account numbers out of source files unless a form asks for them.

04

Who else touches the data

A deliberately short list of providers, each independently audited and bound by data-protection terms.

PROVIDER	ROLE	ASSURANCE
Microsoft Azure US · South Central (Texas)	Hosting, file storage, networking, encryption keys	SOC 2 Type II, ISO 27001, HITRUST
MongoDB Atlas US · same Azure region	Database for form data, over a private endpoint	SOC 2 Type II, ISO 27001
OpenAI Processing only · no storage	AI models, via business API terms that prohibit training on your data; OpenAI Business Associate Addendum signed	SOC 2 Type II
Cloudflare Transit only	Firewall, DDoS protection, HTTPS, DNS	SOC 2 Type II, ISO 27001
Adobe · Google Word files only	Converting Word documents to or from PDF. If you work only in PDF, they're never involved	SOC 2 Type II, ISO 27001

Supporting services with limited account data only: Stripe (payments), Twilio (2FA text messages), SendGrid (account emails) and Amplitude (product-usage analytics). Files you choose to email to our team pass through Google Workspace, our email provider.

We give 30 days' notice before adding or replacing a provider that processes your data, and we remain responsible for each of them.

05

How it's protected

Layered controls across the application, the network, and our own team.

Encryption

TLS 1.2+ in transit. AES-256 at rest, plus a second layer with keys unique to your workspace, held in Azure Key Vault.

Workspace isolation

Every request to the application is checked against your workspace membership, and your data is encrypted under your workspace's own keys.

Sign-in security

Google or Microsoft sign-in, or email and password. Your organization can require two-factor codes for every user.

Network

All traffic passes Cloudflare's firewall. The app runs in a private Azure network, and the database is never exposed to the internet.

Monitoring & logging

Every request is logged with user, workspace and outcome, with automated alerts on anomalies and quarterly security-event reviews.

Secure development

Every change is code-reviewed and deployed through a controlled pipeline, with test and production kept separate.

06

AI and your data

The question we hear most.

Not used for training. Our Data Processing Addendum prohibits using your documents or data to train AI models. OpenAI's business terms for API customers also exclude API data from model training.

The agreement medical practices rely on. In September 2026 we signed OpenAI's Business Associate Addendum, the healthcare-grade agreement for protected health information.

One route, set for you. At onboarding we set your organization to process every fill through OpenAI's API, the service covered by our signed Business Associate Addendum.

Only what the task needs. For each fill, the model sees the form and the source files attached to that fill. It never sees your other documents or other customers' workspaces.

A person stays in control. The AI prepares a draft. You review and edit every value before download, and nothing is submitted to anyone on your behalf.

No decisions about people. The AI fills documents. It doesn't score, profile or make eligibility decisions about the people in your forms.

07

Independent testing & assurance

We don't ask you to take our word for it.

2 weeksWHITE-BOX TEST · NOV
2025**6 of 6**CRITICAL & HIGH
FIXED OR
DOWNGRADED**Annual**INDEPENDENT
TESTING

Penetration test by Iterasec. A two-week white-box test (November 17–28, 2025) of the production app and both APIs, with source-code access, against OWASP and CWE Top 25 standards. The December re-test confirmed the one Critical and four of five High findings fully fixed; the fifth High was reduced to Low. Report available under NDA.

Remediation deadlines. Our Penetration Testing Policy requires Critical and High findings to be fixed within 30 days.

SOC 2 Type II, in preparation. SOC 2-aligned controls have operated since October 2025, with dated evidence: access and security-event reviews, restore tests, and DR and incident-response exercises. Current audit reports for our infrastructure providers are on file.

08

If something goes wrong

Incident response, notice to you, and keeping the service running.

1 hourCRITICAL
RESPONSE**48 hours**NOTICE TO
YOU**4 hours**RECOVERY
TARGET**1 hour**MAX DATA
LOSS

A written incident response program. Identify, contain, eradicate, communicate, review: Critical incidents within 1 hour, High 4, Medium 24, Low 48. Tested every year; the October 2025 exercise contained a simulated compromise in 18 minutes.

You hear from us within 48 hours. If a breach affects your data, we tell you in writing within 48 hours of becoming aware of it: what happened, which data, roughly how many records, and what we're doing. That leaves room for your own reporting deadlines.

Built to recover. Daily database backups with point-in-time restore, geo-redundant file storage, and quarterly restore tests. Our October 2025 disaster-recovery test recovered from a simulated regional outage in 1 hour 25 minutes, inside the 4-hour target.

Status updates. If an outage lasts more than 4 hours, customers get updates at least every 8 hours until service is restored.

09

Retention, deletion & your control

Your data is yours, and it stays only as long as it's useful to you.

DATA

KEPT

THEN

Documents & form data

Until you delete them, or for the number of days you set

Securely deleted within 30 days of account closure

Account data

Subscription term + 90 days

Securely deleted

Backups

30-day rolling window

Expire automatically

Automatic deletion. Your workspace can delete uploaded sources and completed documents automatically after the number of days you choose.

Deletion on request. Ask us to delete everything at any time, or when you close your account, and we'll confirm in writing once it's done.

You own it. Everything you upload and everything the service generates belongs to you. We use it only to provide the service.

10

Our team & internal controls

Security is owned at the top and applies to everyone with access.

An accountable owner. Our CEO is the designated Security Officer. He approves our policies and reviews them at least once a year.

Staff access. Company Google Workspace accounts only, with MFA enforced. Access is least-privilege and approved by the owner, reviewed every quarter with signed acknowledgments, and revoked within 24 hours of offboarding.

Who can see your documents. Only team members who need to, for example an onboarding specialist building your templates at your request. They work under signed confidentiality agreements.

Devices. Full-disk encryption, automatic screen lock, antivirus and automatic updates on every work device, and no customer data on personal devices.

Training & conduct. A security awareness program and a written code of conduct for everyone, contractors included.

11

Mapped to a vendor security review

What compliance teams, IT departments and cyber carriers ask of a service provider, and where each item is answered.

REQUIREMENT	HOW INSTAFILL.AI MEETS IT	
Access controls & MFA Who can sign in, and how	MFA enforced for all our staff. Your organization can require two-factor sign-in for every user.	IN PLACE
Encryption In transit and at rest	TLS 1.2+ in transit; AES-256 at rest; workspace keys in Azure Key Vault.	IN PLACE
Use of your data Purpose limitation	Used only to provide the service. Never sold, shared for marketing, or used to train AI models.	IN DPA
Breach notification Notice to you	Written notice within 48 hours of becoming aware, leaving room for your own deadlines.	IN DPA
Representations & warranties Security in the contract	Our security measures and provider list are contract annexes you can rely on.	IN DPA
Location & subcontractors Where data lives, who touches it	US storage; providers disclosed, with 30 days' notice of changes.	IN DPA
Retention & deletion When you leave	Automatic deletion you control; everything deleted on request or at closure, confirmed in writing.	IN DPA
Due diligence & reassessment Evidence for your file	This blueprint, policies, pen-test results and a completed SIG Lite, refreshed every year on request.	AVAILABLE

This mapping supports your own vendor assessment. It isn't legal advice, and your industry, state or contracts may add requirements of their own. Send them over and we'll work through them with you.

12

Your side of the setup

Settings that complete your own security picture. We'll set them up with you.

- Require two-factor sign-in** for everyone in your organization.
- Invite only people who need access**, and remove leavers the same day.
- Leave out SSNs and bank numbers** unless a form requires them.
- Turn on automatic deletion** if you don't need forms stored with us.
- Report a suspected compromised login** to support@instafill.ai.

13

Quick answers

For a vendor or cyber-insurance questionnaire.

Is data stored outside the US?

No. Microsoft Azure, South Central US (Texas).

Encrypted in transit and at rest?

Yes: TLS 1.2+, AES-256, workspace keys.

Independent penetration test?

Yes, every year. Latest by Iterasec, Nov–Dec 2025.

Breach notification?

In writing, within 48 hours.

Is our data used to train AI?

No, and our contract prohibits it.

Multi-factor authentication?

Enforced for our staff; you can require it for your users.

SOC 2 report?

Type II in preparation; controls running since October 2025.

Can we delete our data?

Yes, any time, with optional automatic deletion.

14

For your file

Available on request. Most can be sent the same day.

DOCUMENT

Data Processing Addendum (DPA)

READY TO SIGN

Security policies & procedures

AVAILABLE

Penetration test report (Iterasec)

UNDER NDA

Completed SIG Lite questionnaire

AVAILABLE

Provider audit reports (Azure, MongoDB, Cloudflare)

AVAILABLE

Instafill.ai SOC 2 Type II report

IN PREPARATION

15

Next steps

A security-first path to your first filled form.

- 01 Review this blueprint and reply to confirm it meets your requirements.
- 02 We send your payment link together with our Data Processing Addendum for signature.
- 03 We set up your account with required 2FA, your AI route and automatic deletion, and build your templates using synthetic data.
- 04 You start filling real forms, with our onboarding team alongside you for the first weeks.

Have a security questionnaire of your own? Send it with your reply and we'll complete it.