Agreement Flow Privacy Policy

Last updated: October 1, 2026

Agreement Flow, based in Charlotte, North Carolina ("Agreement Flow", "we"), runs agreementflow.com, the Agreement Vault application at vault.agreementflow.com ("the Vault"), the Agreement Flow client portal at dashboard.agreementflow.com, and the email and support that go with them (together, the "Services"). This policy explains what personal information we collect through the Services, what we do with it, who we share it with, how long we keep it, and the choices you have.

The short version:

- We do not sell personal information, and we do not show advertising.
- We do not use your documents to train AI models, and neither does the AI provider we use to read them.
- Your documents are yours. You can export everything at any time, and when you leave we delete them on a schedule written into our Terms of Service.
- Every time someone views, downloads or shares a document in the Vault, it is recorded, and the organization that owns the document can see that record.

1. Two kinds of information, two roles

We handle personal information in two different roles, and it matters which one applies to you.

Information about you as our customer, user, guest, prospect or visitor. Your name, work email, how you use the Services, your billing details, your support requests. For this information we decide how it is used, and this policy is the full description.

Information inside a customer's Vault or Flow engagement. Franchise documents name people: franchisees, business owners, guarantors, signers, prospects who receive a Franchise Disclosure Document (FDD), outside counsel invited into a Room. The customer that uploaded the document, entered the record or sent the invitation decides why that information is held and for how long. We hold and process it on that customer's instructions, as its service provider, under our Terms of Service and the Data Processing Agreement at agreementflow.com/dpa, which is part of them.

If you are a franchisee, a prospect or anyone else whose information sits in a customer's Vault because of your relationship with that customer, your questions and requests about it go to that customer first. We will help the customer answer them, and section 10 explains how.

2. What we collect

Account information. When a customer creates an account for you, or you accept an invitation, we hold your name, email address, the organizations and brands you belong to, and your role in each.

Sign-in and security information. In the Vault, sign-in works through links we email to you. Administrators and staff also enroll an authenticator app; we store what is needed to verify your codes, plus recovery codes in a form that lets us check a code you enter but not display it again. The Flow client portal signs you in with a password, which we store only as a hash that lets us check a password you enter but not read it; you can change it in the portal. Once you sign in, a cookie keeps you signed in on that browser until you sign out or it expires.

Activity records. The Vault keeps an append-only record of actions taken in it: sign-ins, document views, downloads, shares, uploads, exports, changes to records, Room activity, and every access by our own staff. Each record says who acted (a user, a guest, our staff, or an automated system), what they did, and when. Our hosting provider also keeps short-lived technical logs of each request, including IP address and browser type, which we use for security and troubleshooting.

Documents and the information read from them. Files uploaded to the Vault, the text and values the Vault reads from them, the values you confirm or correct, previews rendered from them, and the records (units, deals, entities, dates) built on them.

Billing information. Payments are handled by Stripe. We receive and keep your billing contact, billing address, invoice history, and the last four digits and expiry of a card on file. Full card and bank account numbers are entered on Stripe's forms and never reach our servers.

Communications. Emails you send to support@agreementflow.com, messages sent through our contact form, and records of calls or demos you book with us.

Sandbox usage. If you create a sandbox, we record how you use it: pages visited, which guided-tour steps you completed, and whether you uploaded a document. These are the same activity records as above, and we use them to see where prospects get stuck and to follow up with you.

Email delivery events. Our email provider tells us whether each email we send was delivered, bounced or marked as spam, and we record that.

Error reports. When something goes wrong in the Services, an error report goes to our monitoring provider. Error reports contain technical details about what went wrong. They do not include document content, and we strip email addresses from error messages that could carry them.

Website visits. agreementflow.com may use a web analytics tool to count visits and see which pages are read. It also keeps standard server logs.

We do not collect precise location data, and we do not read your email beyond what you send us.

3. How we use it

We use personal information to:

- run the Services: sign you in, keep accounts secure, show each person the documents and brands they are entitled to, and record activity so customers have an audit trail;
- send the emails the Services exist to send: sign-in links, deadline reminders chosen by the customer, Room invitations and notices, FDD delivery through DocuSign, billing notices, and replies to your support requests;
- read uploaded documents with automated tools so we can propose how to file them (section 4);
- keep backups and check that stored files have not been altered;
- bill customers and keep the records tax and accounting law require;
- support you, and follow up with sandbox users about buying the Vault;
- improve the Services, including using the corrections and confirmations customers make to improve how the Vault reads documents, and using sandbox and usage records to see what works;

- protect the Services, our customers and the public: detect abuse, investigate security incidents, enforce our Terms, and meet legal obligations.

We do not use personal information for advertising, and we do not make automated decisions about individuals that have legal or similarly significant effects.

4. Automated reading of documents, including AI

When a document is uploaded to the Vault, software reads it to propose its type, the parties, the dates it sets and certain terms (for example, the length of a franchise term or a territory description). Scanned pages may first be converted to text. Part of this reading is done by sending the document's text to Anthropic's API, a large-language-model service that we use under Anthropic's commercial terms (anthropic.com/legal/commercial-terms), not through any consumer product. Under those terms, content sent to the API is never used to train Anthropic's models, and Anthropic keeps it only briefly, for abuse monitoring, before deleting it.

Everything the software proposes is shown to the customer as a proposal. A person confirms or corrects it before it becomes a record. Nothing is decided about any individual automatically.

Agreement Flow's document preparation service (Flow services) also uses automated tools, including Anthropic's API, to read intake information and prepare documents for signature, under the same provider terms.

5. Who we share information with

We share personal information only in the ways listed here.

The customer that invited you. If you are a user or guest of a customer, that customer's administrators can see your name, email, role, and your activity in their Vault, including what you viewed and downloaded. Guests do not see other people's activity.

People the customer chooses to share with. When a customer invites a guest into a Room, shares a link, or sends an FDD, the recipient receives what the customer chose to send.

Service providers. Companies that process information on our behalf, bound by contracts that limit what they may do with it:

Provider	What it does for us
Supabase	Hosts our database and handles sign-in
Vercel	Hosts the application and the website
Google Cloud	Stores uploaded files and runs scheduled jobs (backups, integrity checks, document previews)
Backblaze	Holds a second, encrypted copy of stored files for disaster recovery
Postmark	Delivers the email we send (sign-in links, reminders, notices, invitations)
Stripe	Processes payments and holds card and bank details
DocuSign	Delivers FDDs and other documents for signature, and returns completed documents and signing records

Provider	What it does for us
Anthropic	Reads documents to propose filing information (section 4)
Sentry	Receives error reports from the Services
ClickUp	Receives messages sent through our contact form, where we track support requests
Google Workspace	Runs our company email, and Google Drive stores working files for Flow services

Legal requirements. We disclose information when the law requires it, such as in response to a subpoena or court order. For a demand aimed at a customer's content, we tell the customer first unless we are legally prohibited, as our Terms describe.

Business transfers. If Agreement Flow or the Vault business is sold or merged, personal information may transfer to the successor, which must honor this policy. Customers' export and deletion rights survive any such transfer.

With your consent, or at your direction.

We never sell personal information, never share it with data brokers, and never share it for advertising.

6. Email we send

All email from the Services is sent from the notify.agreementflow.com domain or from an @agreementflow.com address. Most of it is transactional: it exists because of something you or your organization did or set up. Deadline reminders go to the people a customer's administrators chose, on the schedule they chose, and can be changed in the customer's settings.

If you create a sandbox, we may email you about your sandbox and about buying the Vault. Every such email has an unsubscribe link, or you can reply and ask us to stop.

We do not send newsletters or marketing email to customers or guests without asking first.

7. Cookies

The Vault and the client portal use only the cookies needed to keep you signed in and to protect against forged requests. There are no advertising or third-party tracking cookies in the applications.

agreementflow.com may use an analytics tool that sets cookies to count visits. It uses no advertising cookies.

Because we do not track people across other websites, we do not respond to "Do Not Track" browser signals; there is nothing for them to turn off.

8. How long we keep information

Information	Kept for
Customer documents and records	While the subscription is active, then deleted on the schedule in our Terms: at the later of the end of the access window or 14 days after the first completed full export, removed from live systems within 14 days (records first, then stored files immediately after) and from backups within 30 days
Sandbox data	30 days from creation, then deleted with no copy kept
Account information	While the account exists, then deleted with the customer's data or on request
Activity and audit records	Part of the customer's audit trail while the subscription lasts. When the customer's data is deleted, a sealed copy of the brand's log, referring to deleted documents by identifier only, is kept for three years from the deletion date, then deleted
Billing records	As long as tax and accounting law requires
Sign-in links	One hour, and used once
Shared links	The period the customer chose when creating the link, or until turned off
Download links generated when viewing or downloading a document	One minute
Support correspondence and contact form messages	Three years after the request is closed
Email delivery events	One year
Error reports	90 days
Hosting provider request logs	A short period set by the provider, measured in days

Backups are kept with a second provider and are purged on the same schedule as the live data they copy.

9. How we protect information

- All connections to the Services use TLS encryption, and our providers encrypt stored data at rest.
- In the Vault, sign-in is by one-time emailed link, and administrators and staff must also use an authenticator app. The Flow client portal uses a password, stored only as a hash.
- Access to data is enforced in the database itself, per brand, so a user can only read the brands they belong to.
- Every document view, download and share passes through one audited path; there is no unaudited way to reach a stored file.
- Our staff have no standing access to customer documents. Access is granted for a limited time (at most 90 days per grant), recorded, and visible to the customer's administrators.
- Every Room and shared link requires the invited person to sign in. There is no anonymous access to any document.
- Uploaded files are write-once. Stored files are periodically re-checked against the checksum recorded when they were uploaded, so a changed or missing file is noticed.
- Stored files are backed up nightly to a second provider, in encrypted form.

- Email addresses are removed from error reports before they leave our systems.

No system is perfectly secure. If we learn of a security incident that affects your personal information or a customer's content, we will notify the affected customer's administrators, and anyone else the law requires, without unreasonable delay, and we will say what happened, what information was involved and what we are doing about it.

10. Your choices and rights

See and update your information. Account details can be updated in the application. Customers can export their complete Vault at any time.

Delete. A customer's administrators can delete documents, remove users and guests, cancel the subscription, or ask us to delete the brand's documents and account data sooner than the schedule in our Terms. Guests can ask us to delete their guest account by emailing support@agreementflow.com; the customer's record of past access stays with the customer's records and follows the retention in section 8. Billing records are kept as described in section 8.

Information in a customer's Vault. If you are a franchisee, prospect, signer or other person whose information is in a customer's Vault, contact that customer. If you contact us instead, we will tell you which customer holds your information where we can, pass your request to them, and act on their instructions.

Email. Unsubscribe from sandbox follow-up email using the link in any such email. Transactional email, such as sign-in links, cannot be turned off while you have an account, because the Services do not work without it.

U.S. state privacy laws. The Services are offered to businesses in the United States. We do not sell or share personal information for advertising, and we do not use it for profiling with legal or similarly significant effects. If you are a resident of California or another state with a consumer privacy law and want to know what personal information we hold about you as our customer, user, guest or prospect, correct it, or delete it, email support@agreementflow.com and we will respond as that law requires. We will not treat you differently for making a request. For information in a customer's Vault, we are the customer's service provider, and we will forward your request to the customer.

Outside the United States. The Services are designed for United States franchisors and are hosted in the United States. If you use them from elsewhere, your information is transferred to and processed in the United States.

11. People under 18

The Services are for businesses and the professionals who work with them. They are not directed at people under 18, and we do not knowingly collect information from them.

12. A note for guests

If a customer invited you into a Room or sent you a shared link, here is what that means for your information:

- We hold your name and email because the customer gave them to us to create your access.
- Your sign-ins, views and downloads are recorded and visible to the customer that invited you. They are part of that customer's records and stay with them after your access ends. When the customer's data is deleted, a sealed copy of that log is kept for three years and then deleted.

- A shared link works only for you, after you sign in. Forwarding it gives no one else access.
- Your access ends when the customer removes you, closes the Room, the link expires, or the customer's subscription ends.
- You can ask us to delete your guest account at any time.

13. A note for prospects who receive an FDD

If a franchisor uses the Vault to send you a Franchise Disclosure Document, the franchisor entered your name, email address and state of residence, and the document is delivered to you through DocuSign. We record when the envelope was sent and when the receipt was signed, because the franchisor needs that record. DocuSign's own privacy policy covers the signing experience. Questions about why you were sent the document, or about the information the franchisor holds on you, go to the franchisor.

14. Changes to this policy

When we change this policy we will post the new version at agreementflow.com/privacy with its date. If a change materially reduces your rights or changes how we use information we already hold, we will email customer administrators at least 30 days before it takes effect.

15. Contact

Agreement Flow

Charlotte, North Carolina

support@agreementflow.com