

Privacy Notice

Last updated: 9 September 2026

Who we are

Compliance MVP LLC (“we”, “us”) operates the website at www.compliancemvp.com and the Compliance MVP application at app.compliancemvp.com, and is responsible for the personal information described in this notice.

This is one notice for both. Most of it applies to everyone. Where the website and the application differ, the section says so.

Compliance MVP LLC
65 Wayside Ln
Redding, CT 06896
support@compliancemvp.com

What we collect, and when

We only collect information you or your firm type in, plus the ordinary technical records any website or application keeps.

On the website

If you join our mailing lists, we collect your name, email address, company name, and anything you tell us about the functionality you are interested in.

If you send us a message through the contact form, we collect your name, email address, the message you write, and — if you choose to give them — your company name and a phone number. The phone number is optional and we only use it if you have asked us to call you back.

Whenever anyone visits the site, our hosting provider records standard technical information, including the IP address your connection comes from, the pages requested, and the date and time. We use this to keep the site running and secure. We do not use advertising trackers, we do not build profiles of visitors, and we do not use cookies to follow you to other websites.

In the application

Your account. Your firm's administrator sets up your account with your name, email address, firm and role. You do not sign yourself up; you are invited.

Signing in. Your password is held by our sign-in service and we never see it. Every sign-in requires a second step — a code emailed to you, or a code from an authenticator app if you have set one up. If you set up an authenticator app, we hold the key that makes its codes work.

What you do in the application. When you create, change, approve or sign something, the application records who did it, when, and the IP address it was done from. That record is the Activity Log, and it exists so your firm can show a regulator who did what. An attestation you sign records the same details as evidence of your signature.

Files you upload are stored with the record they belong to.

Technical records of your visits — IP address, browser, pages requested, date and time — are kept to run the application and keep it secure. If something goes wrong, an error report is sent to our error-monitoring provider. Personal details — email addresses, passwords, session tokens, and anything that looks like an account or identification number — are removed from the report before it leaves the application.

Records about other people. Your firm uses the application to keep its own compliance records, and some of those are about people: staff, clients, vendors, the subjects of an issue. Those records belong to your firm. We hold them on your firm's instructions and do not use them for anything else. If you have a question about a record your firm keeps about you, your firm is the right place to ask, and we will help it answer.

We do not knowingly collect information from anyone under 18. This is a business product and it is not directed at children.

Why we use it

- **To tell you when Compliance MVP launches**, if you asked us to, and to invite you to a demonstration.
- **To send you ongoing product updates and news**, if you asked us to. These are two separate choices and you can make either one, both, or neither.
- **To reply to you** if you send us a message. Sending us a message does not sign you up for anything — if you want our emails as well, there are boxes on the form to say so, and they are never ticked for you.
- **To understand which parts of the product people ask about**, so we build the right things.
- **To run the application for your firm**: to sign you in, show you the records your role allows, and keep the Activity Log your firm relies on.
- **To keep the application secure**: to spot sign-ins that look wrong, investigate incidents, and find and fix faults.
- **To send you messages about your firm's subscription** — scheduled maintenance, incidents, billing, and support — and messages your firm has told the application to send, such as reminders, attestation requests and assigned work. See *Email from the application* below.

We do not use your information to make any automated decision about you.

Who else sees it

We do not sell, rent, or trade your personal information, and we do not share it for anyone else's marketing.

Your firm. If you hold a login, your firm’s administrators can see your account details, the records your work touches, and the Activity Log. That is how the product is meant to work: the firm is answerable for its compliance records, and you are acting for it.

Our service providers. We use outside companies to host the website and the application, store data, send email, and watch for faults. They receive only what they need to do that job, they act on our instructions, and — with the one exception noted for Stripe below — they are not permitted to use your information for their own purposes:

Provider	What they receive	What they do
Amazon Web Services	Everything held in the application: accounts, records, uploaded files, the Activity Log, and the email the application sends	Hosts the application, its database, its file storage and its sign-in service, and delivers its email. Data is held in the United States
Cloudflare	Your IP address and page requests, on the website and the application	Serves the website, and stands in front of the application to block attacks
Brevo	Name, email, company, interests, your message, and which emails you agreed to receive	Stores our contact records and sends our marketing and contact-form email
Sentry	Error reports from the application, with personal details removed first	Tells us when the application has a fault so we can fix it
Google	Your IP address	Supplies the typefaces the website displays
Stripe	When we begin charging for the application: the name, card details and billing address of the person paying, and the payment history	Takes payment. Card details go directly to Stripe and we never see the full card number

About Stripe. We do not take payments today. When we do, they will go through Stripe, and the person paying will enter their card into Stripe's own form. Stripe collects those details directly, uses them to screen for fraud and to meet its own legal obligations, and handles them under its own privacy policy, which will be linked from the payment page. We will update this notice, and say so clearly, before the first payment is taken.

We will also disclose information if the law requires it — a subpoena, a court order, or a lawful request from a government authority — or where we need to in order to protect our rights or someone's safety. If our business is ever sold or merged, the information in this notice may transfer with it; if that happens we will say so on this page before it takes effect.

Email from the application

If you hold a login, the application sends you three kinds of email:

- **Sign-in email:** your invitation, and the security code each time you sign in by email. These cannot be switched off; without them you cannot get in.
- **Service messages about your firm's subscription:** scheduled maintenance, incidents, billing, and support. These are sent while your firm holds a subscription and cannot be unsubscribed from, because they are the information a customer needs to have.
- **Messages your firm directs:** reminders, attestation requests, assigned work, and anything else your firm configures the application to send. These are sent on your firm's behalf, and your firm decides what is sent and to whom.

None of these is marketing. We only send marketing email to people who asked for it on the website, and the next section is about that.

An email from the application never carries a file. It carries a link, and the link requires you to sign in before the file is shown. That keeps your firm's documents inside the application, where access can be withdrawn.

Marketing email, and how to stop it

Every marketing email we send carries an unsubscribe link at the bottom. One click stops it. You do not have to give a reason and we will not ask for one.

We use confirmed opt-in: when you ask for our emails, we send you one message asking you to click a link to confirm. If you do not click it, we do not add you. This protects you from being signed up by someone else using your address.

Unsubscribing stops the marketing. If you have asked us to contact you about something specific, we will still reply to that. It does not stop the sign-in and service email described above, which are not marketing.

How long we keep it

We do not hold information longer than we need it — for the business support we provide to our customers, or for as long as a law or regulation requires us to keep it.

On the website

- **If you are on one of our mailing lists**, we keep your details until you unsubscribe or ask us to delete them, whichever comes first.
- **If you sent us a message**, we keep it for as long as we may reasonably need it to deal with what you raised.
- **Website technical logs** are kept for the period our hosting provider retains them, which is short and measured in weeks.

In the application

- **Your account** is kept for as long as your firm keeps it. When your firm closes it, your name stays on the records and Activity Log entries you were part of, because a compliance record with the names removed is no longer a record.
- **Your firm's records**, including the Activity Log and the evidence of attestations, are kept for as long as your firm decides. Firms are regulated and have their own record-keeping

obligations, so the firm controls the retention period. A firm may also choose to keep its records in a tamper-proof form (sometimes called WORM, “write once, read many”) that cannot be altered or deleted by anyone, including us, until its retention period ends.

- **Application technical logs and error reports** are kept for a limited period and then discarded. They are not part of your firm’s records.

If you ask us to delete your information, we will keep only the minimum needed to remember that you asked not to be contacted — otherwise we would have no way to honour it — and, if you held a login, whatever your firm’s record-keeping obligations require it to keep. We will tell you which is which.

Your choices

Whatever state you live in, you can ask us to:

- **tell you** what information we hold about you;
- **correct** anything that is wrong;
- **delete** it; or
- **stop** sending you marketing.

Email support@compliancemvp.com and we will respond within 30 days. We will not charge you, and we will not treat you differently for asking.

If you hold a login, your firm’s administrator can correct your account details directly, and is the first place to ask about records your firm keeps about you. Where a record has to be kept under your firm’s record-keeping obligations, or is held in tamper-proof form, we cannot delete it until that period ends, and we will say so rather than leave you guessing.

Residents of California, Colorado, Connecticut, Virginia and other states with privacy laws have these rights by statute. We extend them to everyone rather than asking where you live.

We do not sell personal information and we do not share it for cross-context behavioural advertising, as those terms are defined under California law.

How we protect it

The website and the application are served over an encrypted connection. Every sign-in to the application requires a second step beyond the password. Information you submit is held by the providers named above in their own secured systems, in the United States, and access on our side is limited to those who need it. Each firm's records are kept separate from every other firm's. No system is perfectly secure and we will not claim otherwise.

We do not hold payment details or financial information, and we do not ask for them. When we begin charging for the application, card details will go directly to Stripe and we will never see the full card number.

Changes to this notice

If we change this notice we will update the date at the top. If the change is significant — a new provider receiving your data, or a new use of it — we will say so clearly rather than quietly amending the page.

Contact

Questions, or any of the requests above:

support@compliancemvp.com

Compliance MVP LLC

65 Wayside Ln

Redding, CT 06896