

Privacy Policy

How Fractional Coordinator collects, uses, retains, and discloses personal information, and the rights you have over your own data. Written in plain language, designed to be read by the people whose data we handle, not just by lawyers.

Effective May 20, 2026 · Next scheduled review November 20, 2026

Fractional Coordinator is a civil rights compliance firm. We collect personal information from three groups: (1) institutional clients who engage us for investigations, fractional leadership, audits, and OCR matters; (2) individual practitioners who register for certifications, bootcamps, and workshops; and (3) visitors to this website. The information we hold, particularly investigation files and case records, is sensitive by nature, and we treat it accordingly.

What we collect, and why

From institutional clients. Names and contact information for engagement leads, scope and matter information necessary to perform the work, documents and data produced during investigations or audits, and billing information. We collect this because we need it to do the work you have engaged us to do.

From training registrants. Name, employer, role, email, phone, billing information, dietary or accessibility needs voluntarily provided for in-person events, and post-program feedback. We collect this to register you, deliver the program, issue your certificate of completion, and improve future cohorts.

From website visitors. Standard server logs (IP address, user agent, pages visited, timestamps) and any information voluntarily submitted through forms (newsletter signups, contact requests, demo requests). We collect this to operate and improve the site, respond to inquiries, and protect against abuse.

Sensitive categories handled in investigation work

Investigation engagements routinely involve information that is sensitive even by privacy-policy standards: allegations of sexual misconduct, race or national-origin-based discrimination, disability status, mental health information, medical records relevant to ADA matters, and the identities of witnesses and complainants who have requested confidentiality. We treat investigation files as legally privileged work product wherever the engagement letter establishes that privilege, and as confidential institutional records in all cases.

Investigation files are not used for any purpose other than the engagement. They are not used to train AI models, not anonymized and republished as case studies without the institution's written consent, and not retained beyond the windows specified below.

How we use the information

- **To perform the work.** Conduct investigations, deliver fractional services, run training programs, manage OCR engagements, and fulfill contract obligations.
- **To communicate with you.** Respond to inquiries, send program logistics, send your certificate, and send the quarterly regulatory digest if you have opted in.
- **To bill you.** Process payment for engagements and program registrations through Stripe, our payment processor; we do not store full credit card numbers.
- **To operate and improve our practice.** Internal training, quality review, and anonymous, aggregated analysis of which programs and services are working.
- **To meet legal obligations.** Respond to subpoenas, regulatory inquiries, and other legal process; comply with tax and recordkeeping requirements.

We do not sell personal information. We do not share personal information with third parties for their own marketing. We do not use personal information from investigation files to train artificial intelligence systems.

Subprocessors and service providers

We use a small number of vendors to operate our practice. Each one is bound by a written data processing agreement that requires them to handle our data only as we direct.

- **Cloud hosting (data and backend), Supabase (United States region).** Hosts the OnePointe application database, authentication services, and FC practice-management infrastructure. SOC 2 Type II compliant.
- **Web hosting and content delivery, Vercel, Inc. (USA).** Hosts and delivers the public marketing experience for fractionalcoordinator.com and the OnePointe site at onepointe.ai, plus supporting serverless functions. Data: HTTP request metadata, deployment logs, edge-cache content. SOC 2 Type II audited; GDPR and CCPA compliant.
- **Payment processing, Stripe.** Processes registration fees and engagement billing. We do not see or store full card numbers.
- **Email delivery, Mailchimp (Intuit Mailchimp; Atlanta, GA, USA).** Sends program logistics, certificates, and digest emails to opted-in subscribers. SOC 2 Type II, GDPR, and CCPA compliant.
- **Document storage and collaboration, Google Workspace (Google LLC; USA).** Used for shared drives, collaborative documents, and internal file management. SOC 2 Type II audited; HIPAA-eligible under a separate Business Associate Agreement when an engagement requires it; GDPR and CCPA compliant.
- **Electronic signature, DocuSign, Inc. (USA).** Used for engagement-letter execution, NDAs, and similar records requiring a verifiable electronic signature. SOC 2 Type II audited; ESIGN Act and UETA compliant.

- **FC private infrastructure.** Active investigation files, work product subject to attorney-client privilege, and sensitive case records are held privately on FC-managed servers in U.S. data centers. The sensitivity of this material requires storage on infrastructure we control directly, rather than on any third-party platform. Access is restricted to authorized FC personnel and audited.
- **Video conferencing, Zoom Video Communications, Inc. (USA).** Used for virtual program delivery and client meetings. SOC 2 Type II audited; HIPAA-eligible under a separate Business Associate Agreement when required. Recordings are not retained beyond the window below unless required by the engagement.
- **Event registration and ticketing, Luma (Luma Team, Inc.; USA).** Processes registrant name, email, and event details when you sign up for a training session or workshop through a Luma registration link. Used to admit you to the session and to send session logistics.
- **Video meetings, Google Meet (Google LLC; USA).** Used for some virtual meetings and sessions under our Google Workspace agreement. May process participant audio, video, and recordings, which are not retained beyond the window below unless required by the engagement.
- **Form delivery, FormSubmit (formsubmit.co; USA).** Relays website form submissions, contact requests, applications, and newsletter signups to our inbox at hello@fractionalcoordinator.com. Processes the fields you submit and any attachments; submissions are delivered by email and are not used by the vendor for other purposes.

Retention

Investigation files are retained for the period specified in the engagement letter, typically seven years from the close of the matter unless the institution requests earlier return or destruction. After the retention window, files are securely destroyed and a destruction certificate is issued.

Training records (registration, attendance, certificate of completion, exam results) are retained for ten years to support credential-verification requests from former attendees. Marketing-list subscriptions are retained until you unsubscribe.

Website logs are retained for 90 days for security and abuse-prevention purposes, then deleted or aggregated.

Billing records are retained for seven years for tax and accounting purposes.

Your rights

Depending on where you live, you have rights over the personal information we hold about you. We extend these rights to all individuals regardless of jurisdiction, because we think they are the right defaults.

- **Right to access.** Request a copy of the personal information we hold about you.
- **Right to correction.** Ask us to correct information that is inaccurate or incomplete.

- **Right to deletion.** Ask us to delete personal information we hold about you, subject to the retention obligations above and the limitation that we cannot unilaterally delete records contained in active engagement files without the engaging institution's consent.
- **Right to portability.** Receive a copy of the information you have provided to us in a structured, commonly used, machine-readable format.
- **Right to opt out** of marketing communications and the quarterly digest at any time. Use the unsubscribe link in any email.
- **Right to know** what personal information we have collected about you and how we have used it.

To exercise any of these rights, write to us at privacy@fractionalcoordinator.com with enough information for us to identify you and verify the request. We respond within 30 days. If your request is unusually complex, we may extend the response window by another 30 days and tell you why.

Children's privacy

Fractional Coordinator does not direct services to children under 13 and does not knowingly collect personal information from anyone under 13. PK-12 engagements are conducted with the institution as the data controller; FC processes student information only on the institution's behalf and only as necessary to perform the engagement. If you believe a child under 13 has provided personal information directly to FC, contact us at privacy@fractionalcoordinator.com and we will delete it.

State-specific disclosures

California residents have additional rights under the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), including the right to know what categories of personal information have been collected, the right to delete, the right to correct, the right to opt out of sale or sharing of personal information (we do not sell or share for cross-context behavioral advertising), and the right to limit use of sensitive personal information. We do not discriminate against California residents who exercise these rights.

Virginia, Colorado, Connecticut, and Utah residents have analogous rights under those states' privacy laws. The substance of those rights is reflected in the Your rights section above; the procedural details follow each state's framework.

EU and UK residents dealing with FC do so as a non-EU controller. To the extent we are subject to GDPR or UK GDPR, the lawful basis for processing personal information is generally legitimate interest (operating our practice, communicating with clients), contract (delivering services you have engaged us for), or consent (marketing communications, the quarterly digest). EU and UK residents have rights to access, rectification, erasure, restriction, portability, and objection. Fractional Coordinator does not currently process personal information of EU or UK residents in the regular course of business and has not designated an Article 27 GDPR representative. If the firm engages clients with substantial EU data-processing requirements, an EU representative will be designated and disclosed in this notice.

Security

We maintain administrative, technical, and physical safeguards designed to protect personal information from unauthorized access, alteration, disclosure, or destruction. Specifics are described in our Security Notice. No system is perfectly secure; if we become aware of a breach affecting personal information, we will notify affected individuals and applicable regulators in accordance with applicable law.

Changes to this policy

We update this policy when our practices change or when applicable law requires it. Material changes will be flagged on this page and, where practicable, communicated to affected individuals by email. The Effective date at the top of this policy reflects the most recent change.

Effective: May 20, 2026. Next scheduled review: November 20, 2026. Prior versions are available on request from privacy@fractionalcoordinator.com.

How to reach us

For questions about this policy, written notices, or formal correspondence, use the channels below or write to us at our mailing address.

Fractional Coordinator, Inc.

830 NE Holladay St., Portland, OR 97232, United States

Phone: (503) 395-0687

Privacy questions: privacy@fractionalcoordinator.com