ExhibitHub

Privacy Policy

Effective date: October 19, 2026 · Last updated: October 19, 2026

Exhibit Hub Inc. ("ExhibitHub," "we," "us") provides a platform that helps marketing teams plan, execute, and measure trade show and conference participation. This policy explains what personal information we collect, how we use it, who we share it with, and the choices available to you.

This policy covers our website, our platform, and our sales and marketing activities.

1. Two roles, two sets of rules

How we handle personal information depends on why we hold it. We act in two distinct capacities, and the difference matters for your rights.

As a service provider (processor). When our customers use the platform, they upload and generate information about their own employees, contractors, vendors, and contacts. We process that information on their instructions, under our agreement with them, in order to provide the service. Customers retain their rights in the information they upload.

Two limited exceptions to that rule are disclosed in this policy and authorized under our customer agreement: we use information about how the platform is used to operate, secure, and improve it, as described in Section 3; and we derive aggregated, de-identified datasets as described in Section 5. Neither exception permits us to use customer content for advertising, to disclose it to other customers in identifiable form, or to train general-purpose AI models for the benefit of others. Where our agreement with a customer sets different terms, that agreement controls.

If you are an individual whose information appears in a customer's ExhibitHub workspace — for example a colleague assigned to staff a booth — the customer is responsible for that information, and requests about it should be directed to them. We will refer you to the relevant customer, or assist them in responding.

As a business (controller). We decide the purposes for information we collect in our own right: account registration data, billing details, support conversations, website visitors, and business contacts we identify for sales outreach. Sections 8 and 9 describe your rights over this information.

2. Information we collect

Account and user information. Name, business email address, job title, organization, and workspace role. We use passwordless authentication, so we do not store account passwords.

Customer content. Information our customers upload to or create in the platform: event records, budgets and expense records, receipts and invoices, uploaded documents, staffing assignments, travel details, schedules, tasks and project management details, and asset and shipment records. This may include personal information about the customer's own personnel and contacts.

Billing information. Billing contact details and subscription records. Payment card details are collected and processed directly by our payment processor and never pass through or reside on ExhibitHub systems.

Usage and technical information. Log data generated when the platform is used, including IP address, browser and device type, pages and features accessed, and timestamps. When you visit our websites, we and our analytics and advertising providers also collect device, browser, and browsing activity information through cookies and similar technologies, as described in Sections 6 and 10.

Communications. Messages you send us by email, support conversations, and — where you are notified in advance and agree — recordings, transcripts, and notes of video calls.

Organization and service provider information. Information about your organization and the service providers it works with, including the exhibit house that supports your exhibit program, collected during onboarding and in your workspace settings. Where you give us a named contact at a service provider, that person's business contact details are handled in the same way as other business contact information described in this policy.

Global event database information. We maintain a global database of trade show and conference information — events, venues, organizers, general contractors, deadlines, schedules, shipping instructions, and related details — that we make available inside the platform. We compile it from two categories of source: publicly available materials, including event and organizer websites, published exhibitor prospectuses and service kits, and materials located at URLs our customers direct us to; and information provided to us by our partners and licensors. This database includes business contact information for individuals in professional roles at event organizers, venues, and general contractors — for example a name, job title, business email address, and business telephone number published in an exhibitor service kit. **We do not use documents uploaded by our customers to build this database.** Section 8 explains how to ask us to correct or remove your information from it.

Business contact information. For sales and marketing, we obtain business contact details about individuals at companies that may benefit from the platform, from third-party business data providers and public sources. Section 9 explains this in detail.

Sensitive information. The platform is not designed to hold sensitive categories of personal information — government identifiers such as passport, Social Security, or driver's license numbers, health or medical information, financial account or full payment card numbers, biometric data, or precise geolocation — and customers must not upload them, including within documents such as receipts, invoices, and travel confirmations. Customers are responsible for removing or redacting such details before submitting a document. We do not seek out this information, and where we become aware that it has been submitted we may delete it or ask the customer to do so.

3. How we use information

We use personal information to:

- provide, operate, secure, and support the platform;
- authenticate users and protect accounts;
- process subscriptions and billing;
- respond to support requests and communicate about the service, including service and security notices;
- monitor performance, diagnose problems, and improve reliability;
- develop and improve product features;

- market and sell the platform to businesses;
- comply with legal obligations and enforce our agreements.

Where we rely on legal bases under European or UK law, those are performance of a contract, our legitimate interests in operating and improving a business service, compliance with legal obligations, and consent where required.

4. Artificial intelligence features

The platform uses AI to reduce manual data entry — extracting event details from documents and websites, parsing forwarded confirmations and invoices into structured records, and other event planning efficiencies. To do this, customer content is sent to AI model providers acting as our service providers.

Three commitments govern this:

- **Customer content is not used to train AI models.** We do not use customer content to train or fine-tune a general-purpose AI model for use by other customers. We do process customer content to provide, secure, support, troubleshoot, and evaluate these features for the customer whose content it is. Our arrangements with third-party AI providers, as we have configured them, prohibit those providers from using customer content to train their models; providers may retain content briefly for abuse monitoring and service delivery.
- **AI output is presented for human review** rather than silently altering customer records.
- **AI providers appear on our subprocessor list** alongside our other service providers.

Operating these features produces diagnostic records ("traces") that may contain customer content, including email addresses. These are retained for a short period for troubleshooting and are described in Section 7.

5. Aggregated and de-identified information

We derive aggregated, de-identified datasets from customer content in order to build benchmarking and cost-projection features, and to publish aggregate market materials such as industry benchmark and cost reports — for example typical accommodation rates in a market, or typical utility costs at a particular venue. Complete data across many customers is what makes these projections useful.

We apply the following safeguards:

- **De-identification.** Derived records contain no customer identity, no individual transaction records, and no field permitting attribution to a specific organization. We de-identify to a standard where the resulting data cannot reasonably be linked back to a customer or an individual. We do not attempt to re-identify it, and we contractually prohibit recipients from doing so.
- **Minimum-cohort suppression.** No derived figure is surfaced unless it is computed from at least five distinct customer organizations, with no single organization contributing more than 30% of the underlying values. Figures failing either threshold are suppressed rather than published with a caveat.
- **Documented method.** Derivation methods, suppression thresholds, and field-level scope are documented and reviewed annually, including a reassessment of whether the thresholds remain appropriate.

We maintain this information in de-identified form and do not attempt to reverse it. The safeguards above apply to every use of these datasets, including anything we publish externally.

6. How we share information

Service providers (subprocessors). We use third-party providers to host, operate, and support the platform. They may process personal information only to provide services to us, under written terms requiring confidentiality and appropriate security. Our current list of subprocessors is available at https://exhibithub.com/legal/subprocessors, where customers may also subscribe to notifications of changes.

Within a customer's workspace. Information in a customer workspace is visible to that customer's authorized users according to the permissions the customer configures.

At a customer's direction. Where a customer connects the platform to another system or forwards information to it, we transmit and receive information as that customer directs.

Legal and safety. We may disclose information where required by law, valid legal process, or governmental request, or where reasonably necessary to investigate suspected fraud, security incidents, or violations of our terms.

Business transfers. If we are involved in a merger, acquisition, financing, or sale of assets, personal information may be transferred as part of that transaction, subject to this policy.

Analytics and advertising on our websites. We use analytics and advertising tools on our websites, such as Google Analytics, PostHog, Meta, and LinkedIn, to understand how visitors use our sites and to measure and deliver our advertising, including on other websites and platforms. These providers may collect device, browser, and browsing activity information through cookies, pixels, and similar technologies, and may use it under their own privacy policies. Under some U.S. state privacy laws, this may be considered "selling" or "sharing" personal information, or processing it for targeted advertising. Section 8 explains how to opt out. We do not sell personal information for money, and we do not use customer content for advertising.

7. Where information is stored, and for how long

Location. Customer data is stored and processed in the United States. The application and primary database run on AWS in the us-east-1 (Northern Virginia) region. AI workflow state is stored in the same region. AI workflow compute runs in a U.S. West (Oregon) region. Diagnostic records generated by AI features are stored in the United States. Some business systems we use to operate the company — such as our CRM, email, and support tools — are provided by vendors that may process limited account and contact information in other regions, under contractual confidentiality, security, and transfer safeguards.

Retention.

Information	Retention
Customer content and account data, active subscription	For the duration of the subscription
Customer content and account data, after cancellation, non-renewal, or the end of a free trial without a purchase	1 year, then deleted, so that data is available if the account is reactivated
AI diagnostic traces	15 days
Billing and transaction records	As required by tax and accounting law

Sales and marketing contact records	Until the contact opts out or the record is no longer commercially relevant
Aggregated, de-identified datasets	Indefinitely, in de-identified form
Global event database records	For as long as the event or organization remains relevant to the database, subject to correction and removal requests under Section 8

Customers may request deletion of their workspace data at any time, including before the periods above expire. Where a customer's agreement specifies a different retention or deletion period, that agreement controls.

Backups are retained on a rolling schedule. Information deleted from active systems persists in backups until those backups expire, and is not restored to active use.

8. Your privacy rights

U.S. state privacy rights. Depending on your state of residence, you may have the right to know what personal information we hold about you, to access or obtain a copy of it, to correct inaccuracies, to request deletion, to opt out of the sale or sharing of personal information and of targeted advertising, and to be free from discrimination for exercising these rights. You can opt out of the analytics and advertising activity described in Section 6 by adjusting your browser's cookie settings, by using the opt-out tools those providers make available, or, where applicable law requires us to honor it, by enabling a Global Privacy Control signal in your browser. To exercise any right, contact us using Section 11. We will verify your identity before responding, except to requests to opt out, which do not require verification. You may use an authorized agent where permitted by law.

European Economic Area and United Kingdom. ExhibitHub is provided from the United States and is offered to businesses in the United States. We do not target or market the platform to individuals or organizations in the European Economic Area or the United Kingdom. Where GDPR or UK GDPR nonetheless applies, you may have the right to access, rectify, erase, restrict or object to processing, and to data portability, as well as the right to lodge a complaint with your supervisory authority. Where we transfer personal information outside the EEA or UK, we rely on Standard Contractual Clauses or another approved transfer mechanism, as set out in our Data Processing Addendum.

Requests about customer workspace data. If your information is in a customer's workspace, direct your request to that customer. We will assist them in responding and will refer you if you contact us directly.

Information in our global event database. If you work at an event organizer, venue, general contractor, or similar organization and your business contact information appears in our global event database, you may ask us what we hold about you, ask us to correct it, or ask us to remove it. Contact us using Section 11. We hold this information in our own right rather than on behalf of a customer, so we handle these requests directly. The database is intended to hold business contact information about people in a professional capacity, and is not intended to hold personal contact details. When we remove your information, we also take steps to prevent it from being added back when we next update the database. If a customer added your information to its workspace from the database before your request, that copy forms part of the customer's records. We will stop updating it from the database and may remove it, and you may also contact that customer directly.

9. Notice at collection for business contacts

If you have not used ExhibitHub but have heard from us, this section explains why.

What we collect. Business contact information — name, business email address, job title, employer, professional profile information, and publicly available details about your role and your company's event activity.

Where it comes from. Third-party business data providers, publicly available professional sources, and company websites. We do not obtain it from you directly, which is why this notice exists.

Why we use it. To identify organizations likely to benefit from the platform, and to contact you about it. Our legal basis, where applicable, is our legitimate interest in business-to-business marketing.

Your choices. You may opt out of further contact using the unsubscribe link in any message or by contacting us at Section 11. On request, we will tell you what we hold about you, correct it, or delete it. Because this information originates with third-party data providers, we can identify the category of source, and will identify the specific provider where we are able to.

10. Additional information

Security. We maintain administrative, technical, and organizational safeguards appropriate to the sensitivity of the information we hold, including encryption in transit and at rest, multi-factor authentication on administrative access, least-privilege access control, periodic access reviews, vendor security assessment, and a documented incident response process. Access to customer content by ExhibitHub personnel is limited to named individuals, granted on a least-privilege basis, permitted only for support, security, and operational purposes, and subject to confidentiality obligations. No system is completely secure, and we cannot guarantee absolute security.

Cookies and similar technologies. We use cookies, pixels, local storage, and similar technologies. Some are necessary for authentication, security, and site function. Others support analytics, so we can understand how our websites and platform are used and improve them, and advertising, so we can measure our marketing and show our ads to relevant audiences on other websites and platforms, as described in Section 6. You can control cookies through your browser settings, though blocking necessary cookies may prevent parts of the service from working. Where the law of your jurisdiction requires consent before non-essential cookies are set, we will ask for it.

Children. The platform is a business product not directed to children. We do not knowingly collect personal information from anyone under 16. If we learn we have, we will delete it.

Changes to this policy. We may update this policy. If we make a material change, we will update the date above and notify customers by email or in-product notice before it takes effect. Where a change would materially expand how we use customer content, the customer agreement governs and any consent required by law will be obtained. Prior versions are available on request.

11. Contact us

Exhibit Hub Inc.

658 Springridge Dr.

Lexington, KY 40503

United States

Privacy inquiries: privacy@exhibithub.com

Security matters: security@exhibithub.com