

Data Processing Addendum

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

This Data Processing Addendum ("DPA") forms part of the ExhibitHub Terms of Service or other written agreement between Exhibit Hub Inc. ("ExhibitHub," "we," "us") and the customer ("Customer," "you") governing use of the Service (the "Agreement"). It applies where we process Personal Data on your behalf.

This DPA takes effect automatically on acceptance of the Agreement. No signature is required. We will provide a countersigned copy on request.

1. Definitions

Terms not defined here have the meaning given in the Agreement.

Data Protection Laws — all laws applicable to the processing of Personal Data under this DPA, including the California Consumer Privacy Act as amended ("CCPA"), other U.S. state privacy laws, the EU General Data Protection Regulation ("GDPR"), and the UK GDPR and Data Protection Act 2018.

Personal Data — information within Customer Data that relates to an identified or identifiable natural person, or that constitutes "personal information" or "personal data" under Data Protection Laws.

Processing, Controller, Processor, Data Subject, Supervisory Authority — as defined in the GDPR, and their equivalents under other Data Protection Laws.

Personal Data Breach — a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data processed under this DPA. It does not include unsuccessful attempts or events that do not compromise the security of Personal Data, such as blocked intrusion attempts, port scans, or failed log-ins.

Subprocessor — a third party engaged by us to process Personal Data on your behalf.

Standard Contractual Clauses or SCCs — the clauses approved by the European Commission in Implementing Decision (EU) 2021/914.

UK Addendum — the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner.

2. Roles and scope

Roles. For Personal Data within Customer Data, you are the Controller (or a Processor acting for another Controller) and we are the Processor (or Subprocessor). Under the CCPA, you are the Business and we are a Service Provider.

Your responsibilities. You are responsible for the lawfulness of your collection of Personal Data, for providing required notices to Data Subjects, for obtaining any required consents, for the accuracy of Personal Data, and for

your instructions to us. You represent that you have the rights necessary to provide Personal Data to us for the processing described here.

Data we handle as Controller. We act as a Controller for the account registration and administrative details of your Users, billing contact and transaction information, the contact and routing metadata of support communications, and information about individuals we contact for our own sales and marketing. Our handling of that data is governed by our Privacy Policy, not by this DPA.

The carve-out is narrow. Where Personal Data drawn from your workspace is contained within a support communication — for example in a screenshot, attachment, exported record, or description of an issue — we process it as a Processor under this DPA, not as a Controller. The Controller carve-out covers the metadata of the interaction, not customer content that happens to travel inside it.

Global event database. We maintain a global database of trade show and conference information, compiled from publicly available materials and from our partners and licensors, which we make available within the Service. That database is our own data. We hold it as a Controller in our own right; it is not Customer Data, is not processed on your behalf, and is outside the scope of this DPA. Your rights of access, return, and deletion under this DPA do not extend to it. Where information from that database is populated into your workspace, the copy in your workspace is Customer Data and this DPA applies to that copy in the ordinary way.

We do not build that database from your data. We do not use documents or files uploaded to the Service to populate the global event database. Where you provide a URL, you authorize us to access it and to use publicly available information found there, and the fact that you have created an event record may prompt us to research that event from public sources; only information we obtain from public sources or from our partners and licensors is added to the database. Personal Data within your workspace is never added to it.

Precedence. This DPA prevails over the Agreement to the extent of any conflict on matters of data protection. Where the SCCs apply, they prevail over this DPA to the extent of conflict.

3. Processing instructions

We will process Personal Data only:

1. in accordance with your documented instructions, which are given by the Agreement, this DPA, your configuration and use of the Service, and any further written instructions you give that we agree to;
2. as described in Annex A;
3. as expressly permitted by Section 15 (aggregated and de-identified data); and
4. as required by applicable law, in which case we will inform you before processing unless that law prohibits it.

If we believe an instruction infringes Data Protection Laws, we will tell you without undue delay. We may decline an instruction that would require us to act unlawfully.

We will not sell Personal Data, share it for cross-context behavioral advertising, retain, use, or disclose it for any purpose other than performing the Service and the purposes permitted by this DPA, or combine it with personal information received from another source except as permitted by the CCPA. We will notify you if we determine we can no longer meet these obligations.

4. Duration

This DPA applies for as long as we process Personal Data on your behalf, and its obligations survive termination of the Agreement until deletion is complete under Section 12.

5. Confidentiality and personnel

We will ensure that personnel authorized to process Personal Data are subject to written confidentiality obligations that survive the end of their engagement, receive appropriate training, and are granted access only to the extent necessary for their role.

6. Security

We will implement and maintain the technical and organizational measures described in **Annex B**, designed to ensure a level of security appropriate to the risk. We may update those measures provided the overall level of protection is not materially reduced.

7. Subprocessors

Authorization. You give general authorization for us to engage Subprocessors. Our current Subprocessors are listed at <https://exhibithub.com/legal/subprocessors>.

Terms. We will impose on each Subprocessor written data protection obligations no less protective than those in this DPA, and we remain liable to you for their performance.

Changes and objection. We will notify you of any new Subprocessor at least **30 days** before it begins processing Personal Data, through the subscription mechanism available on the Subprocessor page. You may object on reasonable data protection grounds within that period. We will work with you in good faith to resolve the objection; if we cannot, you may terminate the affected part of the Service and receive a refund of prepaid fees for the unused portion.

Subprocessors of our Subprocessors. Our Subprocessors may themselves engage providers, and are contractually required to disclose them. **On your written request we will identify the providers engaged by any Subprocessor that processes Personal Data on your behalf**, and will point you to that Subprocessor's own published disclosure. Where a Subprocessor does not disclose a provider we consider material to your data, we will treat that as a factor in our vendor review of that Subprocessor.

Emergency changes. Where a Subprocessor must be replaced urgently for security, legal, or continuity reasons, we may do so before the notice period expires and will notify you as soon as practicable.

8. Data subject requests

Taking into account the nature of the processing, we will assist you by appropriate technical and organizational measures, insofar as possible, in responding to Data Subject requests to exercise rights under Data Protection Laws.

The Service provides functionality allowing you to access, correct, export, and delete Personal Data within your workspace. Where you cannot address a request through the Service, we will provide reasonable assistance on request.

If we receive a request directly from a Data Subject relating to Personal Data we process on your behalf, we will not respond substantively, and will refer them to you and notify you without undue delay.

9. Personal Data Breach

We will notify you **without undue delay** after becoming aware of a Personal Data Breach affecting Personal Data processed on your behalf.

Our notification will describe, to the extent known at the time: the nature of the breach and the categories and approximate number of Data Subjects and records affected, the likely consequences, and the measures taken or proposed. Where information is not available at the time, we will provide it in phases as it becomes available, without undue further delay.

We will take reasonable steps to contain and remediate the breach, and will provide reasonable assistance with your own notification obligations to Supervisory Authorities or Data Subjects.

Our notification is not an acknowledgment of fault or liability.

10. Assistance with impact assessments

Taking into account the nature of the processing and the information available to us, we will provide reasonable assistance with data protection impact assessments and prior consultations with Supervisory Authorities, where required by Data Protection Laws in relation to the Service. Assistance beyond providing existing documentation may be subject to reasonable fees.

11. Audits and assessments

We will make available the information reasonably necessary to demonstrate compliance with this DPA. In the ordinary course this is satisfied by:

- our published security documentation and Subprocessor list;
- completed responses to your security questionnaire; and
- any third-party audit reports or certifications we hold.

Where Data Protection Laws require an on-site or on-system audit, you may conduct one, or appoint an independent auditor who is not our competitor and who signs appropriate confidentiality obligations, subject to: **no more than once in any twelve-month period** (unless required by a Supervisory Authority or following a Personal Data Breach), **at least 30 days' written notice**, during business hours, without unreasonable disruption, limited to information relevant to processing under this DPA, and **at your expense**.

Nothing in this Section requires us to disclose information that would compromise the security or confidentiality of other customers' data or our own systems.

12. Deletion and return

Your choice. On termination or expiry of the Agreement, you may direct us to **return** Personal Data to you, to **delete** it, or both. You may make that election at any time up to the end of the export period below, or afterwards.

Return. For **30 days** after termination, you may export Personal Data through the Service or by written request. We will provide reasonable assistance with an export you cannot complete through the Service. Return covers Personal Data held in the Service. Personal Data held by a Subprocessor solely for diagnostic or observability purposes is short-lived, is not separately exportable, and is deleted rather than returned; where such a Subprocessor offers deletion but no export, we will direct deletion.

Deletion. Where you direct deletion, we will complete it within **30 days** of your direction.

Where you make no election. So that your data remains available if you reactivate your account, we retain Personal Data for **one year** after termination and then delete it. This retention is part of your documented instructions under Section 3 and applies only in the absence of a contrary direction; you may direct deletion at any point during that year and we will act on it under the paragraph above.

Where the GDPR or UK GDPR applies to the Personal Data, no default retention applies. We will delete Personal Data at the end of the export period unless you have directed otherwise.

Where your Agreement or Order Form specifies a different period, that period controls.

Backups. Deleted Personal Data persists in backups until those backups expire in the ordinary course. It is not restored to active use, and remains subject to this DPA until deleted.

Legally required retention. We may retain Personal Data where required by applicable law, for so long as required, and will continue to protect it under this DPA.

13. International transfers

Data location. We process Personal Data in the United States. Annex A describes our processing locations.

EEA transfers. Where you transfer Personal Data subject to GDPR to us, the SCCs apply and are incorporated by reference, with the module and option selections in **Annex D**.

UK transfers. Where UK GDPR applies, the SCCs as modified by the UK Addendum apply, with the selections in Annex D.

Swiss transfers. Where Swiss data protection law applies, the SCCs apply with references construed to include Switzerland and the Federal Data Protection and Information Commissioner as the competent authority.

Alternative mechanisms. If a transfer mechanism referenced here is invalidated or replaced, we will adopt an alternative lawful mechanism without undue delay.

14. U.S. state privacy laws

For Personal Data subject to the CCPA or comparable U.S. state privacy laws:

- We act as a Service Provider (or the equivalent term used by the applicable law) and process Personal Data only for the business purposes set out in Annex A.

- We do not sell Personal Data and do not share it for cross-context behavioral advertising.
- We will comply with applicable obligations and provide the level of privacy protection required.
- You may take reasonable and appropriate steps to ensure our processing is consistent with your obligations, and to stop and remediate unauthorized processing, through the mechanisms in Section 11.

15. Aggregated and de-identified data

You authorize us to create aggregated, de-identified datasets derived from Customer Data, and to use them to operate, analyze, and improve the Service, to provide benchmarking and cost-projection features, and to publish aggregate market materials such as industry benchmark and cost reports. This authorization forms part of your documented instructions under Section 3, and the commitments below apply to every use of those datasets, including anything we publish externally.

We commit that:

- 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 you or to an individual.
- We take reasonable measures to prevent re-identification, do not attempt to re-identify, and contractually prohibit recipients from doing so.
- We publicly commit to maintain and use this data only in de-identified form.
- No derived figure is surfaced unless 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.
- We will not use Personal Data for advertising, disclose it to other customers in identifiable form, or use it to train or fine-tune general-purpose artificial intelligence models for the benefit of others. We may process Personal Data to provide, secure, support, troubleshoot, and evaluate the Service for you, as part of the processing described in Annex A.

Data properly de-identified under this Section is not Personal Data and is outside the scope of the remainder of this DPA.

AI providers. Every AI model provider that receives Personal Data is engaged as a Subprocessor under Section 7 and is listed on our Subprocessor page. Our arrangements with those providers, as we have configured them, prohibit the use of Personal Data to train or improve their models. Providers may retain inputs and outputs briefly for abuse monitoring and service delivery; the retention period applicable to each provider is stated on our Subprocessor page. We do not use Personal Data to train, fine-tune, or improve any model for the benefit of another customer.

16. Liability

Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement. Where the SCCs apply, nothing in this Section limits any liability that cannot be limited under the SCCs or applicable law.

17. General

Changes. We may update this DPA where necessary to reflect changes in Data Protection Laws, the Service, or our processing, provided the change does not materially reduce your protections. Material changes will be notified in accordance with the Agreement.

Severability. If a provision is held invalid, the remainder continues in effect.

Governing law. As set out in the Agreement, except where Data Protection Laws or the SCCs require otherwise.

Annex A — Details of processing

Subject matter. Provision of the ExhibitHub platform for planning, executing, and measuring trade show and conference participation.

Duration. For the term of the Agreement, plus the retention period in Section 12.

Nature and purpose of processing. Hosting, storage, organization, retrieval, transmission, analysis, and deletion of Customer Data as necessary to provide, secure, support, and maintain the Service; extraction and structuring of information from documents submitted by Customer using AI features; provision of support.

Categories of Data Subjects.

- Customer's personnel and contractors who are Users of the Service
- Individuals recorded in the Service who are not Users, including staff scheduled to work an event
- Customer's external collaborators, such as exhibit house and travel coordination personnel
- Customer's vendor, venue, and supplier contacts

Categories of Personal Data.

- Identification and contact data: name, business email address, telephone number, job title, employer, office location
- Account data: user identifier, workspace role, permissions, authentication events
- Event participation data: event assignments, roster entries, schedules, shift and booth assignments, registration records
- Travel and accommodation data: itineraries, booking references, travel dates, accommodation assignments
- Financial and expense data: expense records, receipts, invoices, and cost allocations attributed to individuals
- Content data: documents, files, comments, and notes submitted by Customer that may contain Personal Data
- Technical data: IP address, device and browser information, access logs and timestamps

Special categories. None are required by the Service, and Customer is instructed not to submit them, including within documents such as receipts, invoices, and travel confirmations. Customer is responsible for removing or redacting such details before submission. Where ExhibitHub becomes aware that such data has been submitted, it may delete it or require Customer to do so.

Frequency. Continuous, for the duration of the Agreement.

Processing locations. The United States. Application hosting and the primary database are in AWS us-east-1 (Northern Virginia). AI workflow state is in the same region. AI workflow compute is in a U.S. West (Oregon) region. Diagnostic records generated by AI features are stored in the United States.

Controller contact. As designated in Customer's account.

Processor contact. privacy@exhibithub.com

Annex B — Technical and organizational measures

The following measures are in place. They are described at the level of what we operate, not what we aspire to.

Access control

- Individual named accounts; no shared credentials for systems that support individual accounts
- Multi-factor authentication on administrative access to production systems
- Least-privilege access, granted by role and reviewed quarterly against an access register
- Credentials managed in a dedicated password manager; no credentials in source control
- Access revoked promptly on role change or departure

Encryption

- Personal Data encrypted in transit using TLS
- Personal Data encrypted at rest by the underlying platform providers

Application security

- Passwordless authentication for the Service; no account passwords stored
- Server-side authorization enforced on every request; workspace isolation enforced at the data layer
- Dependency vulnerability monitoring with defined remediation timeframes
- Code changes reviewed before deployment to production

Vendor and Subprocessor management

- Documented vendor risk assessment before a system processes Customer Data
- Maintained inventory of systems and vendors, recording criticality, data types, and Subprocessor status
- Contractual data protection terms with Subprocessors

Operational security

- Documented information security policy set, reviewed at least annually and acknowledged by all personnel
- Documented acceptable use policy governing personnel behavior and third-party application connections
- Documented incident response plan with defined severity levels, roles, and communication paths
- Logging of administrative actions and authentication events
- Company-managed endpoints with full-disk encryption, screen lock, and automatic updates

Personnel

- Confidentiality obligations in place for all personnel
- Background checks for employees, subject to applicable law
- Security awareness expectations documented and acknowledged annually

Annex C — Subprocessors

Our current Subprocessors, the processing each performs, and their locations are published at <https://exhibithub.com/legal/subprocessors>, which forms part of this DPA. Customers may subscribe there to receive notice of changes as described in Section 7.

Annex D — Standard Contractual Clauses selections

Where the SCCs apply under Section 13:

Item	Selection
Module	Module Two (Controller to Processor), or Module Three (Processor to Processor) where Customer acts as a Processor
Clause 7 (docking)	Applies
Clause 9 (subprocessors)	Option 2, general written authorization, with 30 days' notice
Clause 11 (redress)	Optional independent dispute resolution language does not apply
Clause 17 (governing law)	The law of Ireland
Clause 18 (forum)	The courts of Ireland
Annex I.A (parties)	Data exporter: Customer, as identified in its Account or Order Form, acting as Controller (or Processor under Module Three). Contact: the account contact designated by Customer. Activities: use of the Service as described in Annex A. Data importer: Exhibit Hub Inc., 658 Springridge Dr., Lexington, KY 40503, United States, acting as Processor. Contact: privacy@exhibithub.com . Activities: provision of the Service as described in Annex A.
Annex I.B (description of transfer)	As set out in Annex A of this DPA
Annex I.C (competent supervisory authority)	Determined under Clause 13. Where Customer is established in an EU Member State, the supervisory authority of that Member State. Where Customer is not established in the EU but is subject to the GDPR under Article 3(2) and has appointed an Article 27 representative, the supervisory authority of the Member State in which that representative is established. Otherwise, the supervisory authority of Ireland.

Annex II (technical and organizational measures)

As set out in Annex B of this DPA

Annex III (subprocessors)

As set out in Annex C of this DPA

UK Addendum. Where UK GDPR applies, the SCCs are modified by the UK Addendum, completed as follows:

Table	Completion
Table 1 (parties)	As set out in Annex I.A above, with start date being the effective date of the Agreement
Table 2 (selected SCCs)	The SCCs referenced above, with the module, clause, and option selections in this Annex D
Table 3 (appendix information)	Annex A, Annex B, and Annex C of this DPA
Table 4 (ending the Addendum)	Neither party may end the Addendum as set out in Section 19 of the Addendum

For UK transfers, references in the SCCs to the GDPR are read as references to the UK GDPR, the governing law is the law of England and Wales, and the courts of England and Wales have jurisdiction. The competent supervisory authority is the Information Commissioner's Office.

Swiss adaptations. Where Swiss data protection law applies, the SCCs apply with the following clarifications: the competent supervisory authority is the Federal Data Protection and Information Commissioner; references to the GDPR are read as references to the Swiss Federal Act on Data Protection; the term "Member State" does not exclude Data Subjects in Switzerland from bringing proceedings in Switzerland; and, for so long as Swiss law affords such protection, references to personal data include data relating to legal entities.