Acara Data Processing Agreement

DRAFT for legal review — not yet in force. Items marked [●] must be completed or confirmed before publication.

Based on the iubenda GDPR DPA starter template (art. 28 GDPR), adapted for Acara as a SaaS processor and extended for UK GDPR and US state privacy laws.

This Data Processing Agreement ("**DPA**") forms part of the agreement between:

- **Acara Software Limited**, a company registered in England and Wales under number [●], with its registered office at 147 De Beauvoir Road, London, N1 4DL ("**Acara**", the "**Processor**"); and
- the customer identified in the applicable order form, subscription or account ("**Customer**", the "**Controller**"),

for the provision of the Acara event management platform (the "**Main Agreement**", including Acara's Terms and Conditions).

The DPA applies when Customer accepts it, either by signing it or by agreeing to the Main Agreement, and stays in force for as long as Acara processes Customer Personal Data.

Customer enters into this DPA for itself and, where Data Protection Laws require it, on behalf of its affiliates that use the Services under the Main Agreement.

Acara's privacy contact for this DPA is **[●] privacy@acara.io**. Acara sends notices under this DPA to Customer's account owner email address, or to another address Customer designates for privacy notices.

1. Definitions

1.1 "**Data Protection Laws**" means all laws relating to personal data that apply to the processing under this DPA, including: (a) the UK GDPR and the Data Protection Act 2018; (b) Regulation (EU) 2016/679 ("**EU GDPR**"); (c) the Swiss Federal Act on Data Protection; and (d) US state privacy laws, including the California Consumer Privacy Act as amended by the CPRA ("**CCPA**").

1.2 "**Customer Personal Data**" means personal data that Acara processes on Customer's behalf in providing the Services, as described in Annex 1.

1.3 "**Services**" means the Acara platform and related services provided under the Main Agreement.

1.4 "**Sub-processor**" means any third party engaged by Acara to process Customer Personal Data.

1.5 "**Security Incident**" means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data. It does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, such as failed log-in attempts, pings, port scans or denial-of-service attacks.

1.6 "**Restricted Transfer**" means a transfer of Customer Personal Data that requires a transfer mechanism under Chapter V of the UK GDPR or EU GDPR.

1.7 "**Usage Data**" means information about how the Services are accessed and used, such as feature usage, performance, error and security logs, and aggregated or de-identified statistics. It does not include the content of Customer Personal Data.

1.8 "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**Processing**" and "**Supervisory Authority**" have the meanings given in the UK GDPR or EU GDPR, as applicable. "**Business**", "**Service Provider**", "**Sell**" and "**Share**" have the meanings given in the CCPA.

2. Roles and scope

2.1 Customer is the Controller (or, where Customer acts for another controller, a Processor) of Customer Personal Data. Acara is the Processor (or Sub-processor) and acts on Customer's behalf.

2.2 This DPA does not apply to personal data that Acara processes as an independent controller. This includes account and billing data of Customer's own users that Acara uses to manage its customer relationship, and data from visitors to acara.io, which is covered by the Acara Privacy Policy.

2.3 Where Usage Data contains personal data, Acara is its controller. Acara uses Usage Data only to operate, secure, support and improve the Services, and for billing, analytics and reporting. Acara will not use Usage Data to identify Customer's attendees or market to them, and will anonymise or delete the personal data in Usage Data when it is no longer needed.

2.4 The subject matter, duration, nature and purpose of processing, the types of personal data and the categories of Data Subjects are set out in Annex 1.

2.5 Customer is responsible for: (a) the lawfulness of the processing instructions it gives; (b) having a lawful basis for the processing, including any consents required from attendees and other Data Subjects; and (c) giving Data Subjects the notices required under Data Protection Laws.

3. Customer instructions

3.1 Acara will process Customer Personal Data only on Customer's documented instructions, unless applicable law requires otherwise. If it does, Acara will inform Customer before processing, unless that law prohibits it.

3.2 Customer's documented instructions are this DPA, the Main Agreement, and Customer's configuration and use of the Services (including the integrations Customer chooses to connect). Any additional instructions must be agreed in writing.

3.3 Acara will tell Customer promptly if, in its opinion, an instruction infringes Data Protection Laws. In that case Acara may suspend the processing concerned until the instruction is confirmed or changed.

4. Confidentiality

Acara will ensure that anyone it authorises to process Customer Personal Data is bound by an appropriate duty of confidentiality and processes the data only as needed to provide the Services.

5. Security

5.1 Acara will implement appropriate technical and organisational measures to protect Customer Personal Data, as required by art. 32 UK GDPR / EU GDPR. Those measures are described in Annex 2.

5.2 Acara may update these measures as technology develops, provided the overall level of security is not reduced.

5.3 Customer is responsible for its own use of the Services, including: (a) deciding whether the Services meet its security and legal requirements; (b) managing which team members have access and with which roles; (c) securing the email accounts and devices used to log in to the Services; and (d) keeping its own copies of data it needs to retain, for example through the export functions.

5.4 A cyberattack, malware incident, unauthorised access or other act by a third party does not excuse Acara from its obligations under this DPA to the extent the event was caused or contributed to by Acara's breach of this DPA, negligence, personnel or Sub-processors.

6. Sub-processors

6.1 Customer gives Acara general authorisation to engage Sub-processors. The Sub-processors in use on the date of this DPA are listed in Annex 3.

6.2 Acara will impose data protection obligations on each Sub-processor that are no less protective than those in this DPA, as required by art. 28(4) UK GDPR / EU GDPR. Acara remains liable to Customer for each Sub-processor's performance of those obligations.

6.3 Acara will notify Customer of any intended addition or replacement of a Sub-processor at least **[30] days** before the change, by email to Customer's account owner or through an updated Sub-processor list at [●] acara.io/docs/subprocessors. If Acara reasonably needs to replace a Sub-processor urgently to protect Customer Personal Data or avoid a material disruption to the Services, it will give notice as soon as reasonably practicable instead.

6.4 Customer may object to a new Sub-processor on reasonable data protection grounds within that notice period. The parties will discuss the objection in good faith. If they cannot resolve it, Customer may terminate the affected Services by written notice. Acara will refund any prepaid fees for the part of the term after termination.

6.5 Integrations Customer enables (for example HubSpot, Salesforce, Drip or Customer.io) are not Sub-processors of Acara. They are third parties chosen by Customer, and data is sent to them on Customer's instruction.

7. International transfers

7.1 Acara and its Sub-processors may process Customer Personal Data in the countries listed in Annex 3.

7.2 For any Restricted Transfer, Acara will ensure an appropriate safeguard is in place, such as:

- (a) adequacy regulations or decisions, including the EU-US Data Privacy Framework and its UK Extension, where the recipient is certified;
- (b) the EU Standard Contractual Clauses (Commission Decision 2021/914), Module Two or Three as appropriate ("**EU SCCs**");
- (c) the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner ("**UK Addendum**"), or the UK International Data Transfer Agreement.

7.3 Where Customer transfers Customer Personal Data to Acara and that transfer is a Restricted Transfer, the EU SCCs and the UK Addendum are incorporated into this DPA by reference, completed as follows: Module Two (or Three) for Customer Personal Data, and Module One for any Usage Data of which both parties are controllers; clause 7 docking clause applies; clause 9 option 2 with the notice period in section 6.3; clause 11 optional language does not apply; clauses 17 and 18 governed by the laws of, and courts of, Ireland; Annex I, II and III are completed by Annexes 1, 2 and 3 of this DPA. `[●] Confirm whether Acara receives transfers from the EU/UK, given its establishment.`

8. Data Subject rights

8.1 Taking into account the nature of the processing, Acara will assist Customer by appropriate technical and organisational measures, insofar as possible, to respond to requests from Data Subjects to exercise their rights.

8.2 If Acara receives a request directly from a Data Subject about Customer Personal Data, it will forward the request to Customer without undue delay and will not respond except to direct the Data Subject to Customer, unless the law requires otherwise.

8.3 Customer can access, export, correct and delete Customer Personal Data through the Services. Where Customer cannot do so itself, Acara will provide reasonable assistance.

9. Security Incidents

9.1 Acara will notify Customer without undue delay, and in any event within **[48] hours**, after becoming aware of a Security Incident.

9.2 The notice will include, as far as is then known: the nature of the incident; the categories and approximate number of Data Subjects and records concerned; the likely consequences; and the measures taken or proposed. Acara will provide further information as it becomes available.

9.3 Acara will take reasonable steps to contain, investigate and mitigate the Security Incident.

9.4 Acara may delay notice where law enforcement asks it to, or for as long as strictly needed to contain the incident. Any such delay will not count as undue delay.

9.5 Customer remains responsible for notifying Supervisory Authorities and affected Data Subjects where Data Protection Laws require it. Acara will not notify Customer's Data Subjects directly unless Customer instructs it to or the law requires it.

9.6 Notification of a Security Incident is not an acknowledgement of fault or liability.

10. Assistance

Taking into account the nature of the processing and the information available to it, Acara will provide reasonable assistance to Customer with data protection impact assessments, prior consultations with Supervisory Authorities, and Customer's other obligations under arts. 32 to 36 UK GDPR / EU GDPR. Acara may charge reasonable fees for assistance beyond what the Services already provide, unless the need for it arises from Acara's breach of this DPA.

11. Audits

11.1 Acara will make available to Customer the information reasonably necessary to demonstrate its compliance with this DPA and art. 28 UK GDPR / EU GDPR.

11.2 Acara will first meet audit requests by providing written answers to reasonable security questionnaires and, where available, current third-party audit reports or certifications.

11.3 If that information is not enough to demonstrate compliance, or a Supervisory Authority requires it, Customer (or an independent auditor bound by confidentiality) may carry out an audit:

- (a) no more than once in any 12-month period, unless after a Security Incident or at a Supervisory Authority's request;
- (b) with at least 30 days' written notice, during normal business hours, without unreasonable disruption to Acara's operations;
- (c) under a scope and plan agreed in advance, limited to the systems and records relevant to Customer Personal Data;
- (d) subject to confidentiality obligations covering everything learned during the audit;
- (e) at Customer's cost, including Acara's reasonable time at its then-current rates.

11.4 Customer will share the findings of any audit with Acara.

12. Deletion and return

12.1 When the Services end, Customer may export Customer Personal Data using the Services' export functions, for **[30] days** after termination.

12.2 After that period, Acara will delete Customer Personal Data within **[90] days**, unless the law requires Acara to keep it. Backups will be overwritten within their normal rotation cycle of **[●] days**. Retained data stays subject to this DPA.

12.3 On request, Acara will confirm the deletion in writing.

13. US state privacy laws

13.1 Where the CCPA or another US state privacy law applies, Acara acts as Customer's Service Provider (or Processor) and will not:

- (a) Sell or Share Customer Personal Data;
- (b) retain, use or disclose Customer Personal Data for any purpose other than performing the Services, or as otherwise permitted for service providers under the CCPA;
- (c) retain, use or disclose Customer Personal Data outside the direct business relationship between Customer and Acara;
- (d) combine Customer Personal Data with personal data it receives from other sources, except as permitted by the CCPA.

13.2 Acara will comply with applicable obligations under the CCPA and will provide the same level of privacy protection as the CCPA requires of Customer. Acara will notify Customer if it determines that it can no longer meet those obligations.

13.3 Customer may take reasonable and appropriate steps to stop and remediate unauthorised use of Customer Personal Data, including under section 11.

13.4 The processing described in Annex 1 is integral to the Services and within the direct business relationship between Customer and Acara. Acara's access to Customer Personal Data is not part of the consideration exchanged under the Main Agreement.

13.5 Acara certifies that it understands and will comply with the restrictions in this section 13.

14. Liability

14.1 To the maximum extent permitted by law, neither party is liable to the other under or in connection with this DPA for any indirect, special, incidental, consequential, exemplary or punitive loss, or for loss of profits, revenue, goodwill or anticipated savings, however caused.

14.2 To the maximum extent permitted by law, Acara's total aggregate liability arising out of or in connection with this DPA, whether in contract, tort (including negligence), breach of statutory duty or otherwise, will not exceed the greater of: (a) **US$5,000**; and (b) the liability cap calculated under the Main Agreement. This is one shared aggregate cap across this DPA and the Main Agreement, not a separate or additional cap.

14.3 Clause 14.1 does not exclude Customer's reasonable, documented and direct costs of investigating, containing, notifying and remediating a Security Incident caused by Acara's breach of this DPA. Those costs remain subject to clause 14.2.

14.4 Nothing in this DPA limits or excludes: (a) liability for death or personal injury caused by negligence; (b) liability for fraud or fraudulent misrepresentation; (c) a Data Subject's direct statutory rights or claims against either party, including under art. 82 UK GDPR / EU GDPR; (d) liability under the EU SCCs or UK Addendum to the extent a limitation would contradict or undermine them; (e) a Supervisory Authority's powers; or (f) liability that cannot be limited or excluded by law.

14.5 Each party is responsible for administrative fines and penalties imposed directly on it. Neither party must reimburse a fine or penalty imposed on the other party unless, and only to the extent that, such reimbursement is expressly required by the Main Agreement and is permitted by law.

14.6 Nothing in this section prevents either party from seeking contribution from the other under art. 82(5) UK GDPR / EU GDPR to the extent permitted by law. Any contractual limitation on such contribution applies only to the extent it is lawful and does not restrict a Data Subject's rights.

15. General

15.1 If this DPA and the Main Agreement conflict on the processing of Customer Personal Data, this DPA prevails. Claims arising from the same event under this DPA and the Main Agreement do not create separate liability caps. If this DPA and the EU SCCs or UK Addendum conflict, the EU SCCs or UK Addendum prevail.

15.2 Acara may update this DPA where required by changes in Data Protection Laws or guidance from a Supervisory Authority, or where the update does not materially reduce Customer's protections. Acara will give notice of material changes.

15.3 Except where the EU SCCs require otherwise, this DPA is governed by the laws of England and Wales, and the courts of England and Wales have exclusive jurisdiction.

Annex 1 — Details of processing

Subject matter and duration

Processing of Customer Personal Data to provide the Services, for the term of the Main Agreement and the deletion period in section 12.

Nature and purposes of processing

Acara processes Customer Personal Data to:

- create, manage and secure Customer and attendee accounts;
- publish and run Customer's events and event pages;
- collect registrations, process ticket orders, assign tickets and manage refunds;
- send account, registration, ticket and event emails;
- provide check-in, attendance tracking, chat, Q&A, video and streaming features;
- capture, store, organise and export contacts, leads and form responses, including through the lead scanner;
- sync data with CRM and marketing tools that Customer connects;
- host and deliver files, images, video and other event content;
- provide reporting, analytics, security, troubleshooting and audit logs;
- provide AI-assistant features where Customer uses them.

Processing operations include collection, recording, organisation, storage, retrieval, use, transmission, export, restriction and deletion.

Categories of Data Subjects

- Customer's personnel, administrators and invited team members
- Event registrants, ticket purchasers, attendees and ticket assignees
- Leads and contacts who submit forms or are scanned at events
- Speakers, sponsors, exhibitors and their representatives
- Visitors to Customer's event pages
- Users of chat, Q&A, video and streaming features

Categories of personal data

- **Identity and contact:** name, email, phone, postal address, country, company, job title, biography, profile photo, social links
- **Account and access:** user IDs, roles and permissions, login codes and session tokens, IP address, device and browser data, consent records
- **Registration and ticketing:** orders, tickets, ticket assignees, attendance status, discount codes, refunds, amounts paid, Stripe payment references (Acara does not store card numbers)
- **Forms, leads and CRM:** form and survey answers, custom fields set by Customer, lead notes and qualification answers, contact preferences
- **Check-in:** attendee lists, badge fields, check-in records, offline-cached attendee data in the check-in app
- **Engagement and content:** chat messages, Q&A, uploaded files, images, video, and audio or webcam content where users choose to use those features
- **Usage and technical:** page views, URLs, referrers, timestamps, language, timezone, campaign parameters, video engagement, pseudonymous identifiers
- **AI assistant (where used):** prompts, relevant event context and usage records

Special category data

The Services are not designed to process special category data or criminal offence data. Customer must not collect such data through custom form fields unless it has a lawful basis and has assessed the risks. `[●] Consider dietary/accessibility fields, which can reveal health or religious information.`

Frequency

Continuous, for the duration of the Services.

Annex 2 — Technical and organisational measures

`[●] Every item must reflect Acara's actual practice. Remove anything that is not true today.`

Where the EU SCCs or UK Addendum apply, this Annex is Annex II to them.

- **Encryption:** data encrypted in transit (TLS 1.2+) and at rest by the hosting providers.
- **Access control:** passwordless (magic-link) login; role-based permissions within Customer organisations; production access limited to authorised Acara staff on a need-to-know basis; [●] multi-factor authentication for staff access to production systems and provider consoles.
- **Session security:** short-lived login codes (about 30 minutes), session expiry after inactivity, rate limiting on authentication endpoints.
- **Tenant isolation:** logical separation of Customer data by organisation in the application.
- **Infrastructure:** hosting on managed cloud providers (Annex 3) with their physical, environmental and network security controls.
- **Monitoring and logging:** application error monitoring and audit logging; [●] alerting on suspicious activity.
- **Backups and resilience:** [●] automated database backups, retention [●] days, restore tested [●].
- **Payment data:** card payments handled by Stripe (PCI DSS Level 1); Acara does not store card numbers.
- **Staff:** confidentiality obligations for all personnel with access; [●] security and privacy training.
- **Development:** code review before production deployment; [●] dependency vulnerability scanning.
- **Incident response:** documented process to investigate, contain and notify Security Incidents in line with section 9.

- **Physical security:** Acara does not run its own data centres. Physical and environmental controls are provided by the hosting providers in Annex 3 under their own certifications (for example ISO 27001 and SOC 2).
- **Testing:** [●] independent penetration test every [12] months; findings tracked to resolution.
- **Data minimisation and deletion:** Customer controls which fields are collected; deletion and export functions available in the Services.
- **Accountability:** [●] internal data protection and information security policies reviewed at least annually; records of processing activities; Security Incident log.
- **Sub-processor measures:** each Sub-processor must (a) notify Acara of security incidents so Acara can notify Customer; (b) delete data when Acara instructs; (c) not engage further sub-processors without authorisation; (d) not change the processing location without notice; and (e) not process data in a way that conflicts with Customer's instructions.

Annex 3 — Sub-processors

`[●] Confirm each entry, the contracting entity and the processing location. Hosting regions in earlier notes conflict (GKE in northamerica-northeast1 / Canada vs US servers); confirm before publishing.`

Sub-processor	Purpose	Location	Transfer safeguard
Google Cloud Platform (Google LLC)	Application hosting (GKE), file and asset storage	[●]	DPF + UK Extension / SCCs
MongoDB Atlas (MongoDB, Inc.)	Primary database (application, chat, analytics data)	[●]	DPF + UK Extension / SCCs
[●] Redis provider	Caching, rate limiting, real-time messaging, job queues	[●]	[●]
DigitalOcean, LLC	Proxy servers routing service traffic	[●]	DPF + UK Extension / SCCs
BunnyWay d.o.o. (bunny.net)	DNS hosting and resolution	EU (Slovenia)	Adequacy / EU
Stripe Payments Europe Ltd / Stripe, Inc.	Payments, subscriptions, refunds	[●]	DPF + UK Extension / SCCs
Twilio SendGrid (Twilio Inc.)	Transactional email	United States	DPF + UK Extension / SCCs
Mux, Inc.	Video upload, hosting, streaming and analytics	United States	[●]
Functional Software, Inc. (Sentry)	Error monitoring	[●]	DPF + UK Extension / SCCs
PostHog Inc.	Product analytics	[●] US or EU	[●]
OpenAI, L.L.C.	AI assistant (where used)	United States	DPF + UK Extension / SCCs
Anthropic, PBC	AI assistant (where used)	United States	[●]
Google LLC (Maps / Places)	Address autocomplete	United States	DPF + UK Extension / SCCs
Mapbox, Inc.	Map display	United States	[●]

Customer-enabled integrations (HubSpot, Salesforce, Drip, Customer.io) are not Sub-processors; see section 6.5.

The current list is maintained at [●] acara.io/docs/subprocessors and replaces this table once published.

Signatures

Where not accepted electronically through the Main Agreement:

	Customer	**Acara**
Signature		
Name		
Title		
Date		