UK GDPR · ARTICLE 28 COMPLIANT

Data Processing Agreement

This Agreement governs how VenueOra processes personal data on behalf of the Customer in connection with the VenueOra Platform. It forms part of the Terms of Service and is required to be in place before VenueOra processes any personal data on the Customer's behalf.

LEGAL BASIS	GOVERNING LAW	DATA PROCESSOR	VERSION
UK GDPR Article 28	England & Wales	VenueOra Ticketing Limited	1.0 — March 2026

P Parties to this Agreement

DATA CONTROLLER

The Customer

The business or organisation that has entered into the VenueOra Terms of Service and is identified as the "Customer" in the associated account. As Controller, you determine the purposes and means of processing personal data on the VenueOra Platform.

DATA PROCESSOR

VenueOra Ticketing Limited

A company registered in England and Wales. VenueOra operates the Platform and processes personal data solely on the Customer's documented instructions and for the purposes described in this Agreement.

Incorporated into Terms of Service

This Agreement is incorporated by reference into the VenueOra Terms of Service (the "Principal Agreement"). Defined terms used but not defined here have the meanings given in the Principal Agreement. In the event of any conflict between this Agreement and the Principal Agreement regarding data protection matters, this Agreement shall prevail.

B Background

In connection with the provision of the VenueOra Platform, VenueOra will process personal data on behalf of the Customer. The personal data processed includes information about the Customer's members, ticket purchasers, event attendees, and other individuals whose data the Customer has collected and loaded onto the Platform in its capacity as a Data Controller.

This Agreement sets out the terms on which VenueOra (as Processor) will process that personal data on behalf of the Customer (as Controller), as required by Article 28 of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1 Definitions

"Applicable Data Protection Law"	The UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (PECR), and any other applicable data protection or privacy legislation in force from time to time in the United Kingdom.
"Controller"	Has the meaning given in UK GDPR Article 4(7) — the Customer, who determines the purposes and means of processing.
"Data Subject"	An identified or identifiable natural person to whom the personal data relates, including members, ticket purchasers, event attendees, and any other individuals whose data the Customer processes via the Platform.
"Personal Data"	Any information relating to a Data Subject that VenueOra processes on the Customer's behalf via the Platform, as further described in Schedule 1.
"Personal Data Breach"	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by VenueOra on the Customer's behalf.
"Platform"	The VenueOra SaaS platform including the Ticketing, Events, Membership Management, Locker, Kiosk, Communications, and other enabled modules, together with any associated APIs and integrations.
"Processor"	Has the meaning given in UK GDPR Article 4(8) — VenueOra, which processes Personal Data on behalf of the Controller.
"Processing"	Has the meaning given in UK GDPR Article 4(2) — any operation or set of operations performed on Personal Data, including collection, recording, storage, retrieval, use, disclosure, erasure, and destruction.
"Special Category Data"	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic data; biometric data (where processed for the purpose of uniquely identifying a person); data concerning health; data concerning a person's sex life or sexual orientation.
"Sub-Processor"	Any third party engaged by VenueOra (as Processor) to carry out any processing activity on the Customer's Personal Data on VenueOra's behalf.
"Supervisory Authority"	The Information Commissioner's Office (ICO), or any successor body.
"Technical and Organisational Measures" (TOMs)	The security and procedural measures described in Schedule 3 of this Agreement, as updated from time to time.

"UK GDPR"	The General Data Protection Regulation as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended from time to time.

2 Scope & Duration

2.1 Scope of Processing

This Agreement applies to all processing of Personal Data carried out by VenueOra on behalf of the Customer via the Platform. The details of the processing — including the nature, purpose, types of Personal Data, and categories of Data Subjects — are set out in Schedule 1.

2.2 Duration

This Agreement shall remain in force for as long as VenueOra processes Personal Data on behalf of the Customer, beginning on the date the Customer first uses the Platform and ending on the later of:

- the termination or expiry of the Principal Agreement; or
- the date on which VenueOra completes the return or deletion of all Personal Data as required by Clause 11.

2.3 Relationship to the Principal Agreement

This Agreement supplements and forms part of the Principal Agreement. The Customer's continued use of the Platform following the effective date of this Agreement constitutes acceptance of its terms. VenueOra may update this Agreement from time to time in accordance with Clause 13.3, with reasonable advance notice provided.

3 Controller Obligations

⚠️ **Your Responsibilities as Controller**

As the Data Controller, you are responsible for the lawfulness of the personal data you load onto the Platform. VenueOra can only process that data on your instructions — it cannot ensure legality on your behalf.

3.1 Lawful Basis

The Customer warrants and represents that, in respect of all Personal Data it provides to VenueOra for processing via the Platform:

- it has a valid lawful basis under UK GDPR Article 6 for each processing activity;
- where Special Category Data is involved, it has identified and documented a condition under UK GDPR Article 9 that permits that processing;
- it has provided Data Subjects with all required privacy notices and information; and
- it has obtained any consents required by Applicable Data Protection Law.

3.2 Instructions

The Customer's instructions to VenueOra regarding the processing of Personal Data shall be set out in this Agreement and the Principal Agreement. The Customer may issue additional written instructions from time to time, provided those instructions are consistent with Applicable Data Protection Law. VenueOra shall be entitled to charge for any additional work required to comply with instructions outside the scope of the standard Platform functionality.

If the Customer's instructions would, in VenueOra's reasonable opinion, require VenueOra to process Personal Data in a manner that infringes Applicable Data Protection Law, VenueOra shall promptly notify the Customer and shall not be obliged to comply with such instructions until they are amended.

3.3 Own Compliance

The Customer is responsible for:

- maintaining and publishing its own privacy policy to its members and end-users, setting out the processing it undertakes as a Controller — VenueOra provides tools to assist with this but the content is the Customer's responsibility;
- ensuring that its configuration of the Platform (including any special category data features such as biometric check-in, health data collection, or sexual orientation fields) complies with the Applicable Data Protection Law, including any requirement to conduct a Data Protection Impact Assessment (DPIA) prior to use;
- managing its own data subject rights requests in respect of Personal Data it controls, with VenueOra's assistance as described in Clause 6; and
- registering with the ICO as a Data Controller where required to do so.

3.4 Accuracy

The Customer is responsible for the accuracy, integrity, and quality of the Personal Data it submits to the Platform. VenueOra processes data as provided and is not responsible for errors or inaccuracies in data supplied by or on behalf of the Customer.

4 Processor Obligations

4.1 Processing on Instructions Only

VenueOra shall only process Personal Data on the documented instructions of the Controller, as set out in this Agreement and the Principal Agreement, unless required to do so by Applicable Data Protection Law. Where VenueOra is required by law to process Personal Data beyond the Customer's instructions, VenueOra shall inform the Customer of that legal requirement before processing (unless prohibited from doing so by law).

4.2 Confidentiality

VenueOra shall ensure that all persons authorised to process Personal Data on its behalf are subject to appropriate obligations of confidentiality (whether contractual or statutory) and are trained on their data protection obligations. VenueOra shall ensure that access to Personal Data is restricted to those who need it to perform their functions.

4.3 Security

VenueOra shall implement and maintain appropriate Technical and Organisational Measures to ensure a level of security appropriate to the risk of the processing, having regard to:

- the state of the art and the costs of implementation;
- the nature, scope, context, and purposes of processing; and
- the risk to the rights and freedoms of Data Subjects, in particular the risks from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

The Technical and Organisational Measures currently in place are described in Schedule 3. VenueOra may update these measures from time to time provided the overall level of protection is not materially reduced.

4.4 Purpose Limitation

VenueOra shall not process Personal Data for any purpose other than:

- providing the Platform and its contracted features to the Customer;
- complying with Applicable Data Protection Law or any other applicable legal obligation; or
- any other purpose expressly authorised in writing by the Customer.

VenueOra shall not process Personal Data for its own commercial purposes, shall not sell Personal Data to any third party, and shall not use Personal Data to build profiles or datasets for any purpose other than provision of the Platform.

4.5 Assistance with Compliance Obligations

Taking into account the nature of the processing and the information available to it, VenueOra shall provide reasonable assistance to the Customer to enable the Customer to comply with its obligations under Applicable Data Protection Law, including in relation to:

- data security (UK GDPR Article 32);
- notification of personal data breaches (UK GDPR Articles 33–34);
- data protection impact assessments (UK GDPR Article 35);
- prior consultation with the ICO (UK GDPR Article 36); and
- data subject rights requests (Clause 6 of this Agreement).

VenueOra may charge a reasonable fee for assistance that goes beyond routine Platform functionality, provided it notifies the Customer in advance.

5 Sub-Processors

5.1 General Authorisation

The Customer grants VenueOra general written authorisation to engage the Sub-Processors listed in Schedule 2 for the purposes described therein. VenueOra shall not engage any additional Sub-Processor to process Personal Data without giving the Customer prior written notice as described in Clause 5.2.

5.2 New and Replacement Sub-Processors

If VenueOra intends to engage a new Sub-Processor or replace an existing one, it shall give the Customer at least **30 days' written notice** (via dashboard notification and email) before the change takes effect, identifying the new Sub-Processor and the nature of the processing they will carry out.

If the Customer has a reasonable objection to the use of the new Sub-Processor based on data protection grounds, it shall notify VenueOra in writing within 14 days of receipt of the notice. VenueOra will use reasonable endeavours to address the objection. If the parties cannot resolve the objection within a further 30 days, either party may terminate the relevant affected services on 30 days' written notice.

5.3 Sub-Processor Obligations

VenueOra shall impose, by written contract, data protection obligations on each Sub-Processor that are no less protective than those imposed on VenueOra by this Agreement, including in respect of:

- processing only on VenueOra's instructions;
- implementing appropriate Technical and Organisational Measures;
- confidentiality obligations;
- restrictions on further sub-processing; and
- cooperation with audit rights.

5.4 VenueOra's Liability for Sub-Processors

VenueOra remains fully liable to the Customer for the performance of any Sub-Processor's data protection obligations to the extent that the Sub-Processor fails to fulfil them.

6 Data Subject Rights

6.1 Responsibility

As the Data Controller, the Customer is primarily responsible for responding to any requests from Data Subjects exercising their rights under Applicable Data Protection Law (including requests to access, rectify, erase, restrict, or port Personal Data, or to object to processing). VenueOra is responsible for facilitating these requests at the Platform level.

6.2 VenueOra's Assistance

If VenueOra receives a request directly from a Data Subject in relation to Personal Data processed on the Customer's behalf, VenueOra shall:

- promptly (and in any event within **5 working days**) forward the request to the Customer; and
- not respond to the Data Subject directly except to confirm receipt and direct them to the Customer, unless the Customer has expressly authorised VenueOra to respond.

6.3 Platform Tools

The Platform provides the following tools to assist the Customer in discharging its data subject rights obligations:

- **Member profile management:** Customers can view, edit, and delete individual member records via the dashboard;
- **Data export:** Personal data may be exported in structured, machine-readable format (CSV) from the dashboard;
- **Account deletion:** Member accounts can be fully deleted from the dashboard, subject to any data that VenueOra is required to retain by law; and
- **Communication preferences:** Customers can manage members' marketing consent records.

The Customer should use these tools as its first point of action when responding to data subject rights requests. For requests that require action beyond the Platform's standard tools, the Customer may contact VenueOra's support team for assistance.

6.4 Timescales

VenueOra shall provide assistance requested under this Clause within a timeframe that enables the Customer to respond to the Data Subject's request within the applicable statutory period (ordinarily one calendar month under UK GDPR Article 12(3)).

7 Personal Data Breaches

7.1 VenueOra's Notification Obligation

VenueOra shall notify the Customer **without undue delay**, and in any event within **24 hours** of becoming aware of a Personal Data Breach affecting Personal Data processed on the Customer's behalf, to allow the Customer to discharge its own notification obligations to the ICO (within 72 hours) and to affected Data Subjects where applicable.

7.2 Content of Notification

VenueOra's notification shall, to the extent known at the time, include:

- a description of the nature of the breach, including the categories and approximate number of Data Subjects and Personal Data records affected;
- the likely consequences of the breach;
- the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects; and
- a named contact point for further information.

If VenueOra is unable to provide all of this information in its initial notification, it shall provide the information in phases as it becomes available, without further undue delay.

7.3 Customer's Obligations

The Customer is responsible for making its own assessment as to whether the breach requires notification to the ICO or to affected Data Subjects, and for making such notifications within the applicable statutory timeframes. VenueOra's notification under Clause 7.1 does not constitute an admission of fault or liability.

7.4 Cooperation

VenueOra shall co-operate fully with the Customer in the investigation and remediation of any Personal Data Breach and shall take reasonable steps to contain, mitigate, and remedy the breach without undue delay.

8 International Transfers

8.1 Primary Data Location

VenueOra stores Personal Data primarily within the United Kingdom and the European Economic Area. VenueOra will not transfer Personal Data outside the UK/EEA without ensuring that an appropriate transfer mechanism is in place as required by UK GDPR Chapter V.

8.2 Transfer Mechanisms

Where VenueOra transfers Personal Data to a Sub-Processor located outside the UK/EEA, it shall ensure that one of the following safeguards is in place:

- the country of destination has been the subject of an adequacy decision by the UK Secretary of State;
- a UK International Data Transfer Agreement (IDTA) or equivalent Standard Contractual Clauses (SCCs) have been entered into with the recipient; or
- another appropriate safeguard permitted by UK GDPR Article 46 is in place.

The specific transfer mechanisms in place for each Sub-Processor are identified in Schedule 2.

8.3 Customer Transfers

Where the Customer itself transfers Personal Data to VenueOra from outside the UK for processing on the Platform, the Customer is responsible for ensuring that such transfer is lawful and that any applicable transfer mechanisms are in place between the Customer (as exporter) and VenueOra (as importer).

9 Audit & Cooperation

9.1 Records of Processing

VenueOra shall maintain, in writing, all records of processing activities carried out on behalf of the Customer as required by UK GDPR Article 30(2), including the categories of processing, Sub-Processors engaged, and transfer mechanisms in use. These records are available to the ICO on request.

9.2 Audit Rights

VenueOra shall make available to the Customer all information reasonably necessary to demonstrate its compliance with this Agreement and UK GDPR Article 28, and shall allow for and contribute to audits and inspections conducted by the Customer or an auditor appointed by the Customer, provided that:

- the Customer gives VenueOra at least **30 days' written notice** of any such audit, except in the case of a genuine regulatory emergency;
- audits are conducted no more than once per calendar year (absent reasonable cause to suspect a breach);
- audits are conducted during normal business hours and in a manner that minimises disruption to VenueOra's operations;
- the auditing party signs a confidentiality agreement acceptable to VenueOra before accessing VenueOra's systems or records; and
- the Customer bears the reasonable costs of any on-site audit.

9.3 Third-Party Certifications

VenueOra may satisfy the Customer's audit requirements by providing copies of relevant third-party audit reports, certifications (including PCI DSS compliance attestations), or summaries of security assessments, to the extent these cover the relevant compliance requirements. The Customer agrees to accept such materials as a reasonable substitute for an on-site audit where they adequately address the Customer's specific compliance concerns.

9.4 Regulatory Cooperation

Each party shall cooperate with any investigation, audit, or inquiry conducted by the ICO or any other competent Supervisory Authority in relation to the processing activities covered by this Agreement. VenueOra shall promptly notify the Customer of any such investigation to the extent it relates to the Customer's Personal Data, unless prohibited from doing so by law.

10 Special Category Data

⚠️ **Heightened Obligations Apply**

The VenueOra Platform includes features that may involve Special Category Data. The Customer must ensure it has a valid Article 9 condition and, where required, has conducted a Data Protection Impact Assessment (DPIA) before enabling these features.

10.1 Processing of Special Category Data

Certain optional features of the Platform may involve the processing of Special Category Data on behalf of the Customer, including:

- **Sexual orientation and relationship status:** where the Customer enables integration with social platforms or operates venues that collect this information during member onboarding (e.g. event types, community affiliation);
- **Health and dietary data:** where the Customer collects dietary requirements or health information in connection with events or membership; and
- **Biometric data:** where the Customer enables facial recognition functionality for member check-in via kiosk or event access.

10.2 Customer Responsibility

The Customer is solely responsible for ensuring that any processing of Special Category Data via the Platform is lawful. Before enabling any Platform feature that processes Special Category Data, the Customer must:

- identify a valid condition under UK GDPR Article 9 (and, where applicable, Part 2 of Schedule 1 to the Data Protection Act 2018);
- where relying on explicit consent, obtain that consent independently of VenueOra in a manner that satisfies the UK GDPR standard (freely given, specific, informed, unambiguous, and capable of withdrawal without detriment);
- conduct a Data Protection Impact Assessment (DPIA) where required by UK GDPR Article 35, including in all cases where biometric data is to be processed; and
- maintain records of the above as part of its own data protection documentation.

10.3 VenueOra's Role

VenueOra processes Special Category Data strictly on the Customer's documented instructions and only to the extent necessary to deliver the requested Platform feature. VenueOra does not use Special Category Data for any purpose of its own. VenueOra applies additional technical controls to Special Category Data, including access restrictions and enhanced security measures.

10.4 Biometric Data

The biometric check-in feature (where enabled) captures facial imagery solely for the purpose of matching an individual to their member record for the purpose of venue access or event check-in. Biometric templates are not retained beyond the event or session for which they were captured, and are deleted within 30 days of the event unless retained for a specific security or legal purpose with appropriate legal basis. The Customer is responsible for obtaining and evidencing explicit, specific consent from each individual prior to collection of biometric data, and for ensuring that an alternative, non-biometric access method is always available.

11 Return & Deletion of Personal Data

11.1 During the Term

During the term of this Agreement, the Customer may export its Personal Data at any time using the Platform's export functionality. VenueOra provides data export in structured, machine-readable format (CSV) to support data portability.

11.2 On Termination

Within **30 days** of the termination or expiry of the Principal Agreement, VenueOra will, at the Customer's written election:

- **Return:** provide the Customer with an export of all Personal Data in its possession that was processed on the Customer's behalf, in a structured, commonly used, and machine-readable format; and/or
- **Delete:** securely delete or anonymise all Personal Data processed on the Customer's behalf, including any copies held in backup systems, within a reasonable further period not to exceed 60 days.

If the Customer does not make a written election within 30 days of termination, VenueOra shall proceed with deletion by default.

11.3 Retention Exceptions

VenueOra may retain Personal Data beyond the periods set out in Clause 11.2 to the extent that it is required to do so by Applicable Data Protection Law or any other applicable law (including financial record-keeping and anti-money laundering obligations). Where data is retained under this exception, VenueOra shall isolate that data from active processing, restrict access to it, and delete it as soon as the legal retention obligation no longer applies. VenueOra shall inform the Customer of any such retention requirement and the specific data categories affected.

11.4 Confirmation

VenueOra shall provide the Customer with written confirmation of the completion of any deletion or export carried out under this Clause.

12 Liability

12.1 Controller Liability to Data Subjects

As the Data Controller, the Customer accepts that it is primarily liable to Data Subjects for any damage caused by processing that infringes Applicable Data Protection Law. VenueOra, as Processor, shall only be liable to a Data Subject where it has not complied with obligations under Applicable Data Protection Law specifically directed to Processors, or where it has acted outside or contrary to the Customer's lawful instructions.

12.2 Indemnity

Each party shall indemnify and hold harmless the other party in respect of any fines, penalties, awards, damages, or costs awarded against the other party by a court or the ICO that arise solely and directly from the indemnifying party's breach of its obligations under this Agreement or Applicable Data Protection Law, subject to the limitations set out in the Principal Agreement.

12.3 Liability Cap

The total aggregate liability of each party to the other under or in connection with this Agreement shall not exceed the liability cap set out in the Principal Agreement. Nothing in this Agreement excludes or limits either party's liability for:

- death or personal injury caused by negligence;
- fraud or fraudulent misrepresentation; or
- any other matter that cannot be excluded or limited by applicable law.

12.4 Regulatory Fines

Where a fine or penalty is imposed by the ICO or any other regulatory authority on either party as a result of a breach of this Agreement, each party shall bear the fine or penalty imposed on it directly. Where a fine is imposed jointly, the parties shall apportion responsibility for that fine in proportion to their respective culpability for the underlying breach, failing agreement, as determined by a court of competent jurisdiction.

13 General Provisions

13.1 Governing Law & Jurisdiction

This Agreement and any non-contractual obligations arising out of or in connection with it shall be governed by and construed in accordance with the law of England and Wales. The parties irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement.

13.2 Precedence

In the event of any conflict between this Agreement and the Principal Agreement concerning the processing of Personal Data, this Agreement shall prevail to the extent of the conflict. In all other respects, the Principal Agreement shall govern.

13.3 Amendments

VenueOra may amend this Agreement to reflect changes in Applicable Data Protection Law, guidance from the ICO, or changes to the Platform's processing activities. VenueOra shall provide at least **30 days' notice** of any material amendment via the Platform dashboard and by email. Continued use of the Platform after the notice period constitutes acceptance of the amended Agreement. Where an amendment materially increases the Customer's data protection obligations, the Customer may terminate the Principal Agreement on 30 days' written notice.

13.4 Entire Agreement

This Agreement, together with the Principal Agreement and all incorporated Schedules, constitutes the entire agreement between the parties in relation to the subject matter hereof and supersedes all prior agreements, understandings, representations, and warranties relating to data processing between VenueOra and the Customer.

13.5 Severability

If any provision of this Agreement is held to be invalid, unenforceable, or illegal, the remaining provisions shall continue in full force and effect.

13.6 No Waiver

Failure by either party to enforce any provision of this Agreement shall not constitute a waiver of that party's right to enforce that provision or any other provision in the future.

SCHEDULE 1

Details of Processing (UK GDPR Article 28(3))

S1.1 Subject Matter

The provision of the VenueOra SaaS platform for ticketing, event management, membership management, locker management, kiosk access, and related operational features, together with integrated payment facilitation, communications, and analytics tools.

S1.2 Duration

For the duration of the Principal Agreement, plus any post-termination retention period required by Applicable Data Protection Law (see Clause 11.3).

S1.3 Nature and Purpose of Processing

Feature / Module	Nature of Processing	Purpose
Membership Management	Storage, retrieval, update, deletion	Member profile management, subscription administration, policy signing
Ticketing & Events	Collection, storage, retrieval, transmission	Ticket sales, booking management, QR check-in, digital wallet passes
Payment Processing (KYC)	Collection, transmission to Payment Processor	Merchant onboarding, identity verification, payment facilitation
Communications	Storage, retrieval, transmission	Email campaigns, member messaging, push notifications, Telegram groups
Kiosk & Check-in	Capture, matching, deletion	Member check-in, self-service ordering, venue access
Locker Management	Storage, retrieval	Locker assignment, access management, audit logging
Website / Member Portal	Storage, retrieval, display	Member-facing portal content delivery and personalisation
Affiliate Programme	Storage, calculation, transmission	Referral attribution, commission calculation, KYC for payout
Analytics & Reporting	Aggregation, analysis	Business intelligence dashboards for the Customer

S1.4 Types of Personal Data Processed

Category	Data Types
Identity & Contact	Full name, date of birth, email address, phone number, postal address
Account & Access	Username, hashed password, login timestamps, session data
Membership & Booking	Membership number, subscription status, event booking history, ticket details, QR codes
Payment & Financial	Payment confirmation references, tokenised card identifiers, transaction history, payout records (no raw card data)
KYC / Identity Verification	Government-issued identity documents, director/shareholder details, company registration details, bank account details
Communications	Email content, campaign engagement data, push notification tokens, Telegram user identifiers
Technical & Behavioural	IP address, browser and device identifiers, session logs, access logs
Special Category Data (where enabled)	Sexual orientation / relationship status; health and dietary information; biometric facial imagery (check-in only)

S1.5 Categories of Data Subjects

- The Customer's members and club/venue attendees;
- ticket purchasers and event attendees;
- the Customer's staff users and administrators;
- KYC applicants (business owners, directors, shareholders);
- affiliates and referral partners; and
- any other individuals whose Personal Data the Customer loads onto the Platform.

SCHEDULE 2

Approved Sub-Processors

The following Sub-Processors are authorised under Clause 5.1 of this Agreement. VenueOra will provide at least 30 days' notice before adding or replacing a Sub-Processor. Last updated: March 2026.

Sub-Processor	Purpose	Data Processed	Location	Safeguard
Amazon Web Services (AWS)	Cloud infrastructure, hosting, and file storage	All Platform data at rest and in transit	UK / Ireland (EEA)	UK Adequacy / AWS DPA / ISO 27001
Payment Processor (FCA-authorised)	Payment facilitation, merchant KYC, settlement, payouts	KYC identity data, bank details, transaction data	United Kingdom	FCA-regulated; PCI DSS Level 1; contractual DPA
Mailgun Technologies	Transactional and campaign email delivery	Email addresses, email content, engagement data	USA	IDTA / SCCs; Mailgun DPA
Google (Firebase / reCAPTCHA)	Push notifications (FCM), bot detection (reCAPTCHA), analytics	Device tokens, IP addresses, browser fingerprints	USA / EEA	Google Workspace DPA; SCCs
Sentry	Application error and performance monitoring	Error logs; may include truncated data from affected requests	USA	IDTA / SCCs; Sentry DPA; data scrubbing configured
Intercom	Customer support and in-app messaging (Customer-facing)	Customer name, email, account activity, support messages	USA	IDTA / SCCs; Intercom DPA
Slack Technologies	Internal VenueOra team operational alerts	Limited: Customer name and email in automated notifications	USA	SCCs; Slack DPA; restricted to VenueOra staff
TxtSync	SMS delivery for operational notifications	Mobile phone numbers; SMS message content	United Kingdom	UK-based; contractual DPA
Telegram	Member group communication (where enabled by Customer)	Telegram user IDs, usernames; message content	USA / EEA	SCCs; feature-specific; Customer-initiated
SwingHub	Social platform OAuth integration (where enabled)	User identifiers, email, username for account linking only	United Kingdom	Contractual DPA; data used for feature delivery only

Sub-Processor	Purpose	Data Processed	Location	Safeguard
Companies House (GOV.UK)	Business verification API during KYC	Company number submitted; public company data returned	United Kingdom	UK public authority; GDPR Art. 6(1)(c)

SCHEDULE 3

Technical and Organisational Security Measures

This Schedule describes VenueOra's Technical and Organisational Measures (TOMs) as required by UK GDPR Article 32. These measures are subject to regular review and are updated in response to evolving threats and industry best practice.

S3.1 Access Control & Authentication

- User access to the Platform is controlled through secure, authenticated accounts with automatic session expiry after inactivity;
- passwords are never stored in recoverable form — only a secure, irreversible representation is retained;
- multi-factor authentication is available for administrative accounts;
- VenueOra staff access to production data is controlled through role-based access controls, with access limited to what is necessary for each role; and
- VenueOra's highest-privilege system functions are accessible only through secured, network-restricted channels.

S3.2 Encryption & Data Protection in Transit and at Rest

- all data transmitted between users and the Platform is encrypted in transit using industry-standard encryption protocols;
- sensitive documents and files, including KYC identity materials, are stored in encrypted form; and
- access to sensitive stored files is controlled through expiring, purpose-specific access tokens rather than permanent URLs.

S3.3 Network & Infrastructure Security

- the Platform is hosted on enterprise-grade cloud infrastructure with physical and environmental security controls;
- network-level controls including firewalls and monitoring are in place to protect against unauthorised access;
- system and application activity is logged and monitored for anomalous behaviour; and
- regular security assessments and vulnerability reviews are conducted.

S3.4 Data Minimisation & Isolation

- each Customer's data is logically isolated from other Customers' data at the application level;
- VenueOra applies a principle of data minimisation — only data necessary for the provision of the Platform is collected and retained; and
- Special Category Data is subject to additional access restrictions.

S3.5 Availability & Resilience

- the Platform infrastructure is designed for high availability with automated failover capabilities;
- regular data backups are maintained and tested; and
- incident response procedures are in place to manage and recover from disruptions to services.

S3.6 Organisational Measures

- all VenueOra staff are subject to confidentiality obligations and receive appropriate data protection training;
- data protection responsibilities are clearly assigned within the organisation;
- a documented incident response and personal data breach notification procedure is in place; and
- VenueOra conducts Data Protection Impact Assessments where required before introducing new or significantly changed processing activities.

S3.7 Payment Data

VenueOra does not store, process, or transmit raw payment card data. All card transactions are handled directly by VenueOra's PCI DSS Level 1-certified Payment Processor. VenueOra retains only payment confirmation references and tokenised identifiers necessary for reconciliation purposes.

Execution

Electronic Acceptance

By accepting the VenueOra Terms of Service and continuing to use the Platform, the Customer is deemed to have accepted this Data Processing Agreement in its entirety. For enterprise customers or where a wet-ink or separately executed version is required, please contact legal@venueora.com to request a countersigned copy.