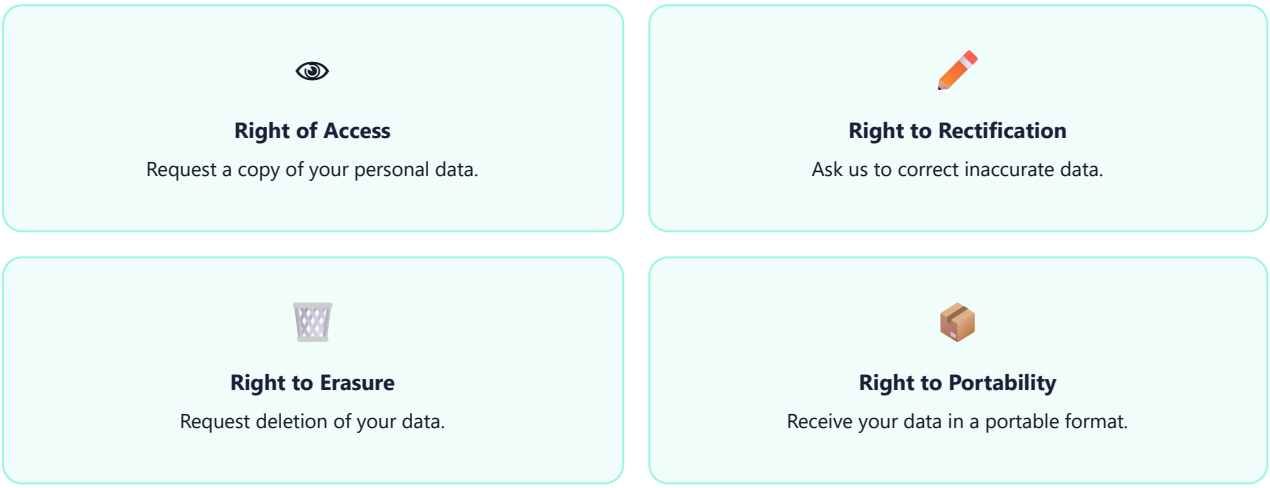
UK GDPR & DATA PROTECTION ACT 2018

Privacy Policy

This Privacy Policy explains how VenueOra collects, uses, stores, and protects personal data in connection with the VenueOra Platform. It applies to our business customers, their staff, end-users of the Platform, and visitors to our services.

GOVERNING FRAMEWORK	DATA CONTROLLER	DATA PROCESSOR ROLE	GOVERNING LAW
UK GDPR & DPA 2018	VenueOra Ticketing Limited	For venue member & ticket data	England & Wales



Important — Two Types of Data Processing: VenueOra operates both as a **data controller** (for data relating to our business customers and their staff) and as a **data processor** (for personal data about members, ticket purchasers, and end-users that our business customers enter into the Platform). If you are an end-user of a venue or event operated by one of VenueOra's customers, you should also refer to that venue's own privacy policy.

1 Who We Are

1.1 Data Controller Identity

VenueOra Ticketing Limited is a company registered in England and Wales. We operate the VenueOra Platform, accessible at venueora.com (https://venueora.com) and associated domains, which provides membership management, events and ticketing, and payment processing services to business customers ("Customers") across the United Kingdom.

For the purposes of UK data protection law, VenueOra Ticketing Limited is the data controller in respect of personal data we collect and process for our own purposes (as described in this Policy). Our contact details are set out in Section 16.

1.2 ICO Registration

VenueOra Ticketing Limited is registered with the Information Commissioner's Office (ICO) as required under the Data Protection Act 2018. You can verify our registration at ico.org.uk (https://ico.org.uk).

2 Scope & Our Dual Role

2.1 What This Policy Covers

This Privacy Policy applies to personal data processed by VenueOra in connection with:

- the registration and use of the VenueOra Platform by business Customers and their staff;
- KYC (Know Your Customer) verification for payment processing onboarding;
- the VenueOra Affiliate & Referral Programme;
- customer support, communications, and billing; and
- personal data about end-users (members, ticket purchasers, attendees) processed by VenueOra on behalf of its Customers as a data processor.

2.2 VenueOra as Data Controller

VenueOra acts as a **data controller** in respect of:

- personal data collected from and about our business Customers and their authorised staff users during registration, onboarding, account management, and billing;
- KYC application data submitted for payment processing setup;
- affiliate and referral data; and
- data collected for our own operational, security, and analytical purposes.

2.3 VenueOra as Data Processor

VenueOra acts as a **data processor** in respect of personal data relating to:

- venue members managed within the Platform by our Customers;
- event attendees and ticket purchasers;
- mailing list subscribers and contact records created by our Customers; and
- any other personal data that our Customers input into the Platform for their own business purposes.

In these circumstances, our Customer is the data controller and VenueOra processes the data solely on their documented instructions under our Data Processing Agreement (incorporated into the Platform Terms of Service). If you are a member, ticket purchaser, or end-user of a venue or event run by an VenueOra Customer, please contact that venue directly to understand how they process your data, and refer to their privacy policy.

2.4 The Platform's White-Label Nature

The VenueOra Platform may be presented to end-users under a venue's own branding and domain. In such cases, VenueOra operates as an invisible infrastructure provider. The venue remains the data controller for its end-users, and VenueOra processes data solely to deliver the Platform's services to that venue.

3 Personal Data We Collect

3.1 Business Customers & Staff

When a business registers for and uses the VenueOra Platform, we collect:

- **Account data:** business name, trading name, registered address, email address, telephone number, website URL, and nature of business activities;
- **Onboarding preferences:** event types operated, existing platforms used, desired features, and onboarding notes;
- **Staff user data:** name, email address, password (stored as a bcrypt hash — we never see your plaintext password), role, and last login timestamp;
- **Login session data:** IP address, browser user agent, login and logout timestamps, and session duration, retained for security audit purposes;
- **Billing data:** Platform Fee payment history and invoice records; and
- **Communications:** email correspondence, support requests, and in-platform messages.

3.2 KYC Data (Payment Onboarding)

To enable live payment processing, Customers must complete our KYC process. During this process we collect (on behalf of ourselves and our FCA-authorised Payment Processor):

- **Personal representative data:** full legal name, date of birth, nationality, email address, and phone number;
- **Business data:** company name, company registration number, incorporation date, registered and trading addresses;
- **Beneficial owner and director data:** name, date of birth, country of birth, gender, nationality, address, ownership percentage, and business roles for each beneficial owner or director;
- **Bank account data:** UK bank account name, account number, and sort code for payout settlement;
- **Identity documents:** scanned copies of passports, driving licences, and proof of address documents; and
- **Business documents:** certificate of incorporation and other regulatory documents.

KYC data is processed to satisfy legal obligations under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and is shared with our FCA-authorised Payment Processor as required for merchant onboarding.

3.3 Members (Processed on Behalf of Customers)

When our Customers manage members through the Platform, the following data categories may be entered and processed by VenueOra as data processor:

- Name, date of birth, email address(es), phone number(s), and postal address(es);
- Partner/couple details (where applicable to the membership type), including partner name, date of birth, and contact details;
- Membership number, type, status, and subscription history;
- Profile photographs and member-uploaded files;
- Member activity logs (e.g. check-ins, email engagement, payments, policy signatures);
- Custom fields defined by the venue operator;
- Social platform identifiers (SwingHub username/ID, Telegram username/chat ID) where linked by the member;
- Policy acceptance records and signed document timestamps; and
- Payment transaction history.

Special category data relating to members is described in Section 5.

3.4 Ticket Purchasers & Event Attendees

When End Customers purchase tickets or register for events through the Platform, the following data may be collected (depending on the event's requirements as configured by the venue):

- Name, email address, phone number, and postal address;
- Date of birth and gender (for age-restricted or gender-restricted events);
- Dietary requirements and accessibility requirements;
- Emergency contact name and phone number;
- Special requirements or notes; and
- Ticket and order details, including payment confirmation references.

Payment card data is processed directly by our Payment Processor via its client-side SDK and is never stored on VenueOra's servers.

3.5 Public Website Users & Mailing List

Where VenueOra Customers operate branded member portals or event ticketing pages built on the Platform, visitors and registrants may provide:

- Name, email address, and phone number at the point of registration or ticket purchase;
- Mailing list subscription requests, including double opt-in confirmation status; and
- Communications preferences.

3.6 Affiliates

Participants in the VenueOra Affiliate & Referral Programme are existing VenueOra Customers. In addition to the data described in Clause 3.1 and 3.2, we record affiliate-specific data including referral codes, commission balances, transaction history, withdrawal references, and payout records. Please refer to the Affiliate & Referral Programme Terms for further detail.

3.7 Data Collected Automatically

When you use the Platform or our websites, we may automatically collect:

- **Log data:** IP addresses, HTTP request and response data, timestamps, and error logs;
- **Device and browser data:** browser type, operating system, screen resolution, and device identifiers; and
- **Usage data:** pages visited, features used, session duration, and navigation patterns.

3.8 Data We Do Not Collect

VenueOra does not collect, store, or process raw payment card numbers (PAN), CVV/CVC codes, or PIN data at any point. All card payment data is processed exclusively by our PCI DSS Level 1-certified Payment Processor via its client-side SDK, which operates outside VenueOra's data environment.

4 Legal Basis for Processing

Under UK GDPR Article 6, we rely on the following legal bases:

PROCESSING ACTIVITY	LEGAL BASIS	ARTICLE 6 GROUND
Creating and managing your Platform account	Contractual Necessity	Art. 6(1)(b)
KYC identity and business verification	Legal Obligation	Art. 6(1)(c)
Payment processing and transaction records	Contractual Necessity	Art. 6(1)(b)
Invoicing and financial records	Legal Obligation	Art. 6(1)(c)
Fraud prevention and security monitoring	Legitimate Interests	Art. 6(1)(f)
Platform security and access logging	Legitimate Interests	Art. 6(1)(f)
Customer support and communications	Contractual Necessity	Art. 6(1)(b)
Transactional and service emails	Contractual Necessity	Art. 6(1)(b)
Marketing and promotional emails	Consent	Art. 6(1)(a)
Platform analytics and improvement	Legitimate Interests	Art. 6(1)(f)
Affiliate commission tracking and payouts	Contractual Necessity	Art. 6(1)(b)
Processing member and ticket data (as Processor)	Customer's instructions as Controller	Art. 28
AML / CTF compliance and sanctions screening	Legal Obligation	Art. 6(1)(c)
Responding to legal process or regulatory requests	Legal Obligation	Art. 6(1)(c)

4.1 Legitimate Interests Assessment

Where we rely on legitimate interests as our legal basis, we have determined that our interests are not overridden by your rights and freedoms, taking into account the nature of the data, the reasonable expectations of the individuals concerned, and the safeguards we have in place. You have the right to object to processing carried out on this basis (see Section 13).

5 Special Category & Sensitive Data

The VenueOra Platform processes several categories of special category personal data under UK GDPR Article 9. These categories require a higher standard of protection and a specific additional legal basis beyond Article 6. The categories below apply primarily to data processed by VenueOra as a data processor on behalf of venue Customers.

5.1 Sexual Orientation & Relationship Status

Where the Platform is used by adult social clubs, lifestyle venues, or similar operators, the Platform may process data that reveals or implies sexual orientation or relationship structure — including membership profile types (e.g. couple, same-sex couple), event gender or couples-only restrictions, and social platform profile data linked via the SwingHub integration.

Legal basis (Art. 9(2)(a)): Explicit consent provided by the data subject to the venue operator as data controller. Venue operators are responsible for obtaining, recording, and managing this consent from their members and must ensure that their own privacy policies and membership agreements reflect this processing.

5.2 Health & Dietary Data

The Platform allows event organisers to collect dietary requirements, accessibility requirements, and special needs information from ticket purchasers and event attendees. This may constitute data concerning health under Article 9(1).

Legal basis (Art. 9(2)(a)): Explicit consent at the point of collection, obtained by the venue/event organiser as data controller. VenueOra processes this data solely to deliver the Platform's ticketing and check-in services.

5.3 Biometric Data & Facial Recognition

The Platform includes a kiosk check-in feature that may use facial image capture and facial recognition technology to verify attendee identity at the point of entry. Where this feature is used, facial images and facial recognition results constitute **biometric data** for the purposes of Article 9(1).

Legal basis (Art. 9(2)(a)): Explicit, freely given, specific, informed, and unambiguous consent must be obtained by the venue operator from each individual whose biometric data is processed, before that processing takes place. Biometric data must not be collected from individuals who have not explicitly consented. VenueOra processes biometric data solely on the venue operator's instruction and does not use it for any VenueOra purpose.

> **Important Note for Venue Operators:** If you enable the facial recognition check-in feature, you are required by law to: (a) conduct a Data Protection Impact Assessment (DPIA) before deployment; (b) obtain explicit, written consent from each individual subject to facial recognition; (c) provide a clear alternative check-in method for those who decline consent; and (d) update your privacy policy to disclose biometric data processing. Please contact dpo@venueora.com for guidance.

5.4 KYC Beneficial Owner Data

KYC applications for limited companies require the submission of personal data (including date of birth, gender, nationality, and identity documents) relating to directors and beneficial owners. This data is processed under our legal obligation to comply with anti-money laundering regulations (Art. 9(2)(g) — substantial public interest, prevention of unlawful acts) and is shared with our Payment Processor for regulatory compliance purposes.

6 How We Use Your Data

6.1 Providing the Platform

We use your personal data to provide, operate, maintain, and improve the VenueOra Platform, including account management, payment processing, event and membership management tools, communications features, and all other core Platform functions.

6.2 KYC & Payment Compliance

We use KYC data to verify the identity and legitimacy of our business Customers, to create and manage Merchant Payment Accounts with our Payment Processor, and to meet our obligations under UK anti-money laundering law. We do not use KYC data for any other purpose.

6.3 Communications

We use contact information to send:

- **Transactional emails** — account confirmations, KYC status updates, payment receipts, payout notifications, and system alerts (legal basis: contractual necessity);
- **Service communications** — policy updates, terms changes, maintenance notices, and important platform notifications (legal basis: contractual necessity / legitimate interests); and
- **Marketing communications** — only where you have provided explicit consent or where permitted by the Privacy and Electronic Communications Regulations 2003. You may withdraw consent or opt out at any time.

6.4 Security & Fraud Prevention

We use login session data, IP addresses, and usage data to detect and prevent fraud, unauthorised access, and misuse of the Platform. This includes monitoring for suspicious transaction patterns, unusual login behaviour, and potential security threats.

6.5 Affiliate Programme

We use referral codes, commission transaction records, and payout data to operate the VenueOra Affiliate & Referral Programme, calculate commissions, process payouts, and maintain programme records.

6.6 Legal Compliance

We may use and retain personal data where required to comply with a legal obligation, including financial record-keeping requirements, anti-money laundering obligations, and responses to lawful requests from courts, regulators, or law enforcement authorities.

6.7 What We Will Never Do

- We will never sell your personal data to any third party.
- We will never share Customer Data with third parties for their own marketing or commercial purposes.
- We will never use member or end-user data (processed on behalf of Customers) for VenueOra's own purposes.
- Where data is shared with integration partners to enrich their systems, end-user personal data is transmitted only to enable the specific feature and is not retained by or permanently transferred to the integration partner.

7 Who We Share Data With

VenueOra only shares personal data with third parties where it is necessary to deliver the Platform's services, to comply with legal obligations, or where you have consented. We never sell data or share it for third-party commercial purposes.

SUB-PROCESSOR / THIRD PARTY	PURPOSE	DATA SHARED	LOCATION	SAFEGUARD
Payment Processor (FCA-authorised)	Payment processing, merchant KYC, settlement, and Internal Transfers	Full KYC application data; payment transaction data; Merchant Payment Account details	United Kingdom	FCA-regulated; contractual DPA; PCI DSS L1
Amazon Web Services (AWS)	Cloud hosting (servers, databases) and file storage (S3)	All Platform data stored on VenueOra's servers; KYC documents; member images	UK / EEA (eu-west-1)	UK adequacy; AWS DPA; encryption at rest
AWS CloudFront	Content Delivery Network for media files	Signed access tokens; media request logs (may include IP)	UK / EEA	UK adequacy; AWS DPA
Mailgun Technologies	Transactional email delivery	Recipient email address; email content (name, order details, notifications)	EU / USA	Standard Contractual Clauses (SCCs)
Google Cloud (Maps API)	Address geocoding and location autocomplete	Member and business addresses submitted for geocoding	USA	SCCs; Google DPA
Google AI (Gemini)	AI-generated event descriptions and images	Event titles, descriptions, and images submitted for AI processing	USA	SCCs; Google DPA; no personal data in scope
Google Wallet	Digital event pass creation	Ticket holder name, event details, QR code data	USA	SCCs; Google DPA
Apple Wallet	Digital event pass creation (.pkpass)	Ticket holder name, event details, QR code data	USA	Apple DPA
Google Firebase (FCM)	Push notifications to mobile and staff devices	Device push tokens (FCM token); notification title and body	USA	SCCs; Google DPA

SUB-PROCESSOR / THIRD PARTY	PURPOSE	DATA SHARED	LOCATION	SAFEGUARD
Google reCAPTCHA	Bot and fraud prevention on forms	IP address; browser fingerprint data	USA	SCCs; Google DPA
Sentry	Application error monitoring and performance tracking	Error stack traces, request URLs; PII transmission is disabled by default	USA	SCCs; Sentry DPA
Intercom	Customer support chat and CRM for Platform staff users	Admin user ID, email, name, company name, and account creation date	USA	SCCs; Intercom DPA
TxtSync	SMS delivery for notifications (locker PINs, alerts)	Mobile phone numbers; SMS message content	United Kingdom	UK-based; contractual DPA
SwingHub	Social platform OAuth integration and member verification	User identifiers, emails, and usernames for account linking only	United Kingdom	Contractual DPA; data used for feature only
Telegram	Member group notifications and communications	Telegram chat IDs, usernames; message content	USA / EEA	SCCs; feature-specific
Companies House (GOV.UK)	Business verification during KYC (API query)	Company number sent; company details returned	United Kingdom	UK public authority; GDPR Art. 6(1)(c)
Slack	Internal VenueOra team alerts for new customer signups	Customer name and email address in automated notifications	USA	SCCs; Slack DPA; limited to VenueOra staff

7.1 Integration Partners

Where VenueOra enables integrations with third-party platforms (such as social networks or communication tools) to enrich those platforms with data from the VenueOra Platform, personal data is transmitted solely to enable the specific integration feature. End-user personal data is not permanently transferred to or retained by integration partners for their own purposes.

7.2 Legal Disclosures

VenueOra may disclose personal data to law enforcement agencies, courts, regulators (including the FCA and ICO), or other authorities where required or permitted to do so by applicable law, court order, or regulatory direction.

7.3 Business Transfers

In the event of a merger, acquisition, or sale of all or substantially all of VenueOra's business or assets, personal data may be transferred to the acquirer, subject to the acquirer assuming equivalent data protection obligations. We will notify affected individuals in advance where practicable.

8 International Data Transfers

8.1 UK Data Storage

VenueOra's primary data infrastructure is hosted within the United Kingdom and the European Economic Area (EEA), using reputable cloud service providers with data centres located in the UK and Ireland. The majority of personal data remains within the UK and EEA at all times.

8.2 Transfers Outside the UK/EEA

Some of our third-party sub-processors (including Google, Mailgun, Intercom, Sentry, Slack, and Telegram) process data in the United States or other countries outside the UK/EEA. Where such transfers occur, VenueOra ensures that appropriate safeguards are in place as required by UK GDPR Chapter V, including:

- **UK Adequacy Regulations** — for transfers to countries or organisations recognised as providing an adequate level of protection;
- **UK International Data Transfer Agreements (IDTAs)** or equivalent Standard Contractual Clauses (SCCs) — incorporated into our data processing agreements with sub-processors; and
- **Binding Corporate Rules (BCRs)** — where applicable for intra-group transfers.

8.3 Transfer Impact Assessments

Where required, VenueOra conducts Transfer Impact Assessments to evaluate the risks associated with international data transfers and to confirm that the rights of data subjects are not undermined by the transfer.

9 Cookies & Tracking Technologies

9.1 What Cookies We Use

The VenueOra Platform uses the following types of cookies and tracking technologies:

COOKIE / TECHNOLOGY	TYPE	PURPOSE	DURATION
Session Cookie	Strictly Necessary	Maintains your authenticated session on the Platform. Stored securely server-side and expires automatically after a period of inactivity.	Expires after inactivity
Security Token	Strictly Necessary	Protects all form submissions against cross-site request forgery and other common web-based attacks.	Session
`affiliate_referral_code`	Functional	Stores your referral code in session when you visit via a referral link, enabling proper attribution during onboarding.	Session
Google reCAPTCHA	Functional / Security	Bot detection on forms. Submits browser fingerprint and IP to Google for fraud scoring.	Persistent (Google-managed)
Intercom (`intercom-session-*`, `intercom-id-*`)	Functional	Powers the customer support chat widget for authenticated admin users. Links your session to your Intercom profile.	9 months (Intercom-managed)
Firebase Analytics (`_ga*`)	Analytics	Where Firebase Analytics is active, Google Analytics cookies may be set to collect usage data. We are reviewing consent requirements for this technology.	Up to 2 years (Google-managed)

9.2 Email Tracking

Outbound emails sent through the Platform on behalf of venue operators may include engagement tracking (open and click tracking) to enable Customers to monitor the effectiveness of their member communications. Where email tracking is enabled by a Customer, the Platform records whether an email was opened or a link was clicked, logged against the relevant member record. VenueOra's own transactional email delivery is configured with tracking disabled at the delivery provider level.

9.3 Your Cookie Choices

Strictly necessary cookies cannot be disabled as they are essential to the Platform's operation. For functional and analytics cookies, you may manage your preferences through your browser settings. Disabling certain cookies may affect the functionality of the Platform.

If you have specific concerns about cookies set by third-party services (such as Intercom or Google), please refer to those providers' own privacy and cookie policies.

10 How Long We Keep Your Data

VenueOra retains personal data only for as long as necessary for the purpose for which it was collected, or as required by applicable law. The retention periods below represent our standard policy. Where a specific legal obligation requires longer retention, we will retain data for that period.

DATA CATEGORY	RETENTION PERIOD	BASIS
Active Customer account data	Duration of subscription + 7 years	Companies Act / tax records
Staff user accounts	Duration of employment/access + 2 years	Legitimate interests (security audit)
KYC application data & identity documents	5 years following end of business relationship	AML Regulations 2017 (legal obligation)
Payment and transaction records	7 years	HMRC / financial record-keeping
Member data (as Processor)	Per Customer's instructions; deleted within 90 days of subscription termination on request	Customer's data retention policy
Ticket purchaser / attendee data	Per Customer's instructions; typically 3 years post-event	Customer's data retention policy
Login session and security logs	2 years	Legitimate interests (fraud prevention)
KYC biometric images (where used)	Duration of event / venue visit; deleted within 30 days unless required for investigation	Explicit consent (revocable)
Affiliate earnings records	7 years from date of payout or last activity	HMRC / financial record-keeping
Email marketing consent records	Until consent is withdrawn + 3 years	Legal obligation (evidence of consent)
Support and correspondence	3 years following resolution	Legitimate interests
Dormant affiliate balances	24 months from last activity; notice given before expiry	Contractual; dormancy policy

10.1 Deletion on Request

Where you exercise your right to erasure (see Section 13), VenueOra will delete or anonymise your personal data within 30 days of the request, subject to any legal obligations that require us to retain specific records. Backup systems may retain encrypted copies for up to 30 additional days before permanent deletion.

11 Security

11.1 Our Approach to Security

VenueOra takes the security of personal data seriously and applies a layered approach to protection across all areas of the Platform. We implement a combination of technical and organisational safeguards designed to prevent unauthorised access, accidental loss, alteration, or disclosure of the data we hold. The specific measures we apply are reviewed and updated regularly in response to evolving threats and industry best practice.

Our technical safeguards include, amongst others:

- **Credential protection:** passwords are never stored in a readable form — only a secure, irreversible representation is retained, so even VenueOra staff cannot access your password;
- **Encryption in transit:** all communication between your browser or application and the Platform is encrypted over secure connections;
- **Encryption at rest:** sensitive documents and files, including KYC identity materials, are stored in encrypted form on secure cloud infrastructure;
- **Time-limited access controls:** access to sensitive files and documents is granted through expiring, purpose-specific access tokens rather than permanent links;
- **Authentication controls:** access to the Platform and its APIs is protected by secure authentication mechanisms with automatic session expiry after a period of inactivity;
- **Request integrity protection:** all form submissions are protected against common web-based attack vectors; and
- **Restricted administrative access:** VenueOra's highest-privilege administrative functions are accessible only through secured, network-restricted channels.

11.2 Organisational Controls

In addition to technical measures, VenueOra maintains robust organisational controls, including:

- a principle of least privilege — staff members are granted access only to the data and systems necessary for their specific role;
- strict separation between day-to-day operations and sensitive administrative functions;
- monitoring and logging of access to sensitive data and critical system operations;
- account protection controls to guard against unauthorised access attempts; and
- ongoing staff awareness of data protection and information security obligations.

11.3 Payment Security

VenueOra does not handle raw payment card data at any point. All card transactions are processed directly by our PCI DSS Level 1-certified Payment Processor in a fully isolated environment. VenueOra retains only the information necessary to identify and reconcile a transaction — no card numbers, security codes, or sensitive authentication data are ever stored on VenueOra's systems.

11.4 Data Breach Notification

In the event of a personal data breach, VenueOra will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach where it is likely to result in a risk to individuals' rights and freedoms. Where the breach is likely to result in a high risk, we will also notify affected individuals without undue delay. VenueOra will notify affected Customers in their capacity as data controllers where the breach relates to data processed on their behalf, enabling them to meet their own notification obligations.

11.5 Your Responsibilities

While VenueOra maintains robust safeguards, the security of your account also depends on the steps you take. You are responsible for keeping your login credentials confidential, ensuring that access to the Platform is appropriately controlled within your organisation, and notifying us promptly if you suspect any unauthorised use of your account. We will never ask for your password by email or phone.

12 Children's Data

12.1 Platform Age Restrictions

The VenueOra Platform is designed for use by business customers and, through those businesses, by adult end-users. Many venues using the Platform operate adult-only environments. The Platform includes age restriction controls that venue operators may configure on individual events and sessions, including hard minimum age enforcement at the point of ticket purchase.

12.2 VenueOra's Direct Services

VenueOra's own direct services (account registration, KYC, affiliate programme) are intended solely for business customers and adults aged 18 or over. VenueOra does not knowingly collect personal data from children under the age of 18 in connection with its direct services. If we become aware that we have inadvertently collected data from a person under 18, we will delete that data promptly.

12.3 Children at Events

Some venues using the Platform may operate events that are open to children (including family leisure events such as ice skating sessions). In such circumstances, the venue operator is the data controller responsible for ensuring lawful processing of children's data, including obtaining appropriate parental consent where required. VenueOra processes children's data in these circumstances solely as a data processor on the venue's instructions.

13 Your Data Protection Rights

Under UK GDPR and the Data Protection Act 2018, you have the following rights in relation to your personal data. These rights apply where VenueOra is acting as a **data controller** in respect of your data. Where VenueOra is acting as a data processor, you should contact the relevant venue or event organiser (as data controller) to exercise your rights.

👁 Right of Access (Subject Access Request) Art. 15 UK GDPR

You have the right to request a copy of the personal data we hold about you, along with information about how and why we process it, who we share it with, how long we keep it, and your other rights in relation to it. We will respond within one calendar month of receipt of a valid request. This period may be extended by a further two months for complex or multiple requests.

🖍 Right to Rectification Art. 16 UK GDPR

You have the right to ask us to correct inaccurate personal data we hold about you, or to complete incomplete data. Many details can be updated directly through your Platform account. For data you cannot update yourself (such as KYC records), please contact us.

🗑 Right to Erasure ("Right to Be Forgotten") Art. 17 UK GDPR

You have the right to ask us to delete your personal data in certain circumstances, including where the data is no longer necessary for the purpose it was collected, where you withdraw consent, or where you object to processing based on legitimate interests. This right is not absolute — we may be required to retain certain data for legal or regulatory reasons (e.g. AML records must be retained for 5 years). We will inform you of any such limitation when responding to your request.

⏸ Right to Restriction of Processing Art. 18 UK GDPR

You have the right to ask us to pause processing of your personal data in certain circumstances, such as while we investigate a challenge to its accuracy or consider an objection you have raised.

📦 Right to Data Portability Art. 20 UK GDPR

Where processing is based on your consent or the performance of a contract, and is carried out by automated means, you have the right to receive your personal data in a structured, commonly used, machine-readable format, and to request that we transmit it to another controller where technically feasible. For Customers, VenueOra provides a data export function within the Platform on termination of your subscription.

✋ Right to Object Art. 21 UK GDPR

You have the right to object to processing of your personal data where VenueOra relies on legitimate interests as its legal basis. You also have an absolute right to object to processing of your data for direct marketing purposes at any time. Where you object, VenueOra will cease the relevant processing unless it can demonstrate compelling legitimate grounds that override your interests, rights, and freedoms.

🔁 Rights Related to Automated Decision-Making Art. 22 UK GDPR

VenueOra does not make decisions that produce legal or similarly significant effects based solely on automated processing, without human involvement. Where automated risk assessments are made (e.g. by the Payment Processor as part of KYC or fraud screening), these are performed by the Payment Processor as an independent controller under its own policies.

🔕 Right to Withdraw Consent Art. 7(3) UK GDPR

Where we rely on your consent as the legal basis for processing (including for special category data such as biometric data, or for marketing communications), you may withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.

14 Exercising Your Rights

14.1 How to Make a Request

To exercise any of the rights described in Section 13, please contact VenueOra's Data Protection Officer (DPO) using the details below:

- **Email:** dpo@venueora.com
- **Subject line:** Data Subject Request — [type of request]
- **Post:** Data Protection Officer, VenueOra Ticketing Limited, 71-75 Shelton Street Covent Garden London, WC2H 9JQ

Please include your full name, email address associated with your account, and sufficient detail to identify the specific data or processing activity your request relates to.

14.2 Verification

For the protection of your data, VenueOra may ask you to verify your identity before processing a request. We will not charge a fee for handling requests unless a request is manifestly unfounded, excessive, or repetitive, in which case a reasonable administrative fee may apply.

14.3 Timescales

We will respond to all valid requests within **one calendar month** of receipt. Where a request is complex or numerous, we may extend this period by a further two months, in which case we will notify you within the first month of the reason for the extension.

14.4 Requests on Behalf of Others

Where a request is made on behalf of a data subject by a third party (such as a solicitor or authorised representative), VenueOra may require evidence of authority to act before processing the request.

15 Changes to This Policy

15.1 How We Update This Policy

VenueOra may update this Privacy Policy from time to time to reflect changes in our data processing practices, the services we offer, or applicable law. We will publish the updated Policy on this page with a revised effective date. Where changes are material, we will notify Platform Customers by email or via an in-Platform notification.

15.2 Version History

The current version of this Privacy Policy is Version 1.0, effective 10th April 2026. Previous versions are available upon request from dpo@venueora.com.

16 Contact & Complaints

16.1 Data Protection Officer

VenueOra's Data Protection Officer (DPO) is responsible for overseeing compliance with this Policy and UK data protection law. You can contact the DPO at:

Email: dpo@venueora.com
General: support@venueora.com
Platform: venueora.com (https://venueora.com)

16.2 Right to Complain to the ICO

If you are dissatisfied with how VenueOra has handled your personal data or a request you have made, you have the right to lodge a complaint with the UK's supervisory authority:

Information Commissioner's Office (ICO)
Website: ico.org.uk (https://ico.org.uk)
Helpline: 0303 123 1113
Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

We would always encourage you to contact us first to try to resolve any concern before escalating to the ICO.