Tiquo – Privacy Policy

Last updated: 08 June 2026

www.tiquo.co respects your privacy. This policy explains how we collect, use, and protect your personal data when you visit our website, use our services, or interact with us.

Who We Are

TIQUO LTD is a UK-incorporated company registered at:

- **Address:** 180 Strand, London, England, WC2R 1EA
- **Company Number:** 16500553

Depending on the context, we act as a data controller, joint controller, or data processor.

Data Protection Lead

Our Data Protection Lead can be contacted at: privacy@tiquo.co

EU Article 27 Representative

Our representative under GDPR Article 27 is based in Paris, France. Contact via: privacy@tiquo.co

How We Use Your Data

We collect and process personal data for the following purposes:

Purpose	Data	Lawful Basis
Account Creation and Service Delivery	Name, email address, organisation details, login credentials, account preferences	Performance of a contract
Customer Support and Enquiries	Contact information, enquiry details, communications, support history	Performance of a contract and legitimate interests

Billing and Payments	Billing address, VAT details, payment references, transaction records	Performance of a contract and legal obligation
News, Updates and Marketing	Email address, marketing preferences	Consent
Cookies and Analytics	Device data, browser data, IP address, usage information	Legitimate interests and consent where required
Security, Fraud Prevention and Monitoring	Login history, IP address, device information, audit logs	Legitimate interests and legal obligation
Compliance with Legal Obligations	Transaction records, tax records, communications	Legal obligation
Business Sale, Merger or Reorganisation	Any personal data relevant to the transaction	Legitimate interests

Sensitive Personal Data

Certain categories of personal data are considered sensitive under applicable law, including racial or ethnic origin, religious or philosophical beliefs, health information, biometric data, precise geolocation, sexual orientation, genetic data, financial account information, and data concerning children.

Tiquo obtains your explicit consent before processing sensitive personal data, unless processing is strictly necessary to provide the services you have requested or is required by law. You may withdraw your consent at any time by contacting us at privacy@tiquo.co.

Where customers use the Tiquo platform to collect sensitive personal data from their own end-users (for example, health-related information in spa or wellness settings), the customer is responsible as the data controller for obtaining appropriate consent from those individuals.

Data Protection Assessments

We conduct data protection assessments for processing activities that present a heightened risk to consumers, including processing for targeted advertising, processing of sensitive personal data, and any processing that involves profiling. These assessments are maintained internally and are available to regulators upon request as required by applicable law.

Who We Share Your Data With

- Business partners who help us operate our service
- Sub-processors (see https://tiquo.co/legals/subprocessor-policy)
- Regulators and law enforcement, where required by law

- Prospective buyers in the event of a business sale or merger

Categories of Personal Information (US Disclosures)

In the preceding 12 months, we have collected the following categories of personal information:

Category	Examples	Sources	Business Purpose
Identifiers	Name, email address, account ID	Directly from you, your employer/ venue	Account creation, service delivery, support
Commercial information	Transaction records, billing history, subscription details	Directly from you, payment processors	Billing, service delivery
Internet/electronic activity	IP address, browser type, device data, usage logs	Automatically collected	Analytics, security, fraud prevention
Professional/ employment information	Organisation name, job title	Directly from you	Account creation, service delivery
Geolocation data	IP-derived approximate location	Automatically collected	Analytics, compliance

Sale and sharing: Tiquo does not sell personal information for monetary consideration. We may share personal information with analytics providers via cookies, which may constitute "sharing" under certain state laws. You may opt out via the mechanisms described in Your Rights or our Cookie Policy.

AI and Automated Processing

We offer optional AI-enabled features that our customers (service businesses such as hotels, restaurants, spas, gyms, clinics, cinemas, event venues, training providers and similar) can choose to enable. These features process data using Anthropic as our AI model provider.

Our AI Features

- Analytics Insights - AI generates explanations from anonymised analytics data
- Customer Overview Summaries - AI creates customer profile summaries
- Customer Name Enrichment - parses email prefixes to infer first and last names during import

- AI Documents and Forms - generates document templates based on your use case
- Email Campaign Designer - AI-assisted email drafting
- Segment Builder - converts natural language into segment rules

No Automated Decision-Making with Legal Effect

None of these AI features make automated decisions that have legal or similarly significant effects on you. Under GDPR Article 22, you have the right not to be subject to solely automated decision-making with legal or significant effects. Our AI features do not do this.

Data Transfer to Anthropic

Where your venue enables AI features, your data may be processed by Anthropic in the United States under Standard Contractual Clauses (SCCs). Anthropic does not use your data for model training.

Your Control

AI features are enabled and managed by the venue (the business you interact with). If you have concerns about how AI features are used in relation to your personal data, please contact your venue directly. As the data controller, your venue is responsible for determining whether and how AI features are applied to your data.

International Transfers

We use cloud infrastructure in multiple regions:

- AWS eu-west-1 (Ireland)
- AWS us-east-1 (Virginia)

Customer data is replicated across both regions. Transfers to us-east-1 are covered by the EU-US Data Privacy Framework, Standard Contractual Clauses, and UK International Data Transfer Agreement as applicable.

Some of our sub-processors are based in the United States (Stripe, Clerk, Anthropic, and others). For international transfers, we rely on:

- EU Standard Contractual Clauses (Decision 2021/914)
- UK International Data Transfer Agreement (IDTA) and Addendum
- Swiss FDPIC-recognised mechanisms
- APEC Cross-Border Privacy Rules (CBPR) where applicable
- Adequacy decisions

Transfer Impact Assessments are maintained and available on request from privacy@tiquo.co

How Long We Keep Your Data

We retain personal data in accordance with our Data Retention Schedule. Key periods include:

- Account data - retained during contract plus 90 days after termination
- Billing records - retained for 7 years (tax compliance)
- Marketing data - retained until you withdraw consent
- Support records - retained for 2 years
- Security logs - retained for 12 months

Breach Notification

In the event of a personal data breach that is likely to result in a risk to your rights, we will notify the relevant supervisory authorities and, where required by applicable law, affected individuals without undue delay. This includes notification to the ICO (UK), relevant EU supervisory authorities, the Office of the Privacy Commissioner of Canada, the Commission d'acces a l'information du Quebec, and any other applicable regulator.

Your Rights

EU/EEA (GDPR)

- Access
- Rectification
- Erasure
- Restriction
- Portability
- Objection
- Complaint to your local DPA

UK (UK GDPR)

- Access
- Rectification
- Erasure
- Restriction
- Portability
- Objection
- Complaint to the ICO

Switzerland (revFADP)

- Access
- Rectification
- Deletion

- Complaint to the FDPIC

United States

The following rights apply to residents of California (CCPA/CPRA), Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), Texas (TDPSA), Oregon (OCPA), Montana (MCDPA), Florida (FDBR), Iowa (ICDPA), Indiana (ICDPA), Tennessee (TIPA), Delaware (DPDPA), New Jersey (NJDPA), New Hampshire (NHDPA), Nebraska (NDPA), Minnesota (MCDPA), Maryland (MODPA), Kentucky (KCDPA), Rhode Island (RIDTPPA), and any other US state with applicable comprehensive privacy legislation.

- Know what personal data we collect and how it is used
- Access your personal data
- Correct inaccurate personal data
- Delete your personal data
- Data portability (receive your data in a structured, commonly used format)
- Opt-out of the sale or sharing of your personal data
- Opt-out of targeted advertising
- Opt-out of profiling in furtherance of decisions that produce legal or similarly significant effects
- Limit the use of sensitive personal information to purposes necessary to provide the services
- Non-discrimination for exercising your rights
- Appeal a denied rights request

You may exercise these rights by contacting us at privacy@tiquo.co. You may also designate an authorised agent to submit a request on your behalf by providing signed written authorisation or a valid power of attorney. We will respond to verified requests within 45 days, with a possible 45-day extension if we notify you of the reason for the delay.

We honour Global Privacy Control (GPC) and other legally recognised universal opt-out signals as valid opt-out requests under applicable state laws.

Tiquo does not sell personal data for monetary consideration. Where processing activities may constitute "sharing" under applicable law (such as cross-context behavioural advertising via cookies), you may opt out as described above and in our Cookie Policy.

Canada (PIPEDA)

- Access your personal information
- Correction of inaccurate or incomplete personal information
- Withdraw consent to the collection, use, or disclosure of your personal information
- Challenge our compliance with PIPEDA principles

Our Data Protection Lead is accountable for our compliance with PIPEDA and can be contacted at privacy@tiquo.co. We obtain meaningful consent (express or

implied, as appropriate to the sensitivity of the information) before collecting, using, or disclosing your personal information. Collection is limited to what is necessary for the identified purposes.

If you are unsatisfied with our response to a complaint, you may escalate it to the Office of the Privacy Commissioner of Canada (OPC).

Canada - Quebec (Law 25)

In addition to your rights under PIPEDA, if you are a Quebec resident, you have the following rights under the Act Respecting the Protection of Personal Information in the Private Sector (Law 25):

- Access your personal information
- Rectification of inaccurate, incomplete, or equivocal personal information
- Data portability (receive your information in a structured, commonly used technological format)
- De-indexing (request that we cease disseminating your personal information or de-index any hyperlink attached to your name where it causes serious harm to your reputation or privacy)
- Withdraw consent to the processing of your personal information
- Be informed about any decision made exclusively by automated processing of your personal information

We conduct Privacy Impact Assessments for any project involving personal information as required by Law 25. We obtain express consent before processing sensitive personal information including biometric data, health information, and information about minors.

Our privacy officer responsible for the protection of personal information can be contacted at privacy@tiquo.co. In the event of a confidentiality incident presenting a risk of serious injury, we will notify the Commission d'acces a l'information du Quebec (CAI) and affected individuals.

Canada - Alberta (PIPA)

- Access your personal information
- Correction of inaccurate personal information
- Withdraw consent
- Complaint to the Office of the Information and Privacy Commissioner of Alberta

We will respond to access requests within 45 days.

Canada - British Columbia (PIPA)

- Access your personal information
- Correction of inaccurate personal information
- Withdraw consent
- Complaint to the Office of the Information and Privacy Commissioner for British Columbia

We will respond to access requests within 30 business days.

Singapore (PDPA)

- Access
- Correction
- Withdraw consent

Hong Kong (PDPO)

- Access
- Correction

Brazil (LGPD)

- Access
- Correction
- Deletion
- Portability
- Information
- Opposition

Japan (APPI)

- Disclosure
- Correction
- Deletion

Australia (APPs)

- Access
- Correction
- Complaint to the OAIC

India (DPDPA)

- Access
- Correction
- Erasure
- Grievance redressal

To exercise any of these rights, please contact us at privacy@tiquo.co

Cookies

For detailed information about our use of cookies, please refer to our Cookie Policy on our website.

Protecting Children's Data

Tiquo does not knowingly collect personal data from children under 16 in the course of its own operations (such as account registration, marketing, or website usage). If we become aware that we have collected such data, we will delete it promptly.

Where our customers use the Tiquo platform to process personal data of their own end-users, including minors, the customer is responsible as the data controller for ensuring appropriate consent, age verification, and deletion in accordance with applicable law.

Under US state laws, Tiquo does not sell or share the personal information of consumers it knows to be under 16 years of age without affirmative authorisation. For consumers under 13, we require verifiable parental consent before collecting personal information.

If you believe we have inadvertently collected data from a child, please contact us at privacy@tiquo.co.

Changes to This Policy

We may update this privacy policy from time to time. We will notify you of material changes via our website or by email where appropriate. Your continued use of our services constitutes acceptance of the updated policy.

Contact Us

If you have any questions about this privacy policy or how we handle your data, please contact:

privacy@tiquo.co