Privacy Policy

iQueuing · Effective date: July 31, 2026 · English controlling language

1. Introduction

This Privacy Policy explains how iQueuing ("we," "us," or "our") collects, uses, and discloses information when you access or use our SaaS platform. When we process personal data on behalf of our B2B customers ("Tenants"), we act as a Data Processor, and our Tenants act as Data Controllers.

2. Information We Collect

We collect information categorized as follows:

- **Account Information:** Name, email, billing details, and credentials.
- **Usage Data:** IP addresses, browser types, log files, and interaction telemetry.
- **Derived/Inferred Data:** Analytics generated from your use of the platform.
- **Tenant Data:** Data uploaded by Tenants or their End Users.
- **Mobile and messaging data:** When Tenants use the Platform for SMS/MMS (for example queue updates, appointment reminders, or marketing where permitted), we and our messaging partners may process mobile telephone numbers, message content, delivery status, timestamps, and related metadata needed to send and measure those messages.

3. Legal Bases for Processing (EEA/UK Users)

We rely on the following legal bases to process personal data:

- **Contract Performance:** To provide the platform and enforce our agreements.
- **Legitimate Interests:** To secure, analyze, and improve our services.
- **Consent:** When legally required, which you may withdraw at any time.

4. Data Sharing and Sub-processors

We do not sell your personal data. We engage a limited set of essential sub-processors to operate the Platform, each bound by data-protection terms:

- **Google Cloud / Firebase:** application hosting, authentication, database, file storage, and serverless compute (infrastructure provider).
- **Stripe:** subscription billing and payment processing; we do not store full payment card numbers.

- **Telecommunications & messaging providers (e.g., Telnyx, SendGrid/Twilio):** transmission, routing, and delivery of SMS/MMS and transactional email, including carrier-compliance activities.

We process **Personally Identifiable Information (PII)** such as guest names and mobile telephone numbers **on the documented instructions of our Tenants (the Data Controllers)** for the purpose of delivering the requested service (for example, sending a queue-ready text). A current list of sub-processors is maintained on our Sub-processors page. We may also disclose data to comply with legal obligations or defend our legal rights.

Additional commitments that apply specifically to **mobile telephone numbers** and **SMS/MMS** are set out in Section 10 below, including the statement required for U.S. toll-free and similar messaging compliance programs.

Localization and machine translation. Where we use AI or machine-translation engines (including listed sub-processors) to generate or refresh non-English UI, documentation, notifications, or legal-page displays, that processing is limited to providing convenience translations. The English versions of our legal documents remain the sole legally binding language of record (see our Terms, Controlling Language section).

5. CCPA/CPRA Disclosures (California Residents)

We do not "sell" personal information as defined by the CCPA.

"Sharing" and cross-context behavioral advertising. If any disclosure qualifies as "sharing" under the CCPA, it is limited to technical signals collected through our own websites or software (for example cookies, pixels, or similar technologies) used to measure marketing performance or product usage. We do **not** use **mobile telephone numbers**, SMS/MMS message content, or text-messaging subscriber or opt-in records for cross-context behavioral advertising, and we do **not** disclose those categories to advertising partners for their independent promotional or marketing use. This aligns with Section 10.

California residents may request access, deletion, and correction of personal information, and may opt out of "sharing" where applicable, subject to verification and any Tenant relationship described elsewhere in this Policy.

6. Data Subject Rights

Depending on your jurisdiction, you may have the right to access, delete, port, or correct your personal data. We will respond to verified requests within forty-five (45) days. We reserve the right to verify your identity before processing any request. If your data is controlled by a Tenant, we will route your request to the respective Tenant.

7. Security

We implement commercially reasonable technical and organizational measures designed to protect your data. However, no internet transmission is entirely secure, and we cannot guarantee absolute security.

8. Children's Privacy

The Platform is intended for business use and is not directed to children under the age of 16. We do not knowingly collect personal data from children under 16. Tenants are solely responsible for ensuring they have lawful grounds for processing any minor's data on the Platform.

9. International Transfers

iQueuing is established in Ireland. Platform infrastructure and certain sub-processors process personal data in the United States and other locations outside Ireland. Where personal data is transferred from the EEA, UK, or Switzerland to a country that does not provide an adequate level of protection, we rely on appropriate safeguards, including the EU Standard Contractual Clauses (SCCs), and other measures required by applicable data-protection law.

10. SMS, MMS, and mobile information (U.S. carrier compliance)

No sale or sharing of mobile information for third-party promotional or marketing purposes. We will not sell or share your mobile information, including your mobile telephone number, with third parties for their promotional or marketing purposes. This statement is included to satisfy common U.S. carrier and toll-free verification expectations, including those described in industry guidance such as Telnyx's Toll Free Verification Request Guide.

For California residents, this commitment works together with the limits on CCPA "sharing" described in Section 5.

How this applies on the Platform. iQueuing provides software to business customers (Tenants). If you are an **end user** of a Tenant (for example you join a waitlist or book an appointment), your mobile number and messages are generally processed because the Tenant instructed us to provide the service. The Tenant is responsible for lawful consent, notice, and program rules. You can typically opt out of further SMS from that Tenant by following instructions in the message (for example replying **STOP** where supported) or by contacting the Tenant directly.

Transactional vs marketing. Where a Tenant sends both transactional and marketing messages, carriers and aggregators often require those programs to be described consistently and for marketing to rely on appropriate consent. We expect Tenants to honor applicable law and carrier policies, including keeping SMS consent separate from other channels (such as email) when required.

Disclosures in opt-in flows. Industry programs frequently require that, before the first non-inbound marketing or subscription message, subscribers see disclosures similar to:

identification of the brand; the use case; that message and data rates may apply; that frequency may vary; how to get help; how to opt out; and links to Terms and Privacy. Tenants should present those disclosures in their own branded opt-in surfaces; we provide configuration tools where applicable.

Privacy policy language for Tenants. Many carriers expect a published privacy policy to state that mobile information will not be sold or shared with third parties for promotional or marketing purposes. The bolded statement at the start of this section is intended to satisfy that expectation for information processed under this Policy. Tenants remain responsible for any additional disclosures required for their own brands, jurisdictions, and campaigns.

Messaging partners. Delivery of SMS/MMS may rely on telecommunications providers and aggregators (for example Telnyx). Their processing is limited to transmitting, routing, filtering, and compliance-related activities. For more detail on categories of vendors, see our Subprocessors page and your agreement with us.

11. Canadian toll-free and double opt-in

If you operate messaging to Canadian subscribers on certain toll-free programs, carriers may require **double opt-in**: after the initial subscription step, send a confirmation message and obtain an affirmative reply before marketing or subscription traffic. Tenants are responsible for implementing any Canada-specific consent flows their counsel or carriers require.