DATA PROCESSING AGREEMENT

GDPR Article 28 / UK GDPR / India DPDP / Global Processing Terms

between

Jal Technology LLC d/b/a QRCodeKey

("Processor")

647 Rose Lane, Bartlett, Illinois 60103, USA

and

[CUSTOMER LEGAL NAME]

("Controller")

[Customer address]

Effective Date: _____

Template Version 1.0 — May 2026

Recitals

This Data Processing Agreement (this "DPA") is entered into as of the Effective Date by and between Jal Technology LLC d/b/a QRCodeKey ("Processor") and the customer identified on the cover page ("Controller"). Processor and Controller are referred to individually as a "Party" and collectively as the "Parties".

WHEREAS, Controller has subscribed to one or more QRCodeKey services (the "Services") under the QRCodeKey Terms of Service available at qrcodekey.com/terms (the "Underlying Agreement");

WHEREAS, in providing the Services, Processor will Process Personal Data on behalf of Controller; and the Parties wish to ensure that such Processing complies with the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR"), the United Kingdom's UK GDPR and Data Protection Act 2018, India's Digital Personal Data Protection Act, 2023 ("DPDP Act"), the California Consumer Privacy Act / California Privacy Rights Act ("CCPA / CPRA"), Brazil's Lei Geral de Proteção de Dados ("LGPD"), Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), Australia's Privacy Act 1988, and any other applicable data-protection law (collectively, "Data Protection Laws");

NOW, THEREFORE, in consideration of the mutual promises set forth in this DPA and in the Underlying Agreement, the Parties agree as follows.

1. Definitions

Capitalized terms used but not otherwise defined in this DPA shall have the meanings ascribed to them in the GDPR. The following terms shall have the meanings set forth below:

“Personal Data” means "personal data" as defined in GDPR Article 4(1), and any analogous term in any applicable Data Protection Law (including "personal information" under CCPA / CPRA, "personal data" under DPDP, "dados pessoais" under LGPD, "personal information" under PIPEDA, etc.), that is Processed by Processor on behalf of Controller in connection with the Services.

“Process” means / "Processing" means any operation or set of operations performed on Personal Data, as defined in GDPR Article 4(2).

“Data Subject” means the identified or identifiable natural person to whom Personal Data relates.

“Sub-processor” means any third party engaged by Processor to Process Personal Data on behalf of Controller.

“Standard Contractual Clauses (“SCCs”)” means the standard contractual clauses for the transfer of personal data to third countries adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended from time to time.

“UK Addendum” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office, as amended from time to time.

“Personal Data Breach” means a breach of security as defined in GDPR Article 4(12).

“Restricted Transfer” means a transfer of Personal Data from a jurisdiction whose laws prohibit or restrict the transfer absent a specific safeguard (including the EEA, the United Kingdom, Switzerland, and any other jurisdiction whose laws apply analogously).

2. Scope and Roles of the Parties

2.1 Roles

With respect to Personal Data Processed under this DPA, Controller is the data controller (or analogous role under applicable Data Protection Laws — "data fiduciary" under DPDP, "business" under CCPA, "controlador" under LGPD) and Processor is the data processor (or analogous role — "data processor" under DPDP, "service provider" under CCPA, "operador" under LGPD).

2.2 Subject Matter and Scope

The subject matter, duration, nature, and purpose of the Processing, the types of Personal Data, and the categories of Data Subjects are set forth in Annex I (Description of Processing).

2.3 Compliance with Data Protection Laws

Each Party shall comply with the obligations applicable to it under the Data Protection Laws. Controller is responsible for the lawfulness of the Personal Data Processing and for the accuracy, quality, and legality of Personal Data, including ensuring that Controller has provided all required notices and obtained all required consents from Data Subjects before sharing Personal Data with Processor.

3. Obligations of Processor

3.1 Documented Instructions

Processor shall Process Personal Data only on documented instructions from Controller, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by EU or Member State law to which Processor is subject. The Underlying Agreement, this DPA (including its Annexes), and Controller's use of features and configurations within the Services constitute Controller's complete and final documented instructions to Processor with respect to the Processing.

3.2 Confidentiality

Processor shall ensure that persons authorised to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.3 Security Measures

Processor shall implement and maintain the technical and organisational measures set forth in Annex II (Security Measures) to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

3.4 Sub-processors

Controller hereby authorises Processor to engage the Sub-processors listed in Annex III (Sub-processors), and any additional Sub-processors notified to Controller in accordance with this Section.

Processor shall: (a) inform Controller of any intended addition, replacement, or change to its list of Sub-processors at least thirty (30) days in advance, providing Controller with the opportunity to object on reasonable data-protection grounds; (b) impose on each Sub-processor data-protection obligations that are no less protective than those in this DPA; and (c) remain fully liable to Controller for the performance of each Sub-processor's obligations.

If Controller reasonably objects to a new Sub-processor on data-protection grounds within thirty (30) days of notice, the Parties shall negotiate in good faith to resolve the objection. If no resolution is reached within thirty (30) additional days, Controller may terminate the Underlying Agreement and this DPA without penalty, with respect to the affected Service, on written notice.

3.5 Assistance with Data Subject Requests

Processor shall, taking into account the nature of the Processing, assist Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Controller's obligation to respond to requests for exercising the Data Subject's rights under Data Protection Laws (right of access, rectification, erasure, restriction, portability, objection, automated decision-making). If Processor receives such a request directly from a Data Subject, Processor shall promptly forward it to Controller and shall not respond except on Controller's instructions, unless required to do so by applicable law.

3.6 Assistance with Controller's Compliance

Processor shall assist Controller in ensuring compliance with the obligations pursuant to GDPR Articles 32 to 36 (security, breach notification, data protection impact assessment, prior consultation), taking into account the nature of the Processing and the information available to Processor.

3.7 Personal Data Breach Notification

Processor shall notify Controller without undue delay, and in any event no later than seventy-two (72) hours after becoming aware of a Personal Data Breach. The notice shall include, to the extent known: (a) the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records concerned; (b) the likely consequences of the Personal Data Breach; (c) the measures taken or proposed to address the Personal Data Breach, including measures to mitigate adverse effects; and (d) the name and

contact details of Processor's contact for follow-up. Processor shall cooperate with Controller and provide reasonable assistance in connection with Controller's notification obligations to supervisory authorities and Data Subjects.

3.8 Deletion or Return

Upon termination of this DPA or at any earlier written request from Controller, Processor shall, at the choice of Controller, delete or return all Personal Data to Controller and delete existing copies, unless EU or Member State law requires storage of the Personal Data. Backup copies shall be deleted in accordance with Processor's ordinary backup retention cycle (not to exceed ninety (90) days).

3.9 Audits and Information

Processor shall make available to Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and shall allow for and contribute to audits, including inspections, conducted by Controller or another auditor mandated by Controller. Processor may satisfy this obligation by providing Controller with: (a) copies of any third-party audit reports (e.g., SOC 2 Type II, ISO 27001) held by Processor; or (b) a written response to a reasonable security questionnaire. On-site audits may be requested no more than once per year (unless triggered by a Personal Data Breach or supervisory-authority instruction), shall be conducted with reasonable advance notice, during business hours, and in a manner that does not unreasonably disrupt Processor's operations.

4. Obligations of Controller

4.1 Lawful Basis

Controller represents and warrants that: (a) it has a lawful basis for the Processing of Personal Data through the Services under applicable Data Protection Laws; (b) it has provided all required notices to Data Subjects (including any privacy notice required by GDPR Articles 13–14, CCPA notice-at-collection, DPDP Section 5, etc.); and (c) where required, it has obtained valid consent from Data Subjects.

4.2 Special Categories

Controller shall not provide to Processor any special-category data (as defined in GDPR Article 9, including biometric data, health data, racial / ethnic origin, religious belief, sexual orientation, etc.) or any data relating to criminal convictions and offences (GDPR Article 10), except where the Services have been specifically configured by Processor to handle such data and Controller has documented its lawful basis. Processor does not currently offer biometric Processing under any product configuration.

4.3 Children's Data

Where Personal Data relates to a child below the applicable age of digital consent (16 default under GDPR Art. 8, lower as set by individual Member States; 13 under COPPA in the US; below the applicable threshold under DPDP Section 9; below the applicable threshold under

analogous laws), Controller represents and warrants that it has obtained verifiable parental or legal-guardian consent in accordance with the applicable law before sharing the child's Personal Data with Processor.

5. International Data Transfers

5.1 Mechanism — EU SCCs

Where Processor's Processing of Personal Data on behalf of Controller constitutes a Restricted Transfer from the European Economic Area (EEA), the Standard Contractual Clauses (Module Two: controller to processor), as adopted by Commission Implementing Decision (EU) 2021/914, are hereby incorporated into and form part of this DPA. The selections in the Annexes to this DPA shall serve as the corresponding selections in the SCCs:

- Module Two (controller to processor) applies.
- Clause 7 (Docking Clause): not used in the standalone version of this DPA; if a third party wishes to accede, the Parties shall agree in writing.
- Clause 9(a) (Sub-processor authorisation): Option 2 (general written authorisation), with thirty (30) days' notice in advance.
- Clause 11(a) (Independent dispute resolution): not used.
- Clause 17 (Governing law): the law of the Republic of Ireland.
- Clause 18 (Choice of forum): the courts of Ireland.
- Annex I (List of Parties, Description of Transfer, Competent Supervisory Authority): see Annex I to this DPA.
- Annex II (Technical and Organisational Measures): see Annex II to this DPA.
- Annex III (Sub-processors): see Annex III to this DPA.

5.2 UK Restricted Transfers

Where the Restricted Transfer is from the United Kingdom, the UK Information Commissioner's Office International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "UK Addendum") is incorporated into this DPA and shall apply with the selections set forth in the Annexes. References in the SCCs to GDPR shall be read as references to UK GDPR; references to Member-State law shall be read as references to UK law; the governing law of the SCCs shall be replaced with the law of England and Wales; the choice of forum shall be replaced with the courts of England and Wales.

5.3 Switzerland

Where the Restricted Transfer is from Switzerland, references in the SCCs to GDPR shall be read as references to the Swiss Federal Act on Data Protection (FADP / nFADP); references to a supervisory authority shall be read as references to the Swiss Federal Data Protection and Information Commissioner; references to natural persons shall include legal persons until the Swiss FADP is updated.

5.4 Other Jurisdictions

For Restricted Transfers from any other jurisdiction (including India under DPDP Section 16, Brazil under LGPD Articles 33–36, China under PIPL Articles 38–43, etc.), the Parties shall implement an applicable safeguard (such as the analogous standard contractual clauses, certification, or government authorisation) before initiating the transfer.

6. CCPA / CPRA Service Provider Terms

To the extent Processor Processes Personal Data of California residents under the CCPA / CPRA, Processor is a "service provider" to Controller. Processor shall:

- Process Personal Data only for the limited and specified purposes set forth in the Underlying Agreement and this DPA;
- Not sell or share Personal Data;
- Not retain, use, or disclose Personal Data outside of the direct business relationship between Controller and Processor;
- Not combine Personal Data received from Controller with Personal Data received from any other source, except as permitted by the CCPA / CPRA;
- Comply with all applicable obligations of a service provider under the CCPA / CPRA;
- Notify Controller if Processor determines that it can no longer meet its obligations under the CCPA / CPRA.

7. India DPDP Act 2023 — Data Processor Terms

To the extent Processor Processes Personal Data of Data Subjects in India under the DPDP Act, Processor is a "data processor" under contract with Controller (the "data fiduciary"). Processor shall: (a) Process Personal Data only on the documented instructions of Controller; (b) implement reasonable security safeguards under DPDP Section 8(5); (c) notify Controller of any Personal Data Breach within seventy-two (72) hours under DPDP Section 8(6); (d) assist Controller in responding to Data-Principal rights requests under DPDP Sections 11–14; and (e) cooperate with the Data Protection Board of India under DPDP Section 27 in the event of an inquiry. Where DPDP Section 16 cross-border transfer rules require a specific safeguard, the Parties shall implement the safeguard before the transfer.

8. Liability and Indemnification

8.1 Liability under Data Protection Laws

Each Party shall be liable to Data Subjects for breaches of the Data Protection Laws as set forth in those laws. Nothing in this DPA limits the liability of either Party to a Data Subject under GDPR Article 82 or analogous provisions.

8.2 Indemnification

Each Party shall indemnify, defend, and hold harmless the other Party and its officers, directors, employees, agents, and successors from and against any third-party claims, demands, actions, suits, judgments, fines, penalties, losses, damages, settlements, costs, and expenses (including reasonable attorneys' fees) to the extent arising out of or resulting from the indemnifying Party's breach of this DPA or the applicable Data Protection Laws. Controller specifically indemnifies Processor against claims arising from Controller's lack of lawful basis, missing notice, or inadequate consent.

8.3 Limitation of Liability

Except for the indemnification obligations in Section 8.2, the Parties' liability under or in connection with this DPA shall be subject to the limitation of liability set forth in the Underlying Agreement.

9. Term, Termination, and Survival

9.1 Term

This DPA shall commence on the Effective Date and shall continue in effect for so long as the Underlying Agreement is in effect or Processor holds any Personal Data of Controller, whichever is later.

9.2 Termination for Material Breach

Either Party may terminate this DPA and the Underlying Agreement upon thirty (30) days' written notice if the other Party materially breaches this DPA and fails to cure the breach within the thirty-day period.

9.3 Survival

Sections 3.7, 3.8, 3.9, 5, 8, 9, and 10 shall survive termination of this DPA.

10. Miscellaneous

10.1 Order of Precedence

In the event of a conflict between this DPA and the Underlying Agreement with respect to the Processing of Personal Data, this DPA shall control. In the event of a conflict between this DPA and the SCCs, the SCCs shall control. With respect to all other matters, the Underlying Agreement shall control.

10.2 Amendment

The Parties shall amend this DPA from time to time as is reasonably necessary to comply with changes in Data Protection Laws.

10.3 Notices

Notices to Processor shall be sent to info.qrcodekey@gmail.com with a copy to the address on the cover page. Notices to Controller shall be sent to the address and email on the cover page.

10.4 Counterparts; Electronic Signature

This DPA may be executed in counterparts, including by electronic signature.

10.5 Entire Agreement

This DPA, together with the Underlying Agreement and the SCCs / UK Addendum (as applicable), constitutes the entire agreement between the Parties with respect to the Processing of Personal Data.

Signatures

IN WITNESS WHEREOF, the Parties have caused this Data Processing Agreement to be executed by their duly authorized representatives as of the Effective Date.

PROCESSOR — Jal Technology LLC d/b/a QRCodeKey

By: _____

Name: Ashvinkumar Chaudhari

Title: Founder & Authorized Signatory

Date: _____

Email: info.qrcodekey@gmail.com

CONTROLLER — [CUSTOMER LEGAL NAME]

By: _____

Name: _____

Title: _____

Date: _____

Email: _____

Annex I — Description of Processing (per SCCs Module Two)

A. List of Parties

Data Exporter (Controller): the customer identified on the cover page. Contact: as set forth on the cover page. Activities: subscribing to QRCodeKey for QR generation, attendance, visitor management, asset tracking, lost-key recovery, group administration, and related services. Role: controller / data fiduciary / business / controlador.

Data Importer (Processor): Jal Technology LLC d/b/a QRCodeKey, 647 Rose Lane, Bartlett, Illinois 60103, USA. Contact: info.qrcodekey@gmail.com. Activities: providing the Services. Role: processor / service provider / operador.

B. Description of Transfer

Categories of Data Subjects whose Personal Data is transferred:

- Controller's authorised users (admins, staff, employees, contractors)
- Group members enrolled by Controller (employees, students if a separate School Data Addendum is in effect, group members generally)
- Visitors to Controller's premises (where the Visitor Management feature is enabled)
- Finders / scanners of Controller's QR codes (third parties who scan a QR code)

Categories of Personal Data transferred:

- Identifiers (name, email, phone number, address, account ID, role)
- Authentication data (password hashes, JWT tokens, session metadata)
- Group / organisational data (membership, role within group)
- Scan / attendance data (QR ID, timestamp, GPS coordinates, device fingerprint, IP address)
- Visitor sign-in data (name, phone, email, purpose of visit, photo if uploaded by visitor, signature, sign-in / sign-out times)
- Payment metadata (payment processor reference IDs only — full card data is not transferred to Processor; PCI-DSS-scoped fields are handled by Stripe)
- Communications metadata (SMS / email logs for transactional notifications)

Sensitive Data: not intentionally Processed; Controller shall not provide special-category data per Section 4.2.

Frequency of transfer: continuous (during the term of the Underlying Agreement).

Nature of Processing: hosting, storage, retrieval, transmission, analysis, deletion, backup, security monitoring, and other operations necessary to provide the Services.

Purpose of transfer and further Processing: provision of the Services to Controller, including QR generation, scan tracking, attendance, visitor management, notifications, reports, support, security, and platform improvement that does not result in disclosure of Personal Data.

Retention period: as set forth in the Underlying Agreement and Section 3.8 of this DPA. Active data is retained for the duration of the Underlying Agreement; backup copies are retained for up to ninety (90) days after deletion.

C. Competent Supervisory Authority

Where the data exporter is established in an EEA Member State: the supervisory authority of that Member State. Where the data exporter is not established in an EEA Member State but falls within the territorial scope of the GDPR, the supervisory authority of the EU representative's Member State.

Where the data exporter is established in the United Kingdom: the UK Information Commissioner's Office (ICO).

Where the data exporter is established in Switzerland: the Federal Data Protection and Information Commissioner (FDPIC).

Annex II — Technical and Organisational Measures

Processor implements and maintains the following technical and organisational measures, in accordance with GDPR Article 32, to ensure a level of security appropriate to the risk:

1. Pseudonymisation and Encryption

- Encryption at rest: AES-256 encryption of all Personal Data stored in MongoDB Atlas, Render disk volumes, and any backup copies.
- Encryption in transit: TLS 1.2 (or stronger) for all client-server communication and all server-server communication between Processor's systems and Sub-processors.
- Password storage: bcrypt with industry-standard cost factor.
- Token storage: JWT signed with HS256 / RS256, rotated regularly.

2. Confidentiality, Integrity, Availability, Resilience

- Multi-factor authentication enforced for Processor's administrative access to production systems.
- Role-based access control with principle of least privilege; access is auto-revoked on workforce departure.
- Audit logging of all administrative access and all Personal Data access where technically feasible.
- Regular vulnerability scanning, dependency-update reviews, and patch management.
- Web application firewall (Helmet, mongo-sanitize, hpp, rate limiting) on all public-facing endpoints.
- DDoS protection at the edge through CDN / hosting provider.

3. Restoration of Availability

- Daily automated backups of MongoDB Atlas with point-in-time recovery.
- Documented disaster-recovery procedure with target RTO of 4 hours and RPO of 24 hours.
- Quarterly test restores from backup.

4. Process for Regularly Testing the Effectiveness of Measures

- Annual security review by Processor's engineering team.
- Penetration testing or third-party security assessment as commercially reasonable.
- Continuous monitoring for anomalous access patterns.

5. Identification and Authorisation

- All workforce members with access to Personal Data are subject to confidentiality obligations under their employment / contractor agreement.
- Background screening for workforce members with administrative access, where permitted by law.
- Annual data-protection and security training.

6. Physical Security

- Personal Data is stored in MongoDB Atlas, Render, and Vercel data centres, each of which maintains physical security controls (24/7 surveillance, controlled access, environmental monitoring) appropriate to a Tier III / SOC 2 Type II facility.

7. Sub-processor Management

- All Sub-processors that handle Personal Data are bound by written agreements with data-protection obligations no less protective than those in this DPA. The current list of Sub-processors is maintained in Annex III and on Processor's website at qrcodekey.com/sub-processors.

8. Personal Data Breach Procedures

- Documented incident response plan covering detection, assessment, containment, notification, and post-incident review.
- Notification to Controller within seventy-two (72) hours per Section 3.7 of this DPA.

Annex III — Authorised Sub-processors

As of the Effective Date, Processor uses the following Sub-processors:

1. MongoDB Atlas — operated by MongoDB, Inc., 1633 Broadway, 38th Floor, New York, NY 10019, USA. Service: cloud database hosting. Region: AWS us-east-1 (US East — N. Virginia) or as configured by Controller. Security: AES-256 at rest, TLS in transit, SOC 2 Type II, ISO 27001, ISO 27017, ISO 27018, GDPR DPA published.

2. Render Services, Inc. — 525 Brannan Street, San Francisco, CA 94107, USA. Service: backend application hosting (Node.js, Express, Socket.io). Region: AWS us-east. Security: SOC 2 Type II, GDPR DPA published, encrypted volumes, automated backups.

3. Vercel Inc. — 340 S Lemon Ave #4133, Walnut, CA 91789, USA. Service: frontend hosting (Next.js), CDN edge, image optimisation. Region: global edge network with primary processing in the US. Security: SOC 2 Type II, GDPR DPA published.

4. Stripe, Inc. — 510 Townsend Street, San Francisco, CA 94103, USA. Service: payment processing and subscription billing. Region: global. Security: PCI-DSS Level 1, SOC 2 Type II, GDPR DPA published. Note: full card data is held by Stripe, not by Processor.

5. Telnyx LLC — 311 W Superior Street, Suite 504, Chicago, IL 60654, USA. Service: SMS and voice notifications, A2P 10DLC brand-verified. Region: US. Security: SOC 2 Type II, HIPAA-eligible, GDPR DPA published.

6. OpenAI, L.L.C. — 3180 18th Street, San Francisco, CA 94110, USA. Service: AI chatbot ("AG") and AI voice agent ("Priya") via the Realtime API and the Chat Completions API. Region: US. Security: SOC 2 Type II, data-processing addendum executed, ZDR mode enabled — Controller Personal Data is NOT used to train OpenAI models.

7. Google LLC — Google Maps Platform (reverse geocoding); Mountain View, CA, USA. Service: address resolution from GPS coordinates. Data shared: GPS coordinates only — no Personal Data identifiers.

8. Twilio Inc. — fallback / alternative SMS provider — 101 Spear Street, San Francisco, CA 94105, USA. (Used as backup; primary SMS path is Telnyx.)

Processor will provide Controller with thirty (30) days' advance written notice of any addition, replacement, or removal of a Sub-processor that handles Personal Data, in accordance with Section 3.4 of this DPA. The current list is maintained at qrcodekey.com/sub-processors.

Annex IV — Controller Contact for Privacy Matters

Controller designates the following contact for privacy and data-protection matters under this DPA:

Name: _____

Title: _____

Email: _____

Phone: _____

Where required by GDPR Article 27 / UK GDPR or analogous law, Controller has appointed an EU / UK representative as follows (if any):

Representative name: _____

Representative address: _____

Representative email: _____

Where required by DPDP, Controller has appointed an India-based Data Protection Officer / Significant Data Fiduciary representative as follows (if any):

DPO name: _____

DPO email: _____