· DATA PROCESSING AGREEMENT · CONFIDENTIAL

Data Processing *Agreement.*

TOOTHMATRIX · TRUST CENTER

Controller [Controller — to be filled by signer]

Processor Toothrocket Labs (T/A Toothmatrix), Doha, Qatar

Requested by — (—)

Generated at 2026-06-12T20:49:22.334349+00:00

Tenant scope platform

Document ID 237dbeba-e6c7-453e-a1a7-1151adbc1b98

Version v1.0 (2026-02)

This template captures the standard data-processing terms applicable to all Toothmatrix tenants. Sections referencing specific regulatory frameworks (PDPPL, GDPR, HIPAA) take precedence where the Controller's jurisdiction triggers them.

1. Definitions

For the purposes of this Agreement:

- **Controller** means [Controller — to be filled by signer], the dental laboratory acting as the data controller.
- **Processor** means Toothrocket Labs (trading as Toothmatrix), incorporated in Qatar.
- **Personal Data** means any information relating to an identified or identifiable natural person, including patient identifiers, contact details, clinical notes, and case file metadata.
- **Sub-processor** means any third-party engaged by the Processor to handle Personal Data on behalf of the Controller (current list available at `/trust`).
- **Applicable Law** means the Qatar Personal Data Privacy Protection Law (PDPPL, Law 13/2016) and, where the Controller's patients are located in the EU or US, the GDPR (2016/679) and HIPAA respectively.

2. Subject matter & duration

The Processor shall process Personal Data on behalf of the Controller solely to provide the Toothmatrix Service (multi-tenant dental lab SaaS). Processing shall continue for the duration of the Service Agreement and end upon termination, subject to the retention requirements in Section 9.

3. Nature & purpose of processing

- Receipt, storage, and routing of case files (scans, prescriptions, design data)
- Generation of invoices, warranty certificates, and case status notifications
- Aggregate analytics (de-identified) to operate and improve the Service
- Email and SMS notifications to dentists and patients with the Controller's instruction

4. Categories of data subjects

Patients of the Controller (data subjects), dental practitioners and staff using the Controller's account, and the Controller's administrative users.

5. Categories of Personal Data

CATEGORY	EXAMPLES	SENSITIVITY
Identifiers	Name, email, phone	Standard

Clinical case data	Tooth charts, shade, scans, restoration type	Sensitive (health data)
Operational metadata	Order date, delivery date, courier tracking	Standard
Financial records	Invoices, payment status, credit balance	Confidential

6. Obligations of the Processor

The Processor shall:

1. Process Personal Data only on documented instructions from the Controller, including transfers outside Qatar.
2. Ensure that all personnel authorised to process the data are under appropriate confidentiality obligations.
3. Implement the technical and organisational measures described in Annex A (Security Measures).
4. Engage sub-processors only with the Controller's general written authorisation, with 30 days' notice of changes.
5. Assist the Controller in fulfilling data-subject requests (access, rectification, erasure, portability) within reasonable timeframes.
6. Notify the Controller without undue delay (and in any case within 24 hours) of becoming aware of a Personal Data breach.
7. Make available to the Controller all information necessary to demonstrate compliance, including the Trust Center evidence at `/trust` and the audit pack available on demand.

7. Sub-processors

The Processor uses the sub-processors listed at the Trust Center page. The current list includes MongoDB Atlas (database), Stripe (payments), Gmail SMTP (email), Twilio (SMS), Emergent Cloud (hosting), and Cloudflare (DNS / DDoS / CDN). The Controller's authorisation of this Agreement constitutes general written authorisation; the Processor shall give 30 days' notice before adding any new sub-processor.

8. International data transfers

Personal Data may be processed in any of the regions where sub-processors operate, including the United States and the European Union. The Processor warrants that all transfers are subject to adequate safeguards, including Standard Contractual Clauses (SCCs) where required by the Controller's jurisdiction.

9. Data retention & deletion

- **Clinical case data**: retained for 7 years after case completion, in line with dental record-keeping norms.
- **Anonymous case quotes**: retained for 6 months for re-engagement.
- **Backups**: 30-day rolling retention, encrypted with separate KMS keys.
- **Audit logs**: indefinite retention; hash-chained for tamper evidence.
- Upon Controller request or termination, Personal Data shall be returned or deleted within 30 days, except where retention is required by Applicable Law.

10. Security measures (Annex A)

- TLS 1.2+ encryption in transit; HSTS preload enabled
- AES-256 encryption at rest (MongoDB Atlas managed)
- bcrypt cost-12 for password storage; HS256/RS256 for session tokens
- Multi-tenant row-level filter (`tenant_id`) on every database query
- Role-based access control with least-privilege defaults (10 distinct roles)
- Hash-chained immutable audit log; integrity verified continuously
- HTTP security headers: HSTS, CSP, X-Frame DENY, X-Content-Type-Options, Referrer-Policy, Permissions-Policy
- Rate-limiting on authentication and case-submission endpoints
- Daily encrypted backups with 30-day retention
- Incident response runbook with 24-hour breach notification SLA

11. Data subject rights

The Processor provides the Controller with mechanisms to fulfil data-subject rights including: access (read endpoints), rectification (edit endpoints), erasure (`DELETE /api/privacy/delete-account`), and data portability (CSV exports of case history).

12. Liability & indemnity

Each Party shall be liable for damages caused by its own breach of this Agreement, subject to the liability caps in the Service Agreement. Where joint liability arises under Applicable Law, the Parties shall apportion responsibility based on their respective contribution to the harm.

13. Governing law

This Agreement shall be governed by the laws of the State of Qatar. Disputes shall be subject to the exclusive jurisdiction of the courts of Doha, Qatar. Where the data subject is located in the EU or US, this clause does not derogate from the data subject's right to lodge a complaint with their local supervisory authority.

14. Signatures

FOR THE CONTROLLER · [CONTROLLER — TO BE FILLED BY SIGNER]

Name & title:

Signature:

Date:

FOR THE PROCESSOR · TOOTHROCKET LABS

Name & title:

Signature:

Date:

Annex B — Document integrity fingerprint

This SHA-256 covers the canonical issuance metadata for this DPA copy. Re-issuing with identical inputs produces the same fingerprint. After both parties counter-sign, retain this fingerprint with the signed copy for future verification.

```
SHA-256 = 189862c7de173663699579b1ed6dfe2c8ecdefc5d23f83193c341221f5987358
```

Questions about this DPA? **dpo@toothrocket.com** · **security@toothrocket.com**