Picca – Data Privacy & Ethical UX (Public v0.1)

> **Purpose** State the non-confidential guarantees Picca makes around privacy, fairness, and user experience so that external contributors (and Codex-1) build against the same baseline.

---

1. Privacy Commitments (MVP)

Principle	Implementation	Public Proof Point
Keypoints-only pipeline	MediaPipe → 34-vector → discard RGB	No RGB objects survive beyond RAM
24 h purge	Cloud Storage lifecycle rule (`tmp/*`, TTL=24 h)	`gsutil lifecycle get` log exposed
Region-locked storage	Buckets & SQL in `asia-northeast1` only	Terraform `location=` pinned
Anonymised telemetry	SHA-256(user-UUID) before export	Sample hash in `infra/telemetry.tf`
Right-to-delete API	`DELETE /api/v1/user/:id` hard-purges keys	Contract in `openapi.yaml`

Full DPIA & RoPA tables are internal and excluded from this extract.

---

2. Bias & Fairness Guardrails

1. **Training diversity pledge** — Min. 30 % data from under-represented kinetic profiles.
2. **Nightly SHAP audits** — Cloud Run Jobs auto-post Δ重要度 to `audit-events`.
3. **Goodhart Sentinel** — p-hack detector flags metric drift > 5 %.
4. **Community RFC** — New metrics require a public RFC with bias analysis section.

---

3. Explainability & Transparency

- Every score returns: `{ "score": 87, "explain": { "symmetry": 0.91, "power": 0.88 } }`.
- `GET /api/v1/audit/:run_id` surfaces full SHAP vector for 7 days.
- 400/403 responses include `reason_code` + doc link.

---

4. Dark-Pattern Policy (UX)

Area	Rule	Example
Consent	**Explicit opt-in** only	No pre-ticked share boxes
Feedback	**Honest latency**	Progress bar bound to p95 latency
Gamification	**No blind loops**	Reveal scoring rubric after 1st run
Monetisation	**No pay-to-pass**	Scores unaffected by subscription tier

---

5. Compliance Matrix (Abridged)

Requirement	GDPR (EU)	個人情報保護法 (JP)	Status
Data minimisation	Art.5-1(c) ✓	第16条-1 ✓	Keypoints only
Right to erasure	Art.17 ✓	第30条 ✓	`DELETE` API live
Breach notice	Art.33 (72 h) ✓	第22条-2 ✓	24 h SLA

---

6. Incident Response (Public SLA)

- **Detect** anomaly ≤ 4 h (log-based alerting)
- **Contain** access & rotate secrets ≤ 8 h
- **Notify** affected users & publish RCA ≤ 24 h

Last updated 2025-07-08