EU AI Act Face Recognition Compliance Checklist

Twelve questions to answer before deploying any face feature in the EU.

1. Classification

- [ ] Does the system identify or verify a person by face?
- [ ] If only detection: no AI Act / Annex III obligations.
- [ ] If recognition: classified as high-risk under Annex III.

2. Article 5 prohibition check

- [ ] Not built from untargeted scraping of web/CCTV.
- [ ] Not deployed for workplace or school emotion recognition.
- [ ] Not used to categorize by race, religion, orientation.
- [ ] Not real-time public identification by law enforcement.

3. GDPR Article 9 lawful basis

- [ ] Explicit consent collected (written / signed / recorded).
- [ ] Consent revocable at any time without detriment.
- [ ] Consent log persisted with per-purpose granularity.

4. Data minimization

- [ ] Raw pixels discarded after the embedding is produced.
- [ ] Smallest embedding dim that solves the task chosen.
- [ ] Storage segregated by purpose (hot / cold / forensics).

5. Retention policy

- [ ] Per-purpose retention period documented in writing.
- [ ] Automatic deletion job runs and is monitored.
- [ ] Right-to-erasure handler tested end-to-end.

6. Liveness / anti-spoofing

- [ ] Passive liveness model trained or licensed.
- [ ] iBeta PAD certification path planned (high-stakes).

7. Article 9 — Risk management (AI Act)

- [ ] Risk register with owner per risk, mitigation evidence.
- [ ] Quarterly re-review scheduled.

8. Article 10 — Data governance

- [ ] Training/validation sets relevant and representative.
- [ ] Demographic accuracy parity tested (NIST FRVT or equiv).
- [ ] Bias metrics published in technical documentation.

9. Article 11 — Technical documentation

- [ ] Annex IV dossier: purpose, architecture, datasets, metrics.
- [ ] Instructions-for-use document for deployers prepared.

10. Article 12 — Record-keeping

- [ ] Tamper-evident log of every identification decision.
- [ ] Model version and threshold changes logged.

11. Article 14 — Human oversight

- [ ] Human review on every consequential match before action.
- [ ] Reviewer UI surfaces source frame, template, confidence.
- [ ] No fully automated denial / arrest / contract decision.

12. Articles 27 + 49 — FRIA + EU registration

- [ ] Fundamental Rights Impact Assessment completed.
- [ ] System registered in EU database before deployment.
- [ ] Article 50 transparency notice shown to end users.