Proctoring Data & Privacy Compliance Checklist

A one-page gate to run before a proctored exam ships. Engineering guidance, not legal advice — confirm specifics with qualified counsel.

A. Lawful basis & consent

- [ ] State an explicit lawful basis for capturing face, room, audio, and screen
- [ ] Collect informed consent before any capture; electronic consent is fine (BIPA SB 2979, 2024)
- [ ] In the EU, offer a genuine non-proctored alternative so consent is freely given (GDPR Art 7)

B. Impact assessment & vendor agreement

- [ ] File a Data Protection Impact Assessment before processing (GDPR Art 35)
- [ ] Sign a written data-processing agreement with the proctoring vendor (GDPR Art 28)
- [ ] For US student records, confirm the vendor fits the FERPA school-official exception
- [ ] For US storage of EU data, confirm a valid transfer mechanism (post Schrems II)

C. Data minimization at capture

- [ ] Capture the fewest signals needed; avoid a room scan unless truly necessary
- [ ] Rule out any emotion / stress inference — prohibited in EU education (AI Act Art 5)
- [ ] Encrypt recordings at rest and in transit; restrict who can access them

D. Retention & destruction

- [ ] Publish a written retention schedule (BIPA 15(a); GDPR storage limitation)
- [ ] Wire automatic deletion on schedule — do not leave destruction manual

E. Human review & high-risk duties

- [ ] A human reviews every flag with context; no flag auto-fails a learner (GDPR Art 22)
- [ ] Provide a documented appeal route for any flagged decision
- [ ] If you build proctoring AI, meet EU AI Act high-risk duties: logging, oversight, accuracy