**Regulatory Pillars Snapshot**

**GDPR + EU AI Act for Institut Premià de Mar**

**(Capstone - Module 10A)**

# 1) What each law covers

**GDPR (data lens):** governs personal data. Requires lawful basis, transparency, data minimisation, security, rights handling (access/erasure) and extra care for special-category data (e.g. health).

**EU AI Act (system lens):** governs AI systems by risk level. Sets rules for risk management, data & model governance, human oversight, technical documentation, post-market monitoring, and transparency (including for general-purpose AI).

*Together: GDPR protects the data you use; the AI Act governs the AI system & its impacts. Any school AI project that touches student/teacher data must satisfy both.*

# 2) Timeline we must plan against

* Prohibited practices + AI literacy duties: apply from early 2025.
* General-Purpose AI (e.g., large language models): obligations from August 2025.
* High-risk AI (Annex III: education uses): obligations from August 2026 (some safety-component cases until August 2027).

# 3) Education = “High-risk” (what that means for us)

High-risk includes AI used to evaluate learners, allocate access to education or programs, or determine student profiling/outcomes. If we deploy such systems, we must have:

* Risk management & testing before use
* Human oversight procedures (who checks, when to override)
* Data/record-keeping & technical documentation awareness (from vendor)
* Post-market monitoring (logs, performance checks, bias detection)
* Clear transparency to students/parents (plain-language notices)
* Trained staff (role-specific AI literacy; avoid automation bias)

# 4) Quick compliance map (use in your Capstone appendix)

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **GDPR (data)** | **EU AI Act (system)** | **Where we show this in the portfolio** |
| Lawful basis, minimisation, DPIA (if needed) | ✅ | — | Legal mapping (Module 2), DPIA notes |
| Transparency to users | ✅ | ✅ | Transparency notice & comms plan (Module 6) |
| Human oversight | — | ✅ (oversight article) | Role-specific training + SOP (Modules 7 & 9) |
| Technical docs awareness | — | ✅ (vendor tech file) | Vendor evaluation + IT runbook (Modules 5 & 7) |
| Monitoring & incident handling | ✅ (security/breach) | ✅ (post-market & serious incidents) | Monitoring plan + Incident Response (Modules 7 & 8) |
| Staff AI literacy | — | ✅ (deployer duty) | Training needs + Continuous Learning Framework (Module 9) |

# 5) What we’ve already prepared (plug into Capstone)

* Governance Policy & RACI (roles, decision rights)
* Vendor & Product Evaluation (checklist + contract asks)
* Transparency Pack (student/parent notices, scripts)
* Monitoring & Audit Kit (KPIs, sampling, bias checks)
* Incident Response Plan (classification, notifications)
* Training Suite (needs assessment, role plans, student curriculum, continuous learning)

# 6) 30-day actions to be “capstone-ready”

1. Pick/confirm the pilot AI system and its risk category (document in inventory).
2. Publish/update transparency notice for the pilot (before first use).
3. Run targeted staff training for roles overseeing the pilot; log attendance.
4. Start monitoring log (outputs sampled, issues, overrides, actions).
5. Do a tabletop incident drill (capture who-does-what, within 30-60 min).
6. Link all evidence in GitHub (README index → modules & artifacts).

# 7) Ownership at Institut Premià de Mar

* AIGO (me): overall framework, training, oversight SOPs, evidence trail
* Principal/Leadership: approval, resources, accountability
* DPO: GDPR alignment (lawful basis, DPIA, rights, breach)
* IT Lead: integration, security, logs, vendor tech docs
* Dept Heads/Teachers: day-to-day oversight, transparency in class