**Assignment: Notification & Reporting Pack (GDPR + EU AI Act)**

**Module 8E**

**Context:** Spanish secondary school (ESO-Bachillerato, ages 12–18) placed in Premià de Mar, Barcelona. DPA is the **AEPD** (Agencia Española de Protección de Datos). The national AI **Market Surveillance Authority (MSA)** is being designated; add the current competent authority link your school uses once confirmed by your region/Ministry.

**1) Notification Decision Log**

*(Once per incident used. Has to be concise. This is the accountability trail.)*

**Incident title:**  
**Date/time discovered (local):**  
**Who reported it:**  
**System involved (vendor/version):**  
**Summary (3–4 lines):**

**Does personal data appear involved?** ☐ Yes ☐ No ☐ Unsure  
**Potential harm to rights/freedoms (GDPR risk)?** ☐ Low ☐ Medium ☐ High  
**High-risk AI system implicated?** ☐ Yes ☐ No ☐ Unsure  
**Possible “serious incident” (AI Act) indicators present?**

* Fundamental rights impact (fairness, non-discrimination, access to education): ☐
* Serious harm to health/safety: ☐
* Other criteria (describe):

**Provisional classification (from 8C matrix):** ☐ Level 1 ☐ Level 2 ☐ Level 3 (Serious) ☐ Level 4 (Critical)

**Provisional decisions (tick all that apply):**

* ☐ Start GDPR 72-hour assessment window (Article 33) - *timer started: (date/time)*
* ☐ Notify AEPD required (risk likely)
* ☐ Notify data subjects required (high risk)
* ☐ AI Act “serious incident” suspected - inform provider immediately; start 15-day report clock
* ☐ Law enforcement / child protection notified (if applicable)
* ☐ Containment actions taken (list):

**Decision rationale (5-8 lines):**

**Approvals:**

* Incident lead:
* DPO (or privacy lead):
* Head of school / SLT:

**Follow-ups & deadlines:**

* DPA notification due by:
* AI Act preliminary report due by:
* Parent/student comms by:

**2) GDPR Breach Assessment and Notification Form**

*(It covers Articles 33–34. Plain language used. Logs/screens attached as needed.)*

**Controller (school):**  
**DPO / contact:**  
**Processor(s) involved (vendors):**

**Nature of the breach** (confidentiality/integrity/availability; how detected; when it began/ended):

**Categories & volume of data affected**

* Data subjects: students / staff / parents (estimate #):
* Data types: names, contact details, grades, SEN info, IDs, recordings, other:
* Special category data involved? ☐ Yes ☐ No ☐ Unknown (describe):

**Likely risk to rights/freedoms** (low/medium/high) and reasoning:

**Immediate containment & mitigation** (what you did within first hours):

**Further measures to address breach** (technical/organisational; vendor actions):

**Article 33 - Supervisory authority notification (within 72h)**

* Required? ☐ Yes ☐ No (give rationale if “No”)
* If Yes: date/time submitted; reference #; channel (AEPD form/portal/email):

**Article 34 - Communication to data subjects (if high risk)**

* Required? ☐ Yes ☐ No (rationale; if encryption or other exception applies, explain)
* If Yes: method (email/letter/portal), date/time sent, who received, support offered:

**Information provided to individuals** (copy/paste the text or attach within report):

* What happened; what data; risks; what we’re doing; how they can protect themselves; DPO contact.

**Evidence & logs attached:** ☐ Yes (list) ☐ No (why)

**Sign-off:** DPO / Headteacher / Legal

**3) AI Act Serious Incident Preliminary Report**

*(Use when a* ***high-risk AI*** *system is causally linked to a “serious incident”. Provider reports to the MSA; as deployer, notify the provider immediately and may assist/submit if required.)*

**Provider name & contact:**  
**Deployer (school):**   
**System name & version; conformity info (if known):**  
**Use case (education context):** grading/admissions/placement/analytics/other

**Incident date/time & location:**  
**Description** (facts; suspected causal link to the AI; how detected):

**Consequences observed**

* Health/safety impact (if any):
* **Fundamental rights impact** (fairness, non-discrimination, access to education, privacy):
* Number of affected persons; vulnerable groups (minors):

**Immediate measures taken by deployer** (containment, suspension, human review):  
**Immediate measures requested/initiated by provider** (patches, rollback, withdrawal):

**Known/suspected root cause** (if unknown, state investigation ongoing):

**Risk of recurrence / spread:**

**Reporting timeline**

* Date provider/deployer became aware:
* **Preliminary report submitted:** [date] (≤15 days)
* **Final report due/target:** [date]

**Attachments** (logs, screenshots, test cases, oversight records):

**Contacts**

* Provider incident lead: (X)
* School incident lead: (X)
* DPO: (X)

**Signature** (provider/deployer, as applicable)

**4) Incident Contacts and Timers**

*(To be filled once only. Copies kept for every new incident.)*

**A. Key contacts**

* **DPO / Privacy Lead:** name | phone | email
* **Incident Lead (AI/IT):**
* **Head of School / SLT:**
* **Communications Officer:**
* **Safeguarding Lead:**
* **Legal Counsel (if any):**

**Supervisory Authority (GDPR) - AEPD**

* Web: (school link)
* Phone / email for breach notifications: +34 XX XXX XX XX / x@x

**AI Market Surveillance Authority (MSA)**

* Name (once designated): (X)
* Contact / portal: (X)

**Law enforcement / child protection**

* Local Police / Mossos: (X)
* Child protection service: (X)

**Vendors / Providers (top 5 AI tools)**

* Tool A: name | 24/7 incident contact | escalation path
* Tool B: …

**B. Timers & clocks (checklist)**

* ☐ **Start 72-hour GDPR clock** when aware of a *likely-risk* personal data breach: ***/***/\_\_\_\_:
* ☐ **Start 15-day AI Act clock** when a *serious incident* linked to high-risk AI is suspected: ***/***/\_\_\_\_:
* ☐ Record **time of containment** and **time of first comms** to stakeholders.
* ☐ Calendar reminders set (DPA draft due, MSA preliminary due, parent letters due).

**C. One-page decision tree (share with the whole team)**

Incident detected

├─ Personal data involved? ── Yes ──> Risk to rights/freedoms likely?

│ ├─ Yes → Notify AEPD ≤72h; consider data subject notice (Art.34)

│ └─ No → Log internally; document rationale (no notify)

│

└─ High-risk AI implicated? ── Yes ──> Serious incident indicators?

├─ Yes → Provider (or deployer if needed) informs MSA ≤15 days

└─ No → Log; monitor; consider provider ticket

Always: contain, document, support affected, brief leadership, plan comms.