



Embed AI

AI ACT READINESS REPORT · 2026

Version 2026.09

2026-09-10 · Practical guide

ANNEX III POINT 3

AI in education and training

Admission, assessment, examination and proctoring,
fair and demonstrable.

Admission

Assessment

Proctoring

Bias and explainability

Legal reference date: 2026-09-10 · Practical guide, not formal legal advice.

FOREWORD FROM THE EXPERT

AI in education and training.

AI used for admission, placement, assessment, examination and proctoring in education and vocational training falls under Annex III point 3 of the EU AI Act (Regulation (EU) 2024/1689) and is therefore considered high-risk in principle.

Zahed Ashkara guides organisations from AI Act obligation to review-ready evidence. This report captures that approach per domain, so your deployment is explainable and defensible towards supervisors and customers.

What this report is

- A practical readiness guide per domain or route
- An explanatory layer on the relevant AI Act articles
- A framework to build evidence

What this report is not

- Formal legal advice or a conformity assessment
- A replacement for DPIA, FRIA or vendor due diligence
- A guarantee of compliance

TABLE OF CONTENTS

What is inside this report.

-
- 01** **Executive summary**
 -
 - 02** **Why education AI is high-risk and what exactly is covered**
 -
 - 03** **Are you a provider or a deployer? Role determination is the foundation**
 -
 - 04** **The Article 6(3) test: is your system really high-risk?**
 -
 - 05** **Human oversight, transparency and students' rights**
 -
 - 06** **Bias, accuracy and the particular risks of proctoring**
 -
 - 07** **AI literacy, logging and the review-ready file**
 -
 - 08** **The obligations at a glance**
 -
 - 09** **Evidence pack: the checklist**
 -
 - 10** **Roadmap: 30, 60, 90 days**
 -
 - 11** **Frequently asked questions**
 -
 - 12** **About the expert**
 -

KEY POINTS

AI in education and training.

AI used for admission, placement, assessment, examination and proctoring in education and vocational training falls under Annex III point 3 of the EU AI Act (Regulation (EU) 2024/1689) and is therefore considered high-risk in principle. Four categories are covered: systems that determine access or admission or assign individuals to institutions (point 3(a)), systems that evaluate learning outcomes or steer the learning process (point 3(b)), systems that assess the appropriate level of education a person will receive or be able to access (point 3(c)), and systems that monitor and detect prohibited behaviour by students during tests, in other words proctoring (point 3(d)). Because these uses directly affect access to education, obtaining qualifications and therefore people's life chances, the legislator places them under heightened obligations.

Status at 10 September 2026. Regulation (EU) 2026/1744 is in force. Chapter III, Sections 1 to 3 duties for high-risk AI under Article 6(2) and Annex III apply from 2 December 2027, except Article 6(5). Assess Article 111 transitional rules separately for existing systems. Article 4 and applicable prohibitions already apply; applicable Article 50 duties have applied since 2 August 2026. Paragraph 2 has a transition until 2 December 2026 only for systems placed on the market before 2 August 2026.

FINDING 01**Why education AI is high-risk and what exactly is covered**

Annex III point 3 names four narrowly defined uses in education and vocational training at all levels.

FINDING 02**Are you a provider or a deployer? Role determination is the foundation**

The weight of your obligations depends on your role under the Regulation.

FINDING 03**The Article 6(3) test: is your system really high-risk?**

Annex III places education AI in the high-risk category in principle, but Article 6(3) provides a narrow exception.

FINDING 04**Human oversight, transparency and students' rights**

Article 26 obliges you as deployer to assign human oversight to natural persons with the necessary competence, training and authority.

IN CONTEXT

Where you stand in the AI Act.

Annex III point 3
TOPIC

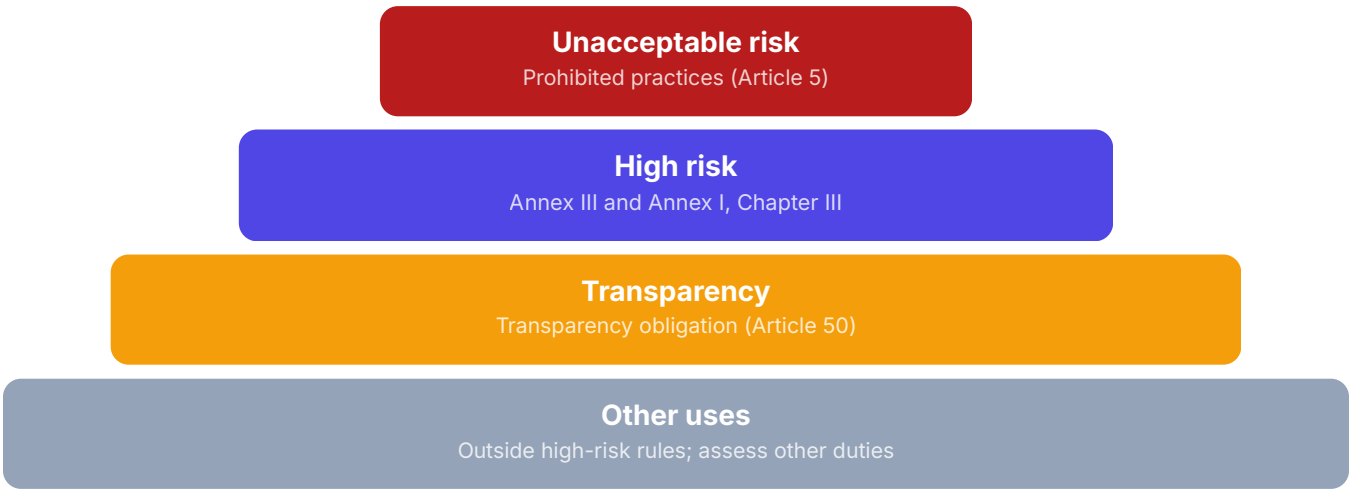
2 dec 2027
ANNEX III: CH. III,
SECTIONS 1-3

6
POINTS TO ASSESS

30 / 60 / 90
PLANNING CADENCE
IN DAYS

This concerns duties for systems under Article 6(2) and Annex III, except Article 6(5). First assess classification and any Article 111 transition. Articles 4, 5 and 50 may already apply.

THE AI ACT RISK PYRAMID



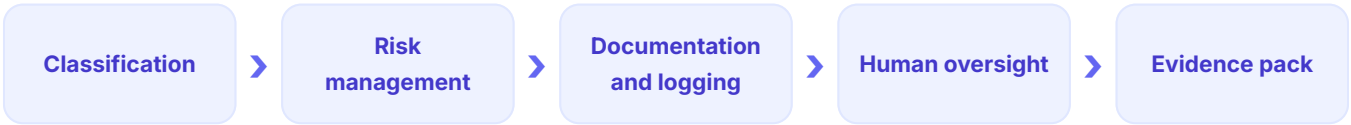
Schematic routes, not mutually exclusive categories: Article 50 can also apply to a high-risk system. Chapter V is a separate route for GPAI model providers. Start with actual use and your role.

THE REGULATION TIMELINE

2 feb 2025	Prohibited practices and AI literacy
2 aug 2025	GPAI model duties; see transition for existing models
27 jul 2026	Omnibus in force; amended AI literacy duty
2 aug 2026	Article 50 applies; GPAI enforcement active
2 dec 2026	Article 50(2) transition ends, only systems before 2 Aug 2026
2 aug 2027	GPAI models placed on the market before 2 Aug 2025
2 dec 2027	Chapter III, Sections 1-3: Article 6(2) / Annex III
2 aug 2028	Chapter III, Sections 1-3: Article 6(1) / Annex I

Chapter III: exception for Article 6(5). Also check Article 111 for each system. This overview is not a uniform deadline for all AI.

FROM OBLIGATION TO EVIDENCE



WHO CARRIES WHICH OBLIGATION

The following allocation concerns high-risk systems where the duty applies. Classification, role and transition determine the outcome.

Provider

Develops or has the system developed and places it on the market or puts it into service under its own name

- Chapter III: risk management, data and documentation (Art. 9 to 15)
- Conformity assessment and CE marking
- Registration under Art. 49: EU or national, where applicable

Deployer

Uses the system under its own authority

- Use per instructions and monitoring (Art. 26)
- Human oversight and log retention
- Fundamental rights assessment where required (Art. 27)

CHAPTER 02

Why education AI is high-risk and what exactly is covered

Annex III point 3 names four narrowly defined uses in education and vocational training at all levels. Point 3(a) concerns AI that determines access, admission or the assignment of individuals to educational and vocational training institutions. Point 3(b) covers AI that evaluates learning outcomes, including where those outcomes are used to steer the learning process. Point 3(c) addresses AI that assesses the appropriate level of education a person will receive or be able to access. Point 3(d) specifically concerns systems that monitor and detect prohibited behaviour by students during tests, the legal core of proctoring.

The legislator classifies these uses as high-risk because they shape the course of someone's education and career path. A wrongful rejection at admission, a biased automated assessment of an exam, or a false positive in a proctoring system has direct and sometimes irreversible consequences for an individual. It is precisely this type of decision with lasting impact on fundamental rights and life chances that the Regulation places under heightened obligations.

Importantly, the classification is functional and does not depend on the product's name. A 'study advice tool', an 'automated marking assistant' or an 'online invigilation solution' falls under point 3 as soon as its actual function matches one of the four descriptions. Always start, therefore, with what the system does in your process, not with what the vendor calls it.

EXAMPLE FROM PRACTICE

A university of applied sciences uses a dashboard that flags students with an 'elevated drop-out risk' based on interim results, after which student counsellors prioritise those students. Because the system evaluates learning outcomes and thereby steers the learning process, it falls under Annex III point 3(b). The institution initially thought it was 'just a tool', but had to build the full deployer file because the flags effectively influenced support and therefore students' chances.

CHAPTER 03

Are you a provider or a deployer? Role determination is the foundation

The weight of your obligations depends on your role under the Regulation. Most educational institutions and examination bodies are deployers: you purchase or license an AI system and use it under your responsibility. Your obligation framework is then mainly Article 26, on top of which come Article 4 (AI literacy) and the transparency duties towards students.

A provider develops an AI system or has it developed and places it on the market or puts it into service under its own name or trademark. A deployer uses a system under its own authority in a professional context. Article 25 can transfer high-risk system provider status through rebranding, a

substantial modification that leaves the system high-risk, or a change of intended purpose that makes a previously non-high-risk system high-risk. Routine configuration or fine-tuning does not automatically change the role; assess the actual modification.

Role determination is not a formality but decides which file you must be able to produce. Therefore record in writing, per system, who is the provider and who is the deployer, which vendor contracts apply, and which responsibilities are contractually allocated. Where responsibility is shared or assumed, an explicit agreement with the vendor is essential to avoid unintentionally carrying the heavier duties.

CHAPTER 04

The Article 6(3) test: is your system really high-risk?

Annex III places education AI in the high-risk category in principle, but Article 6(3) provides a narrow exception. A system is not high-risk where it does not pose a significant risk to health, safety or fundamental rights and does not materially influence the outcome of decision making. This may be the case where the system performs only a narrow procedural task, merely improves the result of a previously completed human activity, only detects decision-making patterns without replacing human assessment, or performs a preparatory task.

This exception is deliberately narrow. A system that effectively drives an exam assessment, ranks an admission decision, or generates a proctoring alert that leads to consequences does influence the outcome and remains high-risk. A purely administrative aid, such as a tool that anonymises or merely formats answers without touching the assessment, may fall under the exception. The line lies in whether the human assessor genuinely decides freely and on an informed basis, or in practice adopts the system's suggestion.

Article 6(3) concerns only systems listed in Annex III. The assessment must establish no significant risk to health, safety or fundamental rights and at least one statutory condition: a narrow procedural task, improvement of completed human work, detection of decision patterns or deviations with proper human review, without replacing or improperly influencing the previous assessment, or preparation for a relevant assessment. Profiling of natural persons rules out the exception. The provider documents the assessment before market placement or putting into service under Article 6(4) and registers under Article 49(2). The deployer can request that reasoning from its supplier.

EXAMPLE FROM PRACTICE

An examination body uses a tool that pre-sorts open answers by text length and language, purely to help distribute work among human markers, with no substantive scoring. After a reasoned Article 6(3) assessment recorded in a memo and registered under Article 49(2), the body concludes that this is a procedural task that does not influence the outcome. A second tool that does propose a draft grade remains high-risk, because markers in practice almost always adopt that grade.

Human oversight, transparency and students' rights

Article 26 obliges you as deployer to assign human oversight to natural persons with the necessary competence, training and authority. For education this means that a qualified teacher, examiner or admissions officer can genuinely understand, weigh and overrule the system's output, and that this person also has the mandate to do so. Oversight that exists in name but in practice amounts to rubber-stamping the system's outcome does not suffice.

In addition, Article 26 requires you to inform the persons concerned when a high-risk system is used to take or support decisions about them. Students and candidates must therefore know that an AI system co-decides on their admission, assessment or proctoring. Where the system is used towards staff or interns in a workplace context, there is also a duty to inform workers and their representatives in advance.

The Regulation does not operate in a vacuum. Almost every educational use also rests on a GDPR legal basis, often with a data protection impact assessment. Proctoring is the sharpest example here: continuous video and audio capture, sometimes behavioural analysis, touches special categories of personal data and students' privacy in their own homes. Therefore combine your AI Act file with your GDPR documentation, and ensure proportionality, less intrusive alternatives and retention periods are demonstrably weighed.

Bias, accuracy and the particular risks of proctoring

Education AI is sensitive to systematic bias. Assessment models may unintentionally favour certain writing styles, languages or backgrounds; admission systems may reproduce historical inequality in training data. For high-risk systems the Regulation requires, through the data governance and accuracy requirements (Articles 10 and 15), that datasets are relevant and sufficiently representative and that the system achieves an appropriate level of accuracy and robustness. As a deployer with control over input data, you must under Article 26 ensure that data is appropriate for the intended purpose.

Proctoring deserves particular attention because the cost of errors is asymmetric and visible. A false positive, where an honest student is wrongly suspected of cheating, leads to a serious accusation and possibly an invalidated exam. Known risks include poorer face detection for darker skin tones, false alarms for neurodivergent students or students with a disability, and problems caused by poor connections or shared living spaces. These risks must be explicitly named and mitigated in your risk analysis.

The practical conclusion is that human re-assessment in proctoring is not a final step but a core safeguard. Every alert that leads to an accusation or consequence should be reviewed by a competent person, with access to the evidence, a right to be heard for the student and a documented outcome. Record how many alerts turn out to be false positives, because those figures are the evidence that your safeguards work and are exactly what a supervisory authority or complaints committee will request.

EXAMPLE FROM PRACTICE

After an exam round a university receives several complaints from students flagged by the proctoring system for 'looking away', who turned out to be students with a visual impairment and students in cramped living rooms. Because the institution had set up human re-assessment with a right to be heard for each flag and tracked false-positive figures, it could reject the flags, adjust the policy and demonstrate that the human safeguard genuinely functioned.

CHAPTER 07

AI literacy, logging and the review-ready file

Since 2 February 2025 Article 4 applies. Since 27 July 2026, providers and deployers must take suitable measures that support the development of AI literacy; they do not have to guarantee a specific individual level. For education, role-based training for admissions staff, examiners, teachers and proctoring supervisors can be a suitable measure. Attendance and completion records help substantiate the approach.

Article 26(6) requires the deployer to retain automatically generated logs insofar as they are under its control. Choose an appropriate period of in principle at least six months, unless applicable Union or national law provides otherwise, including data protection law. Do not retain data longer than needed without a purpose or legal basis.

A coherent dossier connects the system inventory, classification, roles, risk assessment, information to students, log policy, human oversight and evidence of AI literacy measures. The quality and actual operation of safeguards remain decisive. Use the checklist to identify missing evidence and assign an owner to each open point.

The obligations at a glance

1

Annex III point 3 (a) to (d)

Classify as high-risk any system that determines access or admission or assigns individuals to institutions (3a), evaluates learning outcomes or steers the learning process (3b), assesses the appropriate level of education (3c), or monitors and detects prohibited behaviour by students during tests, i.e. proctoring (3d).

2

Article 6(3) and Article 49(2)

Article 6(3) concerns only systems listed in Annex III. The assessment must establish no significant risk to health, safety or fundamental rights and at least one statutory condition: a narrow procedural task, improvement of completed human work, detection of decision patterns or deviations with proper human review, without replacing or improperly influencing the previous assessment, or preparation for a relevant assessment. Profiling of natural persons rules out the exception. The provider documents the assessment before market placement or putting into service under Article 6(4) and registers under Article 49(2). The deployer can request that reasoning from its supplier.

3

Article 26

As deployer, assign competent human oversight, use the system in line with its instructions, ensure appropriate input data where you control it, monitor operation, retain the automatically generated logs for in principle at least six months, and inform the students and candidates concerned that an AI system co-decides about them.

4

Articles 9, 10, 11, 12, 13, 14 and 15

If you become a provider, for example through own development, substantial modification or use under your own name, comply with risk management, data governance, technical documentation, logging, transparency, human oversight and accuracy and robustness, concluded with a conformity assessment.

5

Article 4

Take measures that support the development of AI literacy among staff and third parties operating or using the systems on your behalf, taking account of role, experience, education, context and affected people. Record the measures without guaranteeing an individual outcome.

6

Article 99

For breaches of the other duties listed there, Article 99 sets a maximum of EUR 15 million or 3% of worldwide annual turnover for the preceding financial year. For SMEs, including start-ups, the lower of amount and percentage applies; for other undertakings, the higher. A fine is not automatic: the authority assesses the circumstances. Member States determine whether and to what extent such fines apply to public bodies.

Evidence pack: the checklist

- ✓ System inventory of all AI applications in admission, placement, assessment, examination and proctoring, with intended purpose and vendor
- ✓ Written Article 6(3) classification assessment per system, with registration evidence under Article 49(2) where the exception is invoked
- ✓ Provider versus deployer role determination per system, substantiated with vendor contracts and allocation of responsibilities
- ✓ Bias and fundamental rights analysis addressing data representativeness and known proctoring risks such as false positives for students with a disability
- ✓ Transparency information to students and candidates, plus information to workers and their representatives where used in a workplace context
- ✓ Logging policy aligned with examination regulations and objection and appeal deadlines, with a retention period of in principle at least six months
- ✓ Protocol for human oversight and re-assessment, including the right to be heard and recording of false-positive proctoring alerts
- ✓ AI literacy evidence (training overview, attendance and completion records) for all roles involved

Roadmap: 30, 60, 90 days

Indicative planning cadence. Feasibility depends on scope, existing measures and available evidence.

0 to 30 days

- Draw up a system inventory of all AI in admission, assessment, examination and proctoring, including shadow IT and vendor modules
- Determine for each system the provider or deployer role and gather the associated vendor contracts and instructions for use
- Carry out an initial Article 6(3) screening to establish which systems are high-risk and which may fall under the exception
- Appoint an owner for the AI Act file and connect this to the existing GDPR and examination committee structure

30 to 60 days

- Record the Article 6(3) assessments in writing and register systems where necessary in accordance with Article 49(2)
- Set up the human oversight protocol with competent re-assessment, the right to be heard and escalation, with special attention to proctoring alerts
- Carry out the bias and fundamental rights analysis and align it with the GDPR data protection impact assessment
- Draft transparency texts for students, candidates and, in workplace contexts, workers and their representatives

60 to 90 days

- Implement the logging policy and align retention periods with examination regulations and objection and appeal deadlines
- Roll out targeted AI literacy training for admissions staff, examiners, teachers and proctoring supervisors and record evidence
- Bundle all components into a single review-ready file and test it with an internal dry run as if a supervisory authority or complaints committee requested it
- Plan a periodic review cycle so that classification, false-positive figures and vendor changes remain current

Frequently asked questions

Does every learning platform or piece of educational software with AI automatically fall under high-risk?

No. Only uses that match one of the four descriptions in Annex III point 3 are high-risk in principle: access or assignment, evaluation of learning outcomes or steering the learning process, assessment of the level of education, or proctoring. A pure content library or administrative aid usually falls outside this, but always assess the actual function within your process.

We purchase a proctoring tool from a vendor. Are we still responsible?

Yes. As a user you are the deployer and carry the duties of Article 26, including human oversight, monitoring, log retention and informing students. The vendor carries the provider duties for the system itself, but that does not relieve you of your own responsibility. Set out the role allocation clearly in the contract.

Does the fundamental rights impact assessment of Article 27 also apply to education?

Yes: Article 27 can apply where an educational institution is a body governed by public law or a private entity providing public services and deploys an Annex III high-risk system. Education is not excluded. The duty follows the applicable high-risk date. Separately assess whether GDPR Article 35 requires a DPIA; align the assessments where both are needed.

Can we rely on the Article 6(3) exception to avoid the heavy duties?

Article 6(3) concerns only systems listed in Annex III. The assessment must establish no significant risk to health, safety or fundamental rights and at least one statutory condition: a narrow procedural task, improvement of completed human work, detection of decision patterns or deviations with proper human review, without replacing or improperly influencing the previous assessment, or preparation for a relevant assessment. Profiling of natural persons rules out the exception. The provider documents the assessment before market placement or putting into service under Article 6(4) and registers under Article 49(2). The deployer can request that reasoning from its supplier.

How long must we retain the logs and the evidence?

Article 26(6) requires the deployer to retain automatically generated logs insofar as they are under its control. Choose an appropriate period of in principle at least six months, unless applicable Union or national law provides otherwise, including data protection law. Do not retain data longer than needed without a purpose or legal basis.

ABOUT THE EXPERT



Zahed Ashkara

AI Act consultant · AI governance specialist · lawyer and speaker

Zahed Ashkara advises organisations on the EU AI Act, GDPR and responsible AI adoption, bridging Legal, IT and Business. As a speaker and consultant he translates complex regulation into concrete, demonstrable steps: from classification to a review-ready evidence pack. He is the founder of Embed AI and Praxikon.

Compliance under the AI Act is not a technology question but a classification and evidence question. Start with the right classification, not the model.

About Embed AI

Embed AI makes AI in organisations responsible and customer-ready under the EU AI Act and GDPR. From independent risk check and classification to a review-ready evidence pack, legal and technical, with implementation. For organisations with AI in their processes and vendors who sell AI.

Sources and next step

Version 2026.09 · Reference date 2026-09-10

This report references the official text of Regulation (EU) 2024/1689 and the European Commission guidelines. Read the official sources together with the amendments. Praxikon provides additional domain guidance.

[EU AI Act: Regulation \(EU\) 2024/1689](#)

[Digital Omnibus on AI: Regulation \(EU\) 2026/1744, Article 1\(39\)-\(40\)](#)

[European Commission: implementation timeline](#)

[AI Act amendment: Regulation \(EU\) 2026/1744](#)

[Commission draft guidelines: high-risk classification \(19 May 2026\)](#)

[European Commission: AI literacy questions and answers](#)

[Praxikon](#) · [Current reports](#)

Bring your education use and the open question about assessment, oversight or evidence to the AI Act gap intake. Embed AI helps clarify the open point and determine an appropriate next step.

[Discuss your open question](#)