

● Sample guide for Example Organisation Ltd

EU AI Act compliance

How a UK employer with an EU team classifies its AI systems, finds the gaps and plans the work. A sample gap analysis, accurate as at October 2026.



“Compliance doesn’t have to be complicated. It just has to be right.”

Prepared for
Example Organisation Ltd
a fictional organisation

Prepared by
AI Assist
part of Cloud Assist Group

Regulatory position
As at October 2026
sample edition

Engagement
Compliance and Risk
6 to 10 weeks

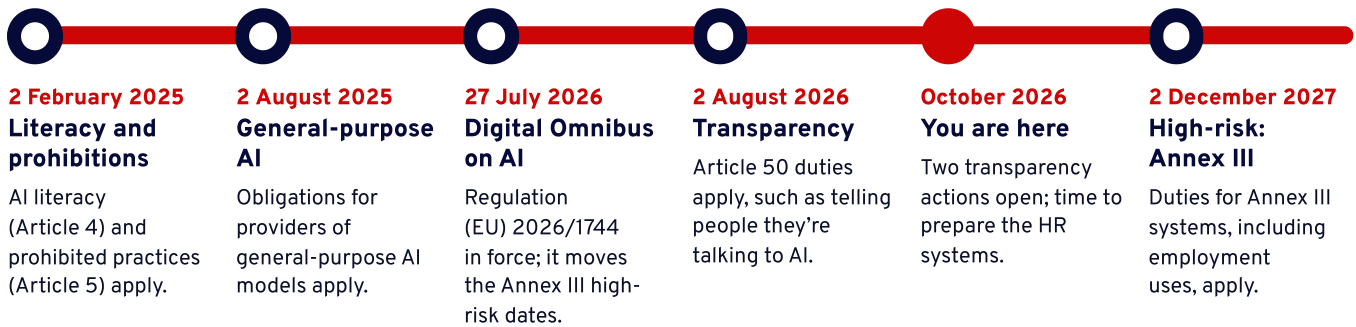
About this sample. This guide shows the format of our compliance gap analysis. Example Organisation Ltd is fictional: a UK employer of about 2,400 people, with a subsidiary team in Dublin. Its systems, findings and scores are invented. This is general information, not legal advice; a real engagement works alongside your legal advisers.

1 Summary

Where Example Organisation stands under the EU AI Act

Example Organisation is a UK company, but its Dublin subsidiary uses AI systems in the EU, so the Act applies to that use. No prohibited practices are in use, and the largest duties, for two HR systems, apply from 2 December 2027. Two transparency actions come first, because those rules already apply.

Key dates



What we found Illustrative

11

AI systems in use or planned

Five more than the organisation knew about.

2

high-risk systems

Both in HR. Deployer duties from 2 December 2027.

3

with transparency duties

Two actions open now.

0

prohibited practices in use

One optional feature must stay switched off.

What we recommend

- 1 Act now on what already applies.** Add an AI notice to the customer chatbot, label training videos that use a synthetic voice, and confirm in the contact-centre contract that the staff emotion feature stays switched off.
- 2 Give AI compliance an owner.** Name one accountable owner, keep the AI inventory as a living register, and plan AI literacy for everyone who uses or oversees AI.
- 3 Prepare the two HR systems properly.** Use 2027 to get evidence from both vendors, design human oversight, update notices and brief employee representatives, ready for 2 December 2027.
- 4 Report to the board each quarter.** A one-page pack tracks systems, gaps and actions, so the board sees progress without the jargon.

Who carries which duty. Most high-risk requirements sit with the provider (here, the vendor). Example Organisation is the deployer of both HR systems, and the provider of the chatbot it built itself.

2 Risk classification

System by system: what each AI use is, and what it means

We found 11 AI systems in use or planned. Each is classified by risk tier and by Example Organisation's role: **provider** (it develops the system, or has it developed, and puts it into use under its own name) or **deployer** (it uses a system under its own authority). Systems are illustrative.

#	System and use	Role	Tier	Why	What Example Organisation must do
1	Applicant tracking: CV screening and ranking (vendor). In trial for Dublin roles.	Deployer	High-risk	Annex III, point 4(a): recruitment and selection. It profiles candidates, so it stays high-risk.	Deployer duties (Article 26) from 2 December 2027; DPIA; candidate notice; a person reviews every shortlist.
2	Workforce analytics: performance ranking (vendor). Ranks Dublin contact-centre staff for coaching and bonus.	Deployer	High-risk	Annex III, point 4(b): monitoring and evaluating performance; decisions affecting terms of work.	As for system 1, plus informing workers' representatives and affected staff before use.
3	Contact-centre platform: staff emotion insights (optional vendor feature). Would infer staff emotions from call audio.	Deployer	Prohibited	Article 5: emotion recognition in the workplace, outside medical or safety reasons.	Keep it switched off. Add a contract clause and confirm the setting each year.
4	Customer chatbot on the Irish website , built in-house on a general-purpose AI model.	Provider	Transparency	Article 50: people must be told they're interacting with an AI system, unless it's obvious.	Add a clear AI notice at the start of each chat. Open now.
5	Training videos using a synthetic copy of a real trainer's voice.	Deployer	Transparency	Article 50: audio that resembles a real person and could seem authentic must be disclosed.	Label each video as AI-generated; record the trainer's consent. Open now.
6	HR policy assistant for staff (vendor). Answers from approved policies.	Deployer	Transparency	Article 50 duty sits with the vendor as provider.	Checked: the vendor's AI notice is switched on.
7	Licensed productivity assistant for drafting and summaries.	Deployer	Minimal	General office use; no Annex III purpose.	Acceptable-use policy; AI literacy for users.
8	Demand forecasting for service centre staffing (pilot).	Deployer	Minimal	Forecasts call volumes, not individuals.	Re-classify if it starts allocating shifts to named people (Annex III, point 4(b)).
9	Invoice matching in the finance system.	Deployer	Minimal	No Annex III purpose.	Keep in the register; review on change.
10	Marketing copy drafting tool.	Deployer	Minimal	No Annex III purpose.	A person edits everything before it's published.
11	Email security threat detection.	Deployer	Minimal	No Annex III purpose.	Keep in the register; review on change.

An Annex III system that profiles people is always high-risk. A deployer can become a provider by putting its own name on a high-risk system or substantially modifying it (Article 25). How the transitional rules apply to systems already in use before 2 December 2027 should be confirmed with your legal advisers; we recommend preparing both HR systems as in scope.

3 Gap analysis

High-risk readiness: the two HR systems

For each requirement area we show who carries the duty and what we found. Most technical requirements sit with the vendors as providers. Example Organisation's job as deployer is to get evidence from them and carry out its own duties under Article 26. Status is illustrative.

Requirement area	Who carries it	What we found	Status	Priority
Risk management system	Provider; you share how you use it	Neither vendor has shared its risk documentation.	Gap	High
Data governance	Provider for training data; you for input data you control	Dublin job data includes fields that can act as proxies, such as career gaps.	Partial	High
Technical documentation and instructions for use	Provider writes them; you follow the instructions for use	Instructions for use aren't held on file for either system.	Gap	Medium
Transparency and user information	Provider designs it; you inform candidates and staff	The candidate privacy notice doesn't mention automated screening.	Gap	High
Human oversight	You: competent people with the training and authority to step in	Recruiters accept rankings as given; overrides aren't recorded.	Gap	High
Accuracy and robustness	Provider declares and tests; you monitor in use	No local check of outcomes since the trial began.	Partial	Medium
Cybersecurity	Provider; you control access	Single sign-on and role-based access are in place.	In place	Low
Monitoring in use	Provider runs post-market monitoring; you monitor and report risks	No monitoring routine or named owner.	Gap	Medium
Incident reporting	You tell the provider and the relevant authority about serious incidents	No route defined for AI incidents.	Gap	Medium
Conformity assessment and registration	Provider	One vendor has shared a timeline; the other hasn't yet.	Partial	Medium
Logs and audit trail	You keep the logs under your control for at least six months	Logs are kept for 90 days.	Partial	Medium
Informing workers	You inform workers' representatives and affected staff before use at work	Not done for the performance ranking module.	Gap	High

Totals: 7 gaps, 4 partial, 1 in place. Five of the open items are high priority.

Beyond the EU AI Act

UK GDPR and EU GDPR

Complete a DPIA for both HR systems. Check the lawful basis, update candidate and staff privacy notices, and make sure a person makes the final decision, with a clear way to challenge it.

Employment and equality law

Test outcomes for indirect discrimination: the Equality Act 2010 for UK use, and Irish employment equality law for Dublin. Check duties to consult employee representatives.

Third-party AI vendors

Run the vendor assessment scorecard on both HR vendors and the contact-centre platform, and add AI terms to each contract at renewal.

4 Roadmap and reporting

A prioritised plan to December 2027, and beyond

Duties that already apply come first. The HR systems then get a full year of preparation, with the board seeing progress every quarter.

Now to December 2026**Close what already applies**

Chatbot AI notice. Labels on synthetic-voice videos. Contract clause keeping emotion insights off. A named AI compliance owner. An AI literacy plan.

January to June 2027**Get the evidence**

Vendor scorecards for both HR systems. DPIAs. Updated candidate and staff notices. Employee representatives briefed.

July to November 2027**Ready for
2 December 2027**

Human oversight designed and trained. Logs kept for six months or more. Monitoring and incident routines. A dry-run audit and board sign-off.

From December 2027**Run and improve**

Quarterly monitoring. Annual re-classification. Every new AI use triaged at intake through the compliance engine.

Vendor assessment scorecard

Extract for the applicant tracking vendor. Illustrative scores, 1 to 5.

Criterion	Score
States intended purpose and risk classification	●●●●○
Provides instructions for use	●●●○○
Conformity assessment and CE marking plan	●●○○○
Evidence of bias and accuracy testing	●●○○○
Logging and export for deployers	●●●○○
Oversight features: overrides and explanations	●●●○○
Data location and GDPR terms	●●●●○
Commits to notify incidents promptly	●●○○○
Total	23 of 40

Board reporting pack

Extract from the quarterly one-page report. Illustrative.

11

AI systems registered

5

high-priority gaps open

2

transparency actions
open

5

actions due by
December 2026

System	Status
CV screening (1)	On track
Performance ranking (2)	At risk
Customer chatbot (4)	Action due
Emotion insights (3)	Switched off

Ongoing monitoring protocol

Extract. The compliance engine schedules each check, records the evidence and flags anything overdue.

Monthly

Outcome checks on both HR systems. Override rates. Complaints and challenges logged.

Quarterly

Board pack. Vendor updates reviewed for significant changes. Register refreshed.

Yearly

Every system re-classified. Bias tests rerun. AI literacy plan refreshed.

On any change

New AI uses and new vendor features are triaged before they go live.

5 About AI Assist

AI that works for people

AI Assist helps organisations use AI where it genuinely helps, and tells them honestly when it won't. We translate regulatory complexity into practical action, so compliance scales as your AI ambitions grow.

No proprietary lock-in

You own everything we create. Our recommendations are vendor-agnostic.

Ethics as standard

Every engagement includes ethical assessment, bias testing, governance and transparency.

Plain English, always

If your finance director can't follow the recommendation, we haven't done our job.

How a Compliance and Risk engagement runs



What the full engagement delivers

- Compliance gap analysis
- Prioritised remediation roadmap
- Documentation templates and examples
- Compliance engine: a checklist and workflow tool
- Vendor assessment scorecard
- Board reporting pack
- Training materials for compliance teams
- Ongoing monitoring protocols

Part of Cloud Assist Group



Book a discovery call

No pitch. No pressure. Just 30 minutes to understand your challenge and explore whether we can help.

AI Assist is part of Cloud Assist Group. ai-assist.cloud. This guide is general information, not legal advice; regulatory position as at October 2026.