30-Day Compliance Action Plan — Anonymised Sample

30-Day Compliance Action Plan — Anonymised Sample

> **Anonymised — Do not redistribute.** Excerpt from a Readiness Sprint deliverable. The customer "Acme Decisions Ltd" and the AI system "AcmeMatch" are illustrative.

Customer: Acme Decisions Ltd · **AI System:** AcmeMatch v3.4 · **Plan version:** 1.0 · **Plan date:** 2026-04-25

Purpose

The Readiness Sprint produces this 30-day action plan as the lightest commercially useful artefact: a concrete, sequenced list of actions Acme Decisions Ltd should take across legal, product, ML, security, and commercial owners to (1) stay safely on the right side of EU AI Act and UK/EU GDPR for AcmeMatch v3.4, and (2) be ready to answer enterprise procurement questionnaires without scrambling.

This plan is **not legal advice**. It is a sequenced workplan informed by the EU AI Act, UK GDPR, and the AcmeMatch evidence pack. Every external commitment that flows from this plan should be reviewed by Acme's solicitor or DPO before action.

How to read this plan

- **Owner** — the named role responsible. If two owners, the first is the lead.
- **Effort** — small (≤ ½ day), medium (1-3 days), large (> 3 days).
- **Gating** — what blocks the action from starting. *None* means start now.
- **Outcome** — what's true after the action lands.

Week 1 — Stop the bleeding (clarity + immediate compliance defenses)

W1-A1 — Confirm intended-purpose statement and lock it in writing

- **Owner:** Head of Product
- **Effort:** Small
- **Gating:** None
- **Outcome:** AcmeMatch's intended purpose, in-scope tasks, and out-of-scope tasks are written, signed off internally, and pasted into the Annex IV technical documentation §1.1 and the Deployer Use Manual.
- *Why first:* every other AI Act obligation cascades from intended purpose. A vague statement creates ambiguity in Article 6(3) derogation and in Article 26 Deployer obligations.

W1-A2 — Confirm risk classification and document the basis

- **Owner:** Head of Product + DPO
- **Effort:** Small
- **Gating:** W1-A1
- **Outcome:** Risk classification memo is signed off internally; Article 5 + Annex III + Article 6(3) analysis is recorded; classification is "high-risk per Annex III §4(a)".

W1-A3 — Stand up Article 12 logging and Article 23 retention

- **Owner:** Head of Engineering
- **Effort:** Medium
- **Gating:** None
- **Outcome:** Tamper-evident audit logs are live across recruiter activity, model output, and override events, retained per the documented retention policy (10 years post-final unit per Article 23 for technical documentation; tighter retention for personal data per UK GDPR Article 5(1)(e)).

W1-A4 — Publish the candidate-facing transparency clause and update Deployer Use Manual

- **Owner:** Head of Product + Marketing (privacy-notice copy)
- **Effort:** Small
- **Gating:** None
- **Outcome:** Candidate-facing privacy-notice clause is published; Deployer Use Manual instructs Deployers to disclose AcmeMatch's role at point of application.

Week 2 — Documentation and oversight rigour

W2-A1 — Complete Annex IV technical documentation §§1-3 and §9

- **Owner:** Head of Product + Head of ML
- **Effort:** Medium
- **Gating:** W1-A1, W1-A2
- **Outcome:** Annex IV first-draft is complete to the standard shown in the Documentation Sprint sample. §9 outstanding actions matches this 30-day plan.

W2-A2 — Run the AcmeMatch human-oversight design review

- **Owner:** Head of Product + external reviewer
- **Effort:** Medium
- **Gating:** None
- **Outcome:** Article 14 (4)(b) "person assigned with the necessary competence" requirement met; oversight checklist signed off; any UI gaps are added to the engineering backlog.

W2-A3 — Lock the bias audit cadence and run the next cycle

- **Owner:** Head of ML
- **Effort:** Medium
- **Gating:** None
- **Outcome:** Quarterly bias audit cycle is published, Q2 audit is in flight, and the bias-treatment process under Article 10 is exercisable.

W2-A4 — DPIA first-draft signed off internally

- **Owner:** DPO
- **Effort:** Medium
- **Gating:** W1-A2
- **Outcome:** DPIA first-draft sits in place; outstanding actions are scheduled with named owners.

Week 3 — Commercial and procurement readiness

W3-A1 — Stand up the supplier-questionnaire response pack

- **Owner:** Head of Commercial + Head of Product
- **Effort:** Medium
- **Gating:** W2-A1, W2-A2, W2-A4
- **Outcome:** A 60-question response pack (or longer) is ready to send within 1 business day of receiving an enterprise buyer questionnaire. Each answer references an evidence document.

W3-A2 — Draft sub-processor annex + cross-border transfer mechanism

- **Owner:** DPO + Head of Engineering
- **Effort:** Medium
- **Gating:** None
- **Outcome:** Sub-processor list is current; UK IDTA + EU SCC + transfer-risk-assessment is in place for any third-country sub-processor.

W3-A3 — Update the Acme Service Agreement to reference Annex IV documentation, transparency obligations, and Deployer obligations under Article 26

- **Owner:** Head of Commercial + external counsel
- **Effort:** Medium
- **Gating:** W2-A1
- **Outcome:** Net-new commercial deals carry the contract terms that match the documented compliance posture.

W3-A4 — Decide on EU authorised representative (Article 22 (Provider))

- **Owner:** CEO + Head of Commercial
- **Effort:** Medium
- **Gating:** None
- **Outcome:** Decision recorded in the risk register; if appointed, the representative's contact details are published in the documentation.

Week 4 — Sustaining controls and post-market readiness

W4-A1 — Activate post-market monitoring per Article 72

- **Owner:** Head of Product
- **Effort:** Medium
- **Gating:** W1-A3
- **Outcome:** "Report a problem" flow surfaces structured incidents into a single workflow; monthly Deployer health-check call is on the calendar; quarterly post-market monitoring report template is live.

W4-A2 — Tabletop the AI incident workflow per Article 73

- **Owner:** Head of Security + DPO + Head of Product
- **Effort:** Medium
- **Gating:** W4-A1
- **Outcome:** Incident playbook is exercised; named contacts and escalation paths are confirmed; gaps are added to the risk register.

W4-A3 — Schedule the external independent review of human oversight

- **Owner:** DPO
- **Effort:** Small
- **Gating:** W2-A2
- **Outcome:** Independent review is booked with a named reviewer; report due 2026-09-30 (per oversight checklist §3.1).

W4-A4 — Publish a customer-facing AI Act / GDPR posture page

- **Owner:** Marketing + DPO
- **Effort:** Small
- **Gating:** W3-A1
- **Outcome:** A short, plain-language posture page lives on the Acme website covering: classification, oversight, bias controls, retention, sub-processors, contact route. Buyers see this before they ever send a questionnaire.

Outstanding items beyond Day 30 (carry into the next plan)

- Quarterly bias audit cadence operating without misses (CTRL-005).
- Annual audit rights exercised by at least one enterprise buyer.
- Article 26 Deployer training pack delivered to every active Deployer.
- ISO 27001 certification audit (scheduled 2026-Q4).
- SOC 2 Type II audit (scheduled 2026-2027).

Document control

Item	Detail
Sample produced	2026-04-25
Anonymised customer	Acme Decisions Ltd (fictional UK SME)
AI system in scope	AcmeMatch v3.4
Tier of artefact	Readiness Sprint (£2,500) — also delivered as part of Documentation Sprint and Audit Pack
Reviewer	Customer's solicitor or DPO before external commitments are made

---

Prepared with support from GeraCompliance. This document is not legal advice and does not guarantee compliance. The customer remains responsible for legal review, implementation, and regulatory obligations.