Supplier Questionnaire Response Pack — Anonymised Sample

Supplier Questionnaire Response Pack — Anonymised Sample

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

Customer: Acme Decisions Ltd · **AI System:** AcmeMatch v3.4 · **Pack version:** 1.0 · **Last review:** 2026-04-25

Purpose

This pack is the structured response Acme Decisions Ltd uses when an EU enterprise buyer or a UK regulated buyer (financial services, public sector, healthcare) sends an AI-vendor procurement questionnaire. It pre-answers the most common 60+ questions seen in 2026-Q1-Q2 procurement cycles, mapped to AcmeMatch's documented evidence pack (Annex IV, risk register, DPIA, oversight checklist, ROPA).

This sample shows **15 representative questions of the 62** in the full pack. The response pattern is the value: a buyer's question gets a one-paragraph plain-language answer, followed by a one-line evidence reference, so the buyer can verify without us drowning them in attachments.

A. AI Act / regulatory questions

A1. "Have you classified your AI system under the EU AI Act?"

Yes. AcmeMatch v3.4 is classified as a **high-risk AI system** under EU AI Act Annex III §4(a) (recruitment / candidate selection). The classification analysis covers Article 5 prohibitions, Annex III applicability, and the Article 6(3) derogation test, all of which are documented in our Risk Classification Memo. Article 6(3) is not available to AcmeMatch as scoped.

Evidence: `02-risk-classification-memo-sample.md` §2 (full deliverable) + Annex IV §1.

A2. "Do you maintain Annex IV technical documentation?"

Yes. We maintain Annex IV technical documentation per Article 11. The documentation covers all 9 Annex IV section headings (general description; development; monitoring; system performance; lifecycle

changes; harmonised standards applied; declaration of conformity; post-market system; outstanding actions). Document retention is 10 years post-final-unit placed on the market, per Article 23.

Evidence: `01-annex-iv-technical-documentation-skeleton-sample.md` (full deliverable) + Article 23 retention policy.

A3. "Do you have a risk-management system per Article 9?"

Yes. We maintain an Article 9 risk-management system covering the lifecycle of AcmeMatch. Risks are scored on a 5×5 matrix; treated and residual scores are recorded; controls are mapped per risk; reviews are at minimum monthly for Critical-rated risks and quarterly for the full register.

Evidence: `03-risk-management-register-sample.md` §1 and §3 (full register: 18 rows; controls: 22 entries).

A4. "Are humans always able to override the AI's output?"

Yes. AcmeMatch is designed so the recruiter cannot move a candidate to interview without affirmatively selecting that candidate, and every shortlist surface includes a labelled override-and-re-rank control. We monitor for "rubber-stamping" patterns and intervene with retraining when override rates fall below threshold.

Evidence: `04-human-oversight-transparency-checklist-sample.md` §1.1 controls 1-5; §1.2 control 8.

A5. "How does your system avoid breaching Article 5 prohibitions, especially emotion recognition in the workplace?"

By design. Our input-side filter rejects emotion-recognition prompts and our system architecture has no biometric or affect-recognition processing. The documentation explicitly enumerates each Article 5(1) prohibition and confirms non-applicability with reasoning.

Evidence: `02-risk-classification-memo-sample.md` §2.1.

B. UK GDPR / EU GDPR questions

B1. "Are you the controller or the processor for our candidate data?"

Acme Decisions Ltd is the **processor** for your candidate data. You are the controller within your tenant. We process candidate data only on your documented instructions, per the Data Processing Agreement attached to the Acme Service Agreement.

Evidence: DPA §2 (Roles); ROPA entry in `05-gdpr-dpia-starter-sample.md` §2.

B2. "Do you process special-category data?"

No. AcmeMatch is **designed not to process special-category data**. Demographic features (name, age, gender, nationality) are stripped at ingestion and not used as ranking signals. If a Deployer uploads structured fields containing special-category data, the ingestion layer rejects them at schema validation.

Evidence: `05-gdpr-dpia-starter-sample.md` §1.3; CTRL-004 in `03-risk-management-register-sample.md`.

B3. "Does Article 22 (solely automated decision-making) apply?"

No. AcmeMatch produces a ranked shortlist; the recruiter retains decision authority and exercises it via UI-enforced human review. The Deployer Use Manual explicitly prohibits using AcmeMatch as the sole basis for adverse decisions.

Evidence: `05-gdpr-dpia-starter-sample.md` §1.4; oversight checklist controls 1-5.

B4. "Have you completed a DPIA?"

Yes. A first-draft DPIA is in place; it is reviewed by our DPO and is updated whenever a material change is proposed. We share the DPIA on a need-to-know basis with enterprise buyers under NDA.

Evidence: `05-gdpr-dpia-starter-sample.md` §3.

B5. "What is your retention period for candidate data?"

For an active role, data is retained for the role's duration plus 30 days, then deleted automatically. For talent-pool retention, only with explicit candidate consent, reviewed annually.

Evidence: ROPA in `05-gdpr-dpia-starter-sample.md` §2; CTRL-012 + CTRL-013 in `03-risk-management-register-sample.md`.

C. Bias, fairness, and accuracy

C1. "How do you test for bias?"

Quarterly bias audits on a held-out evaluation set, reporting selection-rate parity and top-N recall parity by protected sub-group where available. Any sub-group with > 0.05 deviation triggers a model-card review and possible retrain.

Evidence: CTRL-005 + CTRL-006 in `03-risk-management-register-sample.md`; Annex IV §3.3.

C2. "What are the model's headline performance metrics?"

Top-10 recall vs. recruiter ground-truth shortlists ≥ 0.78; Brier score on rationale-tag confidence ≤ 0.18; PSI drift alert at > 0.15 sustained over 30 days.

Evidence: Annex IV §3.2; performance-monitoring dashboard.

C3. "How do you handle adversarial input (e.g. CV stuffing, prompt injection)?"

Multi-layered: input sanitisation, file-type whitelist, length and entropy bounds, output anomaly detection. Cybersecurity controls map to Article 15 obligations.

Evidence: CTRL-010 + CTRL-011 in `03-risk-management-register-sample.md`; Annex IV §3.3.

D. Security and operations

D1. "Are you ISO 27001 / SOC 2 / Cyber Essentials Plus certified?"

ISO 27001-aligned controls operating; certification scheduled for 2026-Q4. Cyber Essentials Plus held since 2025-09. SOC 2 Type II audit scheduled for 2026-2027.

Evidence: certificate copies on request under NDA; AcmeMatch Security Pack §1.

D2. "What is your incident response time?"

Severity 1 incidents (confidentiality breach affecting candidate data, unauthorised access, ransomware): acknowledgement ≤ 1 hour; status update every 4 hours; preliminary report ≤ 72 hours; UK ICO / EU competent authority notification within statutory window if applicable.

Evidence: AcmeMatch Incident Response Playbook §3 (NDA-gated).

D3. "Do you use sub-processors?"

Yes — see the AcmeMatch Sub-Processor Annex. Each sub-processor is contractually bound to GDPR-aligned terms, and each one is reviewed at least annually.

Evidence: AcmeMatch Sub-Processor Annex (current as of 2026-Q1).

E. Commercial / contract

E1. "Will you sign our DPA / our security addendum?"

We start with our standard DPA, attached as an annex to the Acme Service Agreement. We are open to commercially reasonable changes to a buyer's security addendum on request and route any contract-altering questions through Acme's legal team. We do not accept terms that conflict with Article 28 GDPR or with our published sub-processor list.

Evidence: Acme Service Agreement DPA Annex; sample security addendum redlines on request.

E2. "Do you provide audit rights?"

Yes — annual audit rights on reasonable notice, conducted by an independent third-party auditor under NDA, scope limited to our processing of the buyer's candidate data. We share recent SOC 2-style reports, ISO 27001 scope statements, and penetration test summaries in advance to reduce duplication of effort.

Evidence: DPA §"Audit rights"; recent audit summary on request under NDA.

How this pack scales

- The full Documentation Sprint pack covers 62 questions across A-E + section F (incident notification + post-market monitoring).
- The Audit Pack tier extends to a multi-system pack covering up to 3 AI systems and adds a buyer-customisable response builder.
- For each new AI system, a fresh row is added to the register, the Annex IV is extended, and the questionnaire pack inherits answers automatically where the underlying control is shared.

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	Documentation Sprint
Reviewer	Customer's solicitor, DPO, or commercial lead before external send

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.