GDPR Lawful-Basis, ROPA, and DPIA Starter — Anonymised Sample

GDPR Lawful-Basis, ROPA, and DPIA Starter — 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 · **Starter version:** 1.0 · **Last review:** 2026-04-25

Purpose

This starter pack assembles the three GDPR artefacts a UK SME placing AI-assisted recruitment software on the EU/UK market most often needs first:

1. **Lawful-basis assessment** — UK GDPR Article 6 / EU GDPR Article 6 grounds + UK GDPR Article 9 / EU GDPR Article 9 special-category check.
2. **Record of Processing Activities (ROPA) entry** — UK GDPR Article 30 / EU GDPR Article 30.
3. **DPIA (Data Protection Impact Assessment) starter** — UK GDPR Article 35 / EU GDPR Article 35.

Each artefact is shown at first-draft level — enough for a customer's DPO or external counsel to review and finalise.

1. Lawful-basis assessment

1.1 Roles

- **Acme Decisions Ltd** — *processor* on behalf of recruiter customers. Acme processes personal data only on the recruiter customer's documented instructions, per the Data Processing Agreement.
- **Recruiter customer** — *controller* of the candidate's personal data within their tenant.
- **Candidate** — *data subject*.

1.2 Lawful basis (Article 6) — controller's view, accepted by Acme as processor

Lawful basis	Applicable?	Why
(a) Consent	Sometimes	Where the recruiter offers the candidate a "join the talent pool" opt-in, consent is the controller's basis for retention beyond the active role.
(b) Contract	Sometimes	Where the candidate has applied for a specific role, processing necessary to consider the application is generally lawful under "steps prior to entering a contract" with the candidate.
(c) Legal obligation	Rarely	Limited cases (right-to-work checks, equal-opportunities monitoring required by law).
(d) Vital interests	No	Not applicable.
(e) Public task	No	Not applicable to private-sector recruiters.
(f) Legitimate interests	Sometimes	The recruiter's legitimate interest in efficient candidate review *can* support shortlisting if the LIA balancing test is documented and the candidate's rights are respected (clear notice, opt-out, no Article 22 issue).

1.3 Special-category data (Article 9)

Type	Processed?	Mitigation
Racial / ethnic origin	**No**	Excluded at ingestion.
Political opinion	**No**	Excluded.
Religious / philosophical belief	**No**	Excluded.
Trade union membership	**No**	Excluded.
Health data	**No**	Excluded.
Genetic / biometric data	**No**	No biometric processing.
Sex life / sexual orientation	**No**	Excluded.

Conclusion: AcmeMatch is **designed not to process special-category data**. If a Deployer attempts to upload special-category data via the structured ATS field, it is rejected at the schema-validation layer.

1.4 Article 22 — solely automated decision-making with legal or similarly significant effects

- AcmeMatch outputs a **ranked shortlist**, not a hire/no-hire decision.
- The recruiter is required by the Deployer Use Manual and by AcmeMatch's UI design (see `04-human-oversight-transparency-checklist-sample.md` controls 1-5) to exercise meaningful review before any candidate is moved to the next stage.
- **Conclusion:** Article 22 does **not** apply, provided the Deployer follows the Use Manual.

2. ROPA entry (Article 30)

Field	Detail
Name of processing activity	AcmeMatch — AI-assisted candidate-shortlist ranking
Controller	Recruiter customer (per tenant)
Processor	Acme Decisions Ltd
Purpose of processing	Ranking candidate applications against a recruiter-defined role profile to support recruiter shortlist preparation
Categories of data subjects	Candidates who have applied for an open role (or, with consent, candidates retained in the recruiter's talent pool)
Categories of personal data	Identification (name, contact); CV content (work history, education, skills, voluntary statements); structured ATS fields (role, location, recruiter status); ranking-derived data (rank position, rationale tags)
Categories of recipients	Recruiter customer's authorised users; Acme Decisions Ltd internal personnel under role-based access control; Acme's licensed model-API provider (under DPA)
International transfers	Acme processes data primarily in the UK and EU. Where a sub-processor is in a third country, an Article 46 transfer mechanism (e.g. UK IDTA + EU SCC + Transfer Risk Assessment) is in place. The full sub-processor list is in the AcmeMatch Sub-Processor Annex.
Retention period	Active role: data retained for the duration of the role, plus 30 days. Talent pool: retained only with explicit candidate consent, reviewable annually.
Technical and organisational security measures	Encryption in transit (TLS 1.3) and at rest (AES-256); role-based access control; audit logging per Article 12; ISO 27001-aligned controls; quarterly penetration test; documented incident-response process.

3. DPIA starter (Article 35)

3.1 Necessity and proportionality of the processing

- **Necessity:** ranking candidates against a role profile is a core part of the recruiter's hiring workflow. AcmeMatch substitutes a structured AI ranking for a manual sorting step that is otherwise time-consuming and inconsistent.
- **Proportionality:** AcmeMatch processes only the minimum data needed for ranking (CV, structured ATS fields). Sensitive demographic data is excluded by design. The ranking output is consultative, not decision-making.

3.2 Risks to data subjects (high-level — full DPIA expands each)

Risk to data subject	Severity (1-3)	Likelihood (1-3)	Inherent	Treatment	Residual
Unfair ranking due to indirect proxy bias	3	2	6	Bias audit + sub-group parity metrics + retraining trigger (CTRL-004 to CTRL-006)	3
Loss of confidentiality of CV data	3	2	6	Encryption + access control + sub-processor management + breach response	2
Over-retention beyond purpose	2	2	4	Automated 30-day deletion (CTRL-012) + consent-based talent-pool extension	1
Lack of transparency about AI involvement	2	2	4	Deployer-facing privacy notice clause + candidate FAQ template (transparency checklist controls 25-27)	2
Article 22 misuse — Deployer treats ranking as a decision	3	2	6	Deployer Use Manual prohibition + mandatory human-in-loop UI controls (oversight checklist 1-5)	3

3.3 Outcome of consultation

- Internal: Acme's DPO has reviewed v3.4. Outstanding actions: (a) external independent review of the bias audit; (b) confirmation of cross-border transfer mechanism for the licensed model-API provider's regional rotation.
- External: ICO consultation under Article 36 has not been triggered — residual risks are not assessed as "high" after mitigation.

3.4 Sign-off

Role	Name	Signed	Date
Data Protection Officer	[TBD]	[ ]	YYYY-MM-DD
Senior Information Risk Owner	[TBD]	[ ]	YYYY-MM-DD
External counsel review	[TBD]	[ ]	YYYY-MM-DD

3.5 Review cadence

- Reviewed annually, or whenever a material change is proposed (new training data, new processing region, new processing purpose, new sub-processor, new candidate-facing surface).

4. Outstanding actions

1. Customer's DPO finalises the LIA balancing test for the "legitimate interests" lawful basis where used.
2. Customer's external counsel reviews and adopts the DPIA before EU launch.
3. Customer ensures the candidate-facing privacy notice references AcmeMatch's role.
4. Customer ensures the Deployer-side training is delivered to all recruiters who use AcmeMatch.

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 DPO + external counsel before external reliance

---

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.