HR RESEARCH SERIES 2026 - REPORT R16 OF 10 (EXTENDED)

# GDPR-Compliant Recruiting: The Practical Guide 2026

Everything HR teams need to handle candidate data lawfully, with updated enforcement data and common failure points.

Eight years after GDPR came into force, recruitment remains one of the highest-risk data processing activities for most organisations, and one of the most poorly managed from a compliance perspective. High volumes of sensitive personal data, complex processing activities (AI screening, third-party background checks, job board data) and the legal requirement for transparent, lawful processing create a compliance burden that most HR teams are not adequately managing.


Published: May 2026 - tenperzent.com - Report R16 of 10 (Extended)

 

This practical guide is not a legal treatise, it is an operational guide to what you must do, what you should not do, and how to structure your recruitment data processes to be both legally sound and practically workable.

## Lawful basis for candidate data processing

Every data processing activity in recruitment must have a documented lawful basis. The critical mistake is using 'consent' as the lawful basis for initial job applications. Consent must be freely given, a candidate applying for a job cannot genuinely refuse data processing, so true consent does not exist. Legitimate interests is the correct basis for most recruitment data processing.

| Processing activity | Correct lawful basis | Incorrect common practice | Risk if wrong |
|---|---|---|---|
| Receiving and storing applications | Legitimate interests | Consent | Invalid basis, all processing unlawful |
| AI CV screening | Legitimate interests + Article 22 compliance | Consent or no documented basis | Article 22 violation, enforcement risk |
| Background checks pre-offer | N/A, not legal yet | Legitimate interests | Premature processing, minimisation violation |
| Background checks post-offer | Contractual necessity | Legitimate interests | Wrong basis, weaker legal protection |
| Talent pool retention | Explicit consent | Legitimate interests | Retention unlawful without consent |
| Right to work verification | Legal obligation | Legitimate interests | Wrong basis, weak if challenged |

## Data minimisation, collecting only what you need

Data minimisation is the principle of collecting only what is necessary for the specific purpose. Most recruitment forms violate this principle by collecting demographic information, full address details, or detailed personal information at the application stage when it is not yet needed.

- **Application stage**, name, email, phone, CV, cover letter only.
- **Demographic data**, optional, separate, with explicit purpose statement.
- **Full address**, only after offer.
- **Date of birth**, only after offer or for legitimate age-restricted role.
- **Nationality / right-to-work proof**, only after offer (right to work) or with justified anti-discrimination logic.

## Retention limits, the most common violation

| Data type | Maximum retention | Lawful basis for retention | Action at expiry |
|---|---|---|---|
| Application form (unsuccessful) | 12 months from rejection | Legitimate interests (legal claim) | Automated deletion, confirm no SAR pending |
| CV (unsuccessful applicants) | 12 months from rejection | Same as above | Automated deletion |
| Interview notes and scoring | 6 months from decision | Legitimate interests | Deletion, not to HRIS |
| Talent pool (with consent) | 24 months max with renewal | Explicit consent | Re-consent at 18 months, delete if not renewed |
| Assessment results (unsuccessful) | 6 months from decision | Legitimate interests | Deletion |
| Successful applicant data | Transfers to employment record | Employment contract | Follow employment data retention policy |

## AI screening and GDPR Article 22

Article 22 grants individuals the right not to be subject to solely automated decisions that produce legal or similarly significant effects. AI CV screening that determines progression falls squarely within this provision. 'Solely automated' is the key term, a system where AI ranks but a human decides who progresses is not solely automated.

**Practical Article 22 compliance for AI screening: ensure a human reviewer makes the actual shortlisting decision (reviewing AI recommendations, not ratifying them), document the human decision point, and provide candidates with a meaningful explanation of how AI was used if they request it.**

## Subject access requests from candidates

Candidate SARs are increasing 34% year-over-year. Within one month, you must provide all personal data held about the requesting individual, including application data, CV, interview notes, AI screening scores, reference notes, and internal communications containing their personal data.

| Data type | In SAR scope? | Common mistake | Best practice |
|---|---|---|---|
| Application form data | Yes | Not included, assumed admin | Include all responses |
| CV as submitted | Yes | Excluded as 'candidate's own document' | Include, GDPR applies to how you stored it |

| Data type | In SAR scope? | Common mistake | Best practice |
|---|---|---|---|
| Interview scores | Yes | Withheld as internal | Must include unless legal exemption |
| Interview notes | Yes | Notes deleted to avoid SAR | Structured notes retained, unstructured deleted |
| AI screening score and factors | Yes | ATS doesn't export this | Ensure ATS can export AI scoring per candidate |
| Recruiter email discussions | Yes (personal data only) | Not checked | Search email for candidate name |

## Building a GDPR-compliant recruitment process

| Control point | Implementation | Effort | Risk if absent |
|---|---|---|---|
| Lawful basis documentation | Document basis per processing activity in ROPA | Medium | Enforcement risk, fine exposure |
| Data minimisation | Audit and remove unnecessary fields | Low | Minor violation, reputation risk |
| Automated retention | Configure ATS deletion rules | Low-Medium | Most common GDPR violation |
| AI screening documentation | Log all AI decisions with explainability | Medium | Article 22 violation, AI Act overlap |
| SAR response process | Documented 30-day process | Medium | Regulatory action for late or incomplete response |
| DPA for all processors | Contract review and DPA execution | Medium | Liability for third-party violations |

## Forward outlook 2026-2030

Joint EU AI Act + GDPR investigations begin in 2026, automated retention becomes a mandatory ATS feature by 2027, right-to-erasure workflows become fully automated by 2028, and by 2030 privacy-by-design becomes a disqualifying ATS procurement criterion in the EU market.