DPIA template.

A data protection impact assessment for AI interviews, prefilled with what testee does, for your company to complete.

Updated 15 November 2026

Arcolabs OÜ, registry code 17587452, Sepapaja tn 6, 15551 Tallinn, Estonia · hello@testee.ai

Interviewing candidates with an AI system is processing that usually needs a data protection impact assessment under GDPR Article 35: it evaluates people with new technology, in a relationship where they can't easily say no. Under the EU AI Act, deployers of high-risk AI use the provider's information for it.

We've filled in what testee does. Everything marked [Company] is yours: your purpose, your settings, your view of the risks and the sign-off. Arcolabs OÜ can answer questions about testee for your assessment at hello@testee.ai.

About this assessment.

- **Controller.** [Company name, address, contact].
- **Data protection officer.** [Name and contact, or "none appointed"].
- **Processor.** Arcolabs OÜ, registry code 17587452, Sepapaja tn 6, 15551 Tallinn, Estonia, hello@testee.ai, under the testee Data processing agreement.
- **Assessed by.** [Name, role], on [date]. Next review: [date, at least yearly and whenever the use changes].
- **Scope.** [Roles, countries and number of candidates a year interviewed with testee].

The processing.

- **Purpose.** Structured first-round interviews: an AI interviewer asks the questions the company set and follow-ups, and the analysis shows the team how the answers covered

its expectations, with evidence. [Company: why you interview this way, for example consistent first rounds at volume, or flexible times for candidates.]

- **Steps.** Invitation (by hand, a CSV import, the API or a connected applicant tracking system); sign-in with a code emailed to the candidate; the AI notice and consent; the interview by voice or text; the analysis; the team's review and decision; sharing within the team; retention and deletion.
- **People.** Candidates for [roles], aged 16 or over; the company's team members who review them.
- **Data.** Name and email; optional headline and external id; interview audio and transcript; quiz answers, code, whiteboard drawings, written answers and review comments; integrity signals (sizes and times, never content) if on; camera and screen recordings if turned on; the consent record (time, versions and a hash of the texts; no IP address or user agent); the candidate's feedback; the team's reviews, decisions and comments.
- **Special categories.** Not intended, and the AI never infers them. A voice or a video can reveal some (health, origin); no AI processes the video. Accommodation requests can involve health data: [Company: how you handle them, outside testee].
- **Recipients.** The company's team members by role and permission; Arcolabs OÜ; the sub-processors Google Cloud and Firebase (EU), OpenAI (US: interviewer, transcription, analysis; it also gets the browser's connection data, such as the IP address, because the voice goes to it directly), Resend (US: emails) and, only if your company uses the video avatar (Enterprise), Anam (US or EU: the avatar, which gets the interviewer's voice and the connection data, never the candidate's audio or video); Arcolabs OÜ also counts visits to the interview pages for its own statistics, as their controller, without cookies and only as totals (Plausible Analytics, in the EU); [Company: tools you connect, such as your applicant tracking system, Slack or webhooks, and people you share results with].
- **Transfers.** Data is stored in the EU. Transfers to the US rely on the EU–US Data Privacy Framework or the Standard Contractual Clauses. OpenAI doesn't use the data to train its models.
- **Retention.** Defaults: candidates with no activity are erased after 365 days; audio and recordings are deleted 180 days after the interview; the audit log is kept 365 days; testee's AI log (ids, models, versions, statuses and times, no names or content) 190 days after its last entry, which you download to keep your own copy for six months. [Company: your settings and why.]

Lawful basis and transparency.

- **Interviews.** [Company: your basis, for example steps at the candidate's request before a contract (Art. 6(1)(b)) or legitimate interests (Art. 6(1)(f)) with a balancing test. Consent is rarely freely given in hiring.] testee records the candidate's acceptance of the AI notice before every interview, whatever basis you rely on.
- **Camera and screen recording.** Off by default. [Company: whether you turn it on, why it's necessary and your basis.] testee shows the recording notice and records explicit agreement before the interview.
- **Integrity signals.** Off by default; if turned on, candidates are told before they consent. In the EU, the EEA and the UK reading these browser events needs the candidate's consent under ePrivacy rules, so candidates there are asked to agree first, with a checkbox of its own they can leave unticked; without their agreement the interview runs without these notes. [Company: on or off, and why.]
- **No solely automated decisions.** The coverage score is for review; people make every decision and can change any status (GDPR Art. 22). [Company: who reviews, how, and how candidates ask for a human review.]
- **Transparency.** testee's AI notice before the interview. [Company: your notice and where you give it; see the candidate notice templates.]

Necessity and proportionality.

- **Minimal data.** The analysis gets the transcript and the work, never names or emails. No IP address or user agent is kept with a session. Integrity signals record sizes and times, never what was copied or typed.
- **Less intrusive options.** Candidates can type instead of speaking. Camera and screen recording are off unless the company turns them on. [Company: the other ways to be assessed you offer.]
- **Accuracy.** Every status comes with its evidence and reviewers can correct it. Arabic, Dutch, English, German, Hebrew, Italian, Spanish and Urdu are evaluated; Brazilian Portuguese, French, Hindi, Indonesian and Simplified Chinese are in beta. [Company: the languages you use.]

- **Rights.** Export and erasure of a candidate in one step, retention settings per company, human review on request. [Company: your process and deadlines for requests.]

Risks to candidates.

For each risk: what testee does, then your likelihood, severity and measures. [Company: rate each as low, medium or high.]

- **Unfair results for some groups.** For example by accent, disability, first language, age, sex or origin. The analysis judges what was said against the company's expectations and is forbidden to judge accent, fluency or personality; humans decide. [Company: likelihood, severity, your measures, such as reviewing outcomes by group and a bias audit where the law requires one.]
- **Transcription errors.** They can turn into wrong statuses. The analysis reads them charitably; the audio and evidence are there for reviewers; text mode is offered. [Company: …]
- **Over-reliance on the score.** Labeled "for review, not a hiring decision"; there's no automatic rejection. [Company: reviewer training and your review rule.]
- **Candidates not understanding the AI.** The AI notice before every interview, with consent recorded. [Company: your notice.]
- **Integrity signals read as cheating.** Signals have no score, carry "Signals, not proof" and a note about assistive technology, and reviewers mark them explained or dismissed. [Company: …]
- **Intrusive recording.** Camera and screen are off by default, for human review only, every viewing audit-logged. [Company: …]
- **Other people recorded.** The microphone is on only during the interview. [Company: ask candidates for a private place.]
- **Inaccessible interviews.** Text mode, captions and keyboard use; whiteboard and code editor limits stated in the accessibility statement. [Company: your accommodation process.]
- **A data breach.** Encryption in transit and at rest, per-company access checks, two-factor sign-in, audit logs, breach notice to you within 48 hours. [Company: who may access results.]

- **Keeping data too long.** Retention enforced daily by testee. [Company: your settings.]
- **Transfers to the US.** DPF or SCCs, no training on the data, OpenAI keeps API data at most 30 days for abuse monitoring. [Company: …]

Your measures.

- [Reviewers trained in how testee works and its limits, with these instructions: names or roles.]
- [A written review rule: no decision on the score alone; how a decision is recorded.]
- [Notices given, where and when.]
- [Accommodations: who handles requests and how fast.]
- [Retention settings and data request handling.]
- [Who has which role in testee, reviewed on joining and leaving.]
- [The Data processing agreement accepted, the sub-processors reviewed.]

Outcome and sign-off.

- **Residual risk.** [Low / medium / high], because [reasons].
- **Prior consultation.** [Needed / not needed]. If high risk remains after your measures, consult your data protection authority before you start (GDPR Art. 36).
- **Data protection officer's advice.** [Advice, and whether it was followed.]
- **Candidates' views.** [How you sought them, for example feedback after the interview, or why not.]
- **Approved by.** [Name, role, date].