

DPIA Summary

Firstview • Version 1.0 • Updated: 20 October 2026

This is a summary of Firstview's data protection impact assessment (DPIA) for its hiring platform. Customers are the controllers of candidate data and must make their own DPIA where the law requires one; this summary is meant to help with that. It follows Article 35 of the GDPR and also covers Turkish law (KVKK).

1. The processing

Firstview processes candidate data for its customers to run hiring: CV screening against the customer's criteria, AI voice and video interviews with recordings and transcripts, AI interview reports, meeting recording and notes, candidate search (including a sourcing index of public professional profiles), messages to candidates by email and WhatsApp, and an in-app assistant.

People affected: job candidates, people found through sourcing, the customer's users, and other meeting participants.

Data: contact and identity details, CVs and work history, interview audio, video, screen shares and transcripts, AI-generated results, proctoring events, and hiring workflow data. Special category data is not requested, but candidates may volunteer it. Annex I of our DPA has the full list.

Why a DPIA is needed: the processing uses AI to evaluate people for jobs (a high-risk AI system under the EU AI Act), involves systematic evaluation of personal aspects, processes data of people in a weaker position (candidates), and includes large-scale collection of public profiles.

2. Necessity and proportionality

- **Purpose limitation.** Data is used only to run the customer's hiring process (and, for sourcing, to let customers find candidates). It is not used to train AI models, sold or used for advertising.
- **Minimisation.** The AI assesses only against criteria and competencies the customer sets for the job. The interviewer does not ask follow-ups on protected topics. No face, emotion or personality analysis is done. Proctoring records events (such as tab changes), not continuous screen or camera analysis.
- **Lawful basis.** Set by the customer: usually steps before an employment contract or legitimate interest, and explicit consent before the online interview where Turkish law requires it. For the sourcing index, Firstview relies on its legitimate interest, limited to information people made public for professional purposes.
- **Transparency.** Candidates are told they are interviewed by an AI. We publish a candidate privacy notice, an AI notice and this summary.
- **Rights.** Access, correction, deletion, objection and human review can be requested from the customer or from security@firstview.ai. Sourced people can have their profile removed and blocked from future searches.

3. Risks and measures

Risk to people	Measures in place	Remaining risk
An unfair or wrong AI result harms a candidate's chances	People make every decision; every result has reasons and evidence; recordings and transcripts stay available; candidates can ask for human review; changes are tested before release.	Medium. Reviewers may still rely too much on the AI. No formal bias audit yet.
Discrimination on protected characteristics	Interviewer avoids protected topics; reports describe behaviour, not emotional state or personality; no face analysis.	Medium; high where a customer uses age or gender criteria. CV screening evaluates these if a customer writes them, and may estimate age from CV dates and gender from the name. The customer chooses the criteria and is responsible for their lawfulness. Action: section 4.
Speech recognition errors affect the result	Transcripts and recordings can be checked; backups if the main speech provider fails.	Medium for strong accents and poor connections.
Unauthorised access to candidate data	Encryption in transit and at rest; private files behind expiring signed links; customer isolation; role-based access; private network and VPN for infrastructure; secrets manager; breach plan with 48-hour customer notice.	Low to medium. Multi-factor login is not yet available.
Candidates feel watched or are wrongly suspected of cheating	Proctoring events are disclosed, shown in context and do not change the AI assessment; the camera check measures only brightness.	Low to medium. Reviewers may misread an innocent event.
Data kept longer than needed	Customers decide retention; deletion on request within 30 days; deletion within 30 days after the contract ends.	Medium. No automatic retention schedule yet.
Transfers outside the EU and Türkiye	Database and servers in the EU; EU Standard Contractual Clauses; KVKK standard contracts to be signed with each provider; no model training; zero data retention at AI providers where offered. See the transfer impact summary.	Low to medium. Recordings and some AI processing are in the US.
Sourced people do not know they are in the index	Only public professional data; removal and blocking on request.	Medium. People are not yet told individually when they are added.

4. Actions

Action	Status
Warn about or block age and gender criteria in CV screening	Planned before 2 December 2027
Automatic retention schedule (interview videos 6 months, transcripts 12 months)	Planned
Multi-factor login, which organizations can require	Planned
Notice to people added to the sourcing index	Planned
Bias audit and published accuracy figures for the EU AI Act	Planned before 2 December 2027
Move remaining US processing to the EU where providers allow	In progress

5. Conclusion

With the measures above, the processing can go ahead. We review this assessment when the processing changes in a meaningful way, and at least once a year.

Owner: Barkin Kutucu, Firstview. Contact: security@firstview.ai