

Data Processing Agreement

Firstview • Version 1.0 • Updated: 19 October 2026

This Data Processing Agreement ("DPA") forms part of the agreement under which Firstview provides its hiring platform to the Customer (the "Agreement"). It applies whenever Firstview processes Customer Personal Data on the Customer's behalf. If this DPA and the Agreement conflict, this DPA wins on data protection matters.

1. Parties

- **Customer:** the organization that signed the Agreement, acting as controller (or as processor for its own clients, in which case Firstview is its sub-processor).
- **Firstview:** the Firstview entity that signed the Agreement, acting as processor. That is either Firstview Technology and Consulting Inc. (Delaware, United States) or Firstview Teknoloji ve Danışmanlık A.Ş. (Istanbul, Türkiye; MERSİS 0386106881500001).

2. Definitions

"Data Protection Law" means every law that applies to the processing under this DPA, including the EU General Data Protection Regulation 2016/679 ("GDPR"), the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection, Turkish Law No. 6698 on the Protection of Personal Data ("KVKK") and the California Consumer Privacy Act as amended ("CCPA").

"Customer Personal Data" means personal data that Firstview processes on the Customer's behalf to provide the Services. "Personal Data Breach", "processing", "controller", "processor", "data subject" and "supervisory authority" have the meanings given in the GDPR (or the equivalent terms in other Data Protection Law). "Sub-processor" means a third party Firstview engages to process Customer Personal Data.

3. Processing on instructions

3.1 Firstview processes Customer Personal Data only on the Customer's documented instructions. The Agreement, this DPA and the Customer's use and configuration of the Services are the Customer's complete instructions. Further instructions must be in writing and consistent with the Agreement.

3.2 Firstview will tell the Customer if it believes an instruction breaks Data Protection Law, or if law requires Firstview to process data in another way (unless that law forbids telling the Customer).

3.3 The subject matter, duration, nature and purpose of the processing, and the types of data and data subjects, are set out in Annex I.

3.4 The Customer is responsible for having a lawful basis for the processing, for giving candidates the notices the law requires (including that they are interviewed or assessed by an AI system), and for the criteria and questions it configures in the Services.

4. No model training

Firstview does not use Customer Personal Data to train or improve AI models, and does not allow its Sub-processors to do so. Firstview configures every AI provider it uses to refuse training on the data it sends.

5. Confidentiality

Firstview gives access to Customer Personal Data only to staff who need it to provide, support or secure the Services. All of them are bound by a duty of confidentiality.

6. Security

Firstview keeps the technical and organizational measures in Annex II. Firstview may update those measures over time, but will not lower the overall level of protection.

7. Sub-processors

7.1 The Customer gives general authorization for Firstview to use Sub-processors. The current list, with each Sub-processor's purpose and region, is at <https://firstview.ai/trust#subprocessors> (also available as RSS and JSON feeds).

7.2 Firstview will tell the Customer at least 30 days before adding or replacing a Sub-processor, through the feeds above and by email to the Customer's account owner. The Customer may object on reasonable data protection grounds within that period. The parties will then discuss the objection in good faith. If they cannot resolve it, the Customer may end the affected part of the Services and receive a refund of prepaid fees for the unused period.

7.3 Firstview signs a written contract with each Sub-processor with data protection terms no less protective than this DPA. Firstview remains responsible for its Sub-processors.

8. Data subject requests

Firstview will help the Customer answer requests from data subjects to exercise their rights (access, correction, deletion, restriction, portability, objection, and the right not to be subject to a decision based solely on automated processing). If Firstview receives a request directly, it will pass it to the Customer without undue delay and will not answer it except on the Customer's instructions.

9. Personal Data Breaches

9.1 Firstview will tell the Customer without undue delay, and in any case within 48 hours, after it becomes aware of a Personal Data Breach affecting Customer Personal Data.

9.2 The notice will describe, as far as known at the time: what happened, the categories and approximate number of people and records affected, the likely consequences, and the steps taken or proposed. Firstview will send further information as it learns more.

9.3 Firstview will take reasonable steps to contain the breach and limit its effects, and will help the Customer meet its own obligations to notify supervisory authorities and data subjects. Notice under this section is not an admission of fault.

10. Assistance

Taking into account the nature of the processing and the information available to it, Firstview will give the Customer reasonable help with data protection impact assessments and prior consultations with supervisory authorities. Firstview publishes a DPIA summary, a transfer impact summary and a system card at <https://firstview.ai/trust>.

11. Deletion and return

11.1 During the Agreement the Customer can export its data or ask Firstview to delete specific records at any time by writing to security@firstview.ai. Firstview will complete the deletion within 30 days.

11.2 Within 30 days after the Agreement ends, Firstview will delete all Customer Personal Data, unless the Customer asks for a copy first or law requires Firstview to keep it. Data in encrypted backups is deleted when those backups expire on their normal cycle and is not restored in the meantime except to recover from a failure.

12. Audits

12.1 Firstview will make available the information needed to show compliance with this DPA, including written answers to the Customer's reasonable security questionnaires (at most once a year, unless after a Personal Data Breach or at a supervisory authority's request).

12.2 If that information is not enough to show compliance, or a supervisory authority requires it, the Customer (or an independent auditor bound by confidentiality) may audit Firstview once a year, with 30 days' written notice, during business hours and at the Customer's cost. The parties will agree the scope in advance, and the audit must not access other customers' data.

13. International transfers

13.1 Firstview and its Sub-processors process Customer Personal Data in the regions listed on the sub-processor list. Some of these are outside the European Economic Area, the United Kingdom, Switzerland and Türkiye.

13.2 **EU.** For transfers of Customer Personal Data subject to the GDPR to a country without an adequacy decision, the EU Standard Contractual Clauses (Commission Implementing Decision 2021/914) are incorporated by reference: Module Two where the Customer is a controller, Module Three where it is a processor. For the Clauses: the optional docking clause 7 applies; clause 9(a) Option 2 applies with the notice period in section 7.2; the optional wording in clause 11 does not apply; clauses 17 and 18 choose the law and courts of Ireland; Annexes I and II are Annexes I and II of this DPA, and Annex III is the sub-processor list.

13.3 **UK.** For transfers subject to the UK GDPR, the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner (version B1.0) applies. Table 1 is completed with the parties in section 1, Table 2 with the choices in section 13.2, Table 3 with Annexes I and II, and in Table 4 either party may end the Addendum as set out in its section 19.

13.4 **Switzerland.** For transfers subject to the Swiss Federal Act on Data Protection, the Clauses in section 13.2 apply with these changes: the competent supervisory authority is the Federal Data

Protection and Information Commissioner; references to "Member State" include Switzerland, so data subjects there can sue in Switzerland; and references to the GDPR include the Swiss Act.

13.5 Türkiye. For transfers of Customer Personal Data subject to KVKK to a country without an adequacy decision, the parties (and Firstview with its Sub-processors) will use the standard contracts published by the Personal Data Protection Board, unchanged, as Article 9 of KVKK and the Regulation on the Procedures and Principles for the Transfer of Personal Data Abroad require. The party that makes the transfer notifies the Board within 5 business days of signing.

13.6 If a transfer mechanism above is found invalid or replaced, the parties will move to a valid replacement.

14. California

Where the CCPA applies, Firstview is a service provider. Firstview will not: sell or share Customer Personal Data; keep, use or disclose it for any purpose other than providing the Services under the Agreement; keep, use or disclose it outside the direct business relationship with the Customer; or combine it with personal information it receives from other sources, except as the CCPA allows. Firstview will tell the Customer if it can no longer meet these obligations, and the Customer may then take reasonable steps to stop unauthorized use. Firstview understands and will comply with these restrictions.

15. General

This DPA lasts as long as Firstview processes Customer Personal Data. Each party's liability under this DPA is subject to the limits in the Agreement, except where Data Protection Law does not allow them. This DPA is governed by the law that governs the Agreement, except where section 13 says otherwise.

Annex I: Description of the processing

Data exporter: the Customer (controller, or processor for its own clients). Contact: as stated in the Agreement.

Data importer: Firstview (processor). Contact: security@firstview.ai.

Data subjects

- Job candidates and applicants of the Customer
- People the Customer finds through candidate sourcing
- The Customer's users (recruiters, hiring managers, interviewers and administrators)
- Other participants in meetings the Customer records with the notetaker

Categories of personal data

- Identity and contact details: name, email, phone number, location, LinkedIn or other profile links

- CV and professional data: work history, education, skills, languages, certificates, salary expectations and other information in CVs and applications
- Interview data: audio and video recordings, screen shares, transcripts, answers to questions, and AI-generated summaries, scores and reports
- Proctoring events: the time and duration of tab changes, full-screen exits, lost window focus, camera-off, virtual cameras, multiple screens, wrong or ended screen shares and low light (measured from image brightness only); browser name and version
- Meeting data: recordings, transcripts and notes of meetings the Customer records
- Hiring workflow data: stages, notes, comments, scores and decisions made by the Customer's team
- User account and usage data: name, email, role, and logs of actions in the Services

Special categories: the Services are not designed to collect special category data, and Firstview does not ask for it. Candidates may volunteer it (for example, in a CV or an interview answer). The AI interviewer is instructed not to ask follow-up questions about protected characteristics.

Frequency: continuous, for as long as the Customer uses the Services.

Nature and purpose: to provide the Services under the Agreement: AI voice and video interviews, CV parsing and scoring, interview reports and candidate briefs, meeting recording and notes, candidate sourcing and search, the in-app assistant, notifications to candidates by email and WhatsApp, and the support, security and reliability of these Services.

Duration and retention: for the term of the Agreement, then deleted as described in section 11.

Sub-processors: as listed at <https://firstview.ai/trust#subprocessors>.

Annex II: Technical and organizational measures

Encryption

- All traffic to and between the Services uses TLS.
- The database and file storage encrypt data at rest with AES-256.
- Integration tokens (for example calendar and email connections) are encrypted with AES-256-GCM.

Access control

- CVs, recordings and transcripts are never public. They open only through signed links that expire.
- Each customer can see only its own data. Inside a customer, roles control what each user can see and change.
- Servers and the Kubernetes API are reachable only through a private network and VPN.
- Secrets are kept in a dedicated secrets manager, never in source code.
- Staff get access to production systems only when their work needs it.

Infrastructure

- The database runs in Frankfurt, Germany; application servers run in Germany and Finland.
- Services run without root privileges and with restricted permissions.
- The database is backed up every day.
- Requests from providers (webhooks) are signed and verified.

AI providers

- Every AI provider is configured to refuse training on Firstview's data.
- Model provider requests go through providers with zero data retention where they offer it.

Operations

- Errors are tracked and alerted on, so failures and unusual behaviour are found quickly.
- A written breach response plan names an owner and a backup and sets the 48-hour customer notice.
- Vulnerability reports are accepted at security@firstview.ai under a published disclosure policy, with a reply within 3 business days.
- Staff are bound by confidentiality.

Sub-processors

- Each Sub-processor signs data protection terms. The list, with regions, is public and changes are announced 30 days in advance.

Signatures

	Customer	Firstview
Name		
Title		
Date		
Signature		