LEGAL

Data processing agreement (DPA)

This is the template of a data processing agreement for a company (HR) processing candidate data on the Sizin Karyera platform. Legal entity details will be added after registration. Contact us for a signed copy or to discuss changes.

Last updated: 21 November 2026

This translation is provided for information. The Azerbaijani version is the authoritative text.

This is a template (draft). Legal entity details will be filled in after registration. Have it reviewed by counsel before signing.

1. Parties and roles

- “Company” means the employer registered or invited in the Sizin Karyera HR panel. “Platform” means the party providing the Sizin Karyera service (details to be published after registration).
- For data of candidates who apply to its vacancies, the Company determines the purposes and means of processing (controller). The Platform stores and processes that data on the Company’s behalf and under its instructions (authorised processor).
- For a candidate’s own account data (profile, CV, account, notifications), the Platform is separately responsible as described in the Privacy Policy.

2. Description of processing

- Subject matter: storing and displaying data so the Company can receive and assess applications to its vacancies and communicate with candidates.
- Data categories: name, email, phone, date of birth, links, CV content, motivation letter, answers to questions, exam results, exam and application video (when required), interview details, chat messages, Company notes (rating, comment, stage).
- Data subjects: candidates applying to the Company’s vacancies.
- Duration: while the Company’s account is active or until the data is deleted. Video recordings are deleted automatically after 14 days.

3. Company instructions

- The Platform processes candidate data only on the Company's instructions given through the panel, the Terms of Use and this agreement, and does not use it for its own purposes (such as advertising).
- If the Platform believes an instruction is unlawful, it informs the Company.

4. Confidentiality

Platform staff with access to candidate data are bound by confidentiality, and access is granted only when needed to provide the service and support.

5. Security measures

- The Platform applies reasonable technical and organisational measures: HTTPS, AES-256-GCM encryption of sensitive fields (CV contact details, messages, interview phone), role- and permission-based access, rate limiting, encrypted backups and service health monitoring.
- The current description of the measures is on the /security page and in the security questionnaire. The Platform may update the measures without reducing the protection of the data.

6. Sub-processors

- The Company authorises the Platform to use these sub-processors: Google/Firebase (sign-in and notifications), LiveKit (video interviews), a hosting provider (servers and backups in Finland) and an AI service provider (Anthropic; only when AI features are used).
- The Platform binds sub-processors to terms that protect data no less than this agreement. When a sub-processor is added or replaced, the Company is notified in advance (by email or on the website) and may object on reasonable grounds.

7. International transfers

Servers and encrypted backups are in Finland. Google/Firebase, the AI provider and some other sub-processors may process data in the United States and other countries. The Company acknowledges this and is responsible for informing candidates in its own privacy notice.

8. Assisting with candidate rights

- When a request arrives to access, correct or delete candidate data or to withdraw consent, the parties cooperate. When a candidate deletes their account, the Platform deletes or anonymises their personal data, and the Company deletes the copies it holds (exported files, correspondence).
- Requests can be sent to support@sizinkaryera.life.

9. Breach notification

- If the Platform detects a security breach affecting the Company's candidate data, it informs the Company without undue delay and, where possible, within 72 hours, and provides what is known (affected data, likely consequences, measures taken).
- The Company reports suspected account takeover or data leakage to support@sizinkaryera.life immediately.

10. Deletion and return

- When the service ends or on the Company's request, the Company may export its data using the panel's features, and the Platform deletes the Company's data. Deleted data may remain in encrypted backups for about 30 days and is then removed automatically.
- Cases where the law requires retention are an exception.

11. Audit and documentation

On the Company's reasonable request, the Platform provides information showing compliance with this agreement, including answers to the security questionnaire. On-site audits are agreed in advance and must not unreasonably disrupt the Platform's operations.

12. Liability, governing law and contact

- Liability, governing law and dispute resolution follow the company part of the Terms of Use. This agreement is interpreted in line with the personal data legislation of the Republic of Azerbaijan.
- Contact: support@sizinkaryera.life