SVAYZ LTD

Data Processing Agreement

Employer and Recruitment Agency Customers

Version 1.3

Last updated: 11 March 2026

Effective date: 26 February 2026

Parties

This Data Processing Agreement ("**DPA**") is entered into between:

(1) SVAYZ Ltd, a company incorporated in England and Wales under company number 17001057 and registered office at 124-128 City Road, London, England, EC1V 2NX, United Kingdom ("**SVAYZ**"); and

(2) The Customer identified in the Terms of Service for Employers and Recruitment Agencies (the "**Customer**").

This DPA is incorporated into and forms part of the Terms of Service for Employers and Recruitment Agencies (the "**Principal Agreement**"). In the event of a conflict between this DPA and the Principal Agreement, this DPA shall prevail in respect of data protection matters.

1. Definitions

1.1 In this DPA, the following terms have the following meanings:

Term	Definition
"Applicable Data Protection Laws"	The UK GDPR, the EU GDPR, the Data Protection Act 2018, and any other applicable laws relating to the processing of personal data and the privacy of individuals, as amended or replaced from time to time.
"Candidate Data"	Personal data relating to candidates that is processed by SVAYZ on behalf of, or jointly with, the Customer in connection with the Customer's use of the Platform. The categories of data are set out in Annex 1.
"Controller"	Has the meaning given in Article 4(7) of the UK/EU GDPR.
"Data Subject"	An identified or identifiable natural person to whom Candidate Data relates (i.e. a candidate).
"EEA"	The European Economic Area.
"IDTA"	The International Data Transfer Agreement issued by the ICO under Section 119A of the Data Protection Act 2018.
"Joint Controller Processing"	The processing activities in respect of which SVAYZ and the Customer act as joint controllers, as described in Section 4.

"Personal Data Breach"	Has the meaning given in Article 4(12) of the UK/EU GDPR.
"Processor"	Has the meaning given in Article 4(8) of the UK/EU GDPR.
"Processor Processing"	The processing activities in respect of which SVAYZ acts as the Customer's processor, as described in Section 3.
"SCCs"	The Standard Contractual Clauses for the transfer of personal data to third countries approved by the European Commission under Commission Implementing Decision (EU) 2021/914.
"Sub-processor"	A third party engaged by SVAYZ to process Candidate Data on behalf of the Customer.
"UK Addendum"	The International Data Transfer Addendum to the EU SCCs issued by the ICO.

1.2 Terms not defined in this DPA shall have the meaning given to them in the Principal Agreement or, failing that, in the Applicable Data Protection Laws.

2. Roles of the Parties

2.1 The parties acknowledge that, in respect of Candidate Data processed through the Platform, the relationship between SVAYZ and the Customer is not a simple controller-processor relationship. The nature of the Platform means that different processing activities attract different data protection roles. The parties' respective roles are as follows:

Processing Activity	SVAYZ Role	Customer Role	Rationale
Hosting and storing Candidate Data uploaded by or on behalf of candidates	**Processor**	**Controller**	Customer determines the purposes of accessing and reviewing candidate applications
Providing pipeline management tools (tracking candidates through recruitment stages)	**Processor**	**Controller**	Customer determines the processing purposes; SVAYZ provides the technical means
AI candidate ranking, scoring, and matching (determining evaluation methodology, algorithms, and criteria)	**Joint Controller**	**Joint Controller**	SVAYZ independently determines the AI methodology; Customer determines which roles and candidates are evaluated
AI-conducted interviews (interview	**Joint Controller**	**Joint Controller**	SVAYZ designs the interview system and

design, recording, transcription, assessment)			assessment logic; Customer enables the feature and determines the role requirements
AI content generation (job descriptions, candidate summaries)	**Processor**	**Controller**	Customer initiates generation and determines the use of the output
Platform analytics and service improvement (aggregated, anonymised data)	**Controller**	**N/A**	SVAYZ determines purposes independently. Anonymised data falls outside GDPR scope.

3. SVAYZ as Processor -- Article 28 Terms

This Section 3 applies to the Processor Processing (i.e. those processing activities where SVAYZ acts as the Customer's processor, as identified in the table in Section 2).

3.1 Customer's Instructions

3.1.1 SVAYZ shall process Candidate Data only on the documented instructions of the Customer (the "**Instructions**"), unless required to do so by applicable law, in which case SVAYZ shall (to the extent permitted by law) inform the Customer of that legal requirement before processing.

3.1.2 The Customer's Instructions are set out in:

(a) this DPA and the Principal Agreement;

(b) the Customer's configuration of the Platform (including the selection of features, roles posted, and candidates processed); and

(c) any additional written instructions agreed between the parties from time to time.

3.1.3 If SVAYZ considers that an instruction from the Customer infringes Applicable Data Protection Laws, SVAYZ shall promptly inform the Customer. SVAYZ is not obliged to assess the legality of the Customer's instructions but shall not knowingly process data in a manner that it believes to be manifestly unlawful.

3.2 Confidentiality

3.2.1 SVAYZ shall ensure that all persons authorised to process Candidate Data are subject to a binding obligation of confidentiality (whether contractual or statutory).

3.3 Security Measures

3.3.1 SVAYZ shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the UK/EU GDPR. The current security measures are described in **Annex 2**.

3.3.2 SVAYZ may update the security measures from time to time, provided that the updated measures do not materially decrease the overall level of protection.

3.4 Sub-processing

3.4.1 The Customer provides **general written authorisation** for SVAYZ to engage Sub-processors for the Processor Processing, subject to this Section 3.4.

3.4.2 The current list of Sub-processors is set out in **Annex 3**. SVAYZ shall make the current list available to the Customer upon request and shall update it when Sub-processors are added or replaced.

3.4.3 SVAYZ shall notify the Customer at least **30 days** in advance of any intended addition or replacement of a Sub-processor, providing the Customer with an opportunity to object.

3.4.4 If the Customer reasonably objects to a new Sub-processor on legitimate data protection grounds, the parties shall discuss the Customer's concerns in good faith. If no resolution can be reached within 30 days, the Customer may terminate the Principal Agreement without penalty by giving written notice.

3.4.5 SVAYZ shall impose on each Sub-processor, by way of a written contract, data protection obligations no less onerous than those imposed on SVAYZ under this DPA. SVAYZ shall remain fully liable to the Customer for the performance of any Sub-processor's obligations.

3.5 Data Subject Rights

3.5.1 SVAYZ shall, taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures (insofar as this is possible) in responding to requests from Data Subjects exercising their rights under Chapter III of the UK/EU GDPR.

3.5.2 If SVAYZ receives a request from a Data Subject directly, SVAYZ shall promptly notify the Customer and shall not respond to the request unless instructed to do so by the Customer (except to acknowledge receipt and inform the Data Subject that their request has been forwarded to the relevant controller).

3.5.3 The Platform provides self-service tools enabling Data Subjects to exercise certain rights (including access, rectification, deletion, and data portability). SVAYZ shall maintain and make available these tools throughout the term of the Principal Agreement.

3.6 Personal Data Breach Notification

3.6.1 SVAYZ shall notify the Customer **without undue delay** (and in any event within **48 hours**) upon becoming aware of a Personal Data Breach affecting Candidate Data processed under the Processor Processing.

3.6.2 The notification shall include, to the extent available:

(a) a description of the nature of the breach, including the categories and approximate number of Data Subjects and records concerned;

(b) the name and contact details of SVAYZ's data protection contact;

(c) a description of the likely consequences of the breach; and

(d) a description of the measures taken or proposed to be taken to address the breach and to mitigate its possible adverse effects.

3.6.3 SVAYZ shall cooperate with the Customer and take reasonable steps to assist in the investigation, mitigation, and remediation of the breach.

3.7 Assistance with Compliance

3.7.1 SVAYZ shall, taking into account the nature of the processing and the information available to SVAYZ, provide reasonable assistance to the Customer in ensuring compliance with the Customer's obligations under Articles 32 to 36 of the UK/EU GDPR (security, breach notification, data protection impact assessments, and prior consultation).

3.8 Audit Rights

3.8.1 SVAYZ shall make available to the Customer all information reasonably necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits, including inspections, conducted by the Customer or a third-party auditor mandated by the Customer.

3.8.2 The Customer shall give SVAYZ at least **30 days' prior written notice** of any audit. Audits shall be conducted during normal business hours, shall not unreasonably disrupt SVAYZ's operations, and shall be subject to reasonable confidentiality obligations.

3.8.3 The Customer shall bear the costs of any audit, unless the audit reveals a material breach of this DPA by SVAYZ, in which case SVAYZ shall bear the reasonable costs.

3.8.4 Where SVAYZ obtains an independent third-party audit report or certification (e.g. SOC 2 Type II or ISO 27001) in the future, SVAYZ may satisfy the Customer's audit request by providing a copy of such report, subject to confidentiality, as an alternative to an on-site audit. As at the date of this DPA, no such certification has been obtained.

3.9 Data Deletion and Return

3.9.1 Upon termination or expiry of the Principal Agreement, SVAYZ shall, at the Customer's election:

> **(a)** return all Candidate Data to the Customer in a commonly used, machine-readable format; or
>
> **(b)** delete all Candidate Data (including all copies) from SVAYZ's systems.

3.9.2 The Customer must notify SVAYZ of its election within **30 days** of termination. If no election is received, SVAYZ shall delete all Candidate Data within 90 days of termination.

3.9.3 SVAYZ may retain Candidate Data to the extent required by applicable law (including tax, regulatory, or litigation hold requirements), provided that SVAYZ shall: (a) limit such retention to the minimum necessary; (b) continue to protect the data in accordance with this DPA; and (c) delete the data when the retention obligation expires.

4. Joint Controller Arrangement -- Article 26 Terms

This Section 4 applies to the Joint Controller Processing (i.e. AI candidate ranking, scoring, matching, and AI-conducted interviews), where SVAYZ and the Customer act as joint controllers within the meaning of Article 26 of the UK/EU GDPR.

4.1 Respective Responsibilities

Obligation	SVAYZ Responsibility	Customer Responsibility
Transparency / Privacy notices	SVAYZ provides the AI Transparency Notice and Privacy Policy to candidates, explaining the AI processing, logic involved, and Data Subject rights.	Customer shall ensure its own privacy notice references the use of SVAYZ's AI features and directs candidates to SVAYZ's disclosures.
Lawful basis	SVAYZ conducts and maintains a Legitimate Interest Assessment (LIA) for AI features (or is in the process of completing one where a feature is newly introduced).	Customer ensures it has its own lawful basis for requiring candidates to undergo AI processing (including mandatory AI interviews).
Data Subject rights	SVAYZ provides self-service tools for candidates to exercise rights (access, deletion, portability, objection, human review). SVAYZ is the primary point of contact for candidates.	Customer cooperates with SVAYZ in responding to requests. Customer honours candidates' right to object and right to human review.
Data Protection Impact Assessment (DPIA)	SVAYZ conducts and maintains a DPIA for the AI features.	Customer may need to conduct its own DPIA for its specific use of AI features. SVAYZ shall provide information reasonably necessary to support the Customer's DPIA.
Security	SVAYZ implements and maintains technical and organisational security measures (see Annex 2).	Customer secures access to Platform accounts and ensures Authorised Users follow security practices.
Breach notification	SVAYZ notifies the Customer within 48 hours of becoming aware of a breach, notifies the ICO/supervisory authority where required, and notifies affected Data Subjects (candidates) where required under Article 34 of the UK/EU GDPR, as SVAYZ is the primary contact point for candidates.	Customer notifies its own supervisory authority and affected Data Subjects where required in respect of data under its control. Customer cooperates with SVAYZ in respect of any breach affecting the Joint Controller Processing.

4.2 Contact Point for Data Subjects

4.2.1 In accordance with Article 26(1) of the UK/EU GDPR, the parties agree that **SVAYZ shall be the primary contact point** for Data Subjects (candidates) in respect of the Joint Controller

Processing. Candidates may exercise their rights by contacting SVAYZ at infra-admin@svayz.com.

4.2.2 Notwithstanding clause 4.2.1, Data Subjects retain the right to exercise their rights against either or both joint controllers, regardless of the allocation of responsibilities in this DPA (Article 26(3) UK/EU GDPR).

4.3 Essence of the Arrangement Made Available to Data Subjects

4.3.1 In accordance with Article 26(2) of the UK/EU GDPR, the essence of this joint controller arrangement shall be made available to Data Subjects through SVAYZ's AI Transparency Notice and Privacy Policy. The Customer shall include a summary in its own privacy notice or a link to SVAYZ's disclosures.

4.4 Automated Decision-Making Safeguards

4.4.1 The parties acknowledge that the Data (Use and Access) Act 2025 (amending the UK GDPR with effect from 5 February 2026) replaced Article 22 with new Articles 22A--22D. In respect of the Joint Controller Processing, the parties shall implement the following safeguards in accordance with Article 22C of the UK GDPR (as amended):

(a) providing candidates with clear information about automated decisions taken about them (including AI scores, rankings, and match results);

(b) enabling candidates to make representations about such decisions;

(c) enabling candidates to obtain human intervention from a competent decision-maker; and

(d) enabling candidates to contest automated decisions.

4.4.2 Where a Data Subject exercises their right to object under Article 21 of the UK/EU GDPR in respect of the Joint Controller Processing (including objection to processing based on legitimate interests), SVAYZ shall, as the primary contact point, assess the objection and cease the relevant processing unless SVAYZ demonstrates compelling legitimate grounds that override the Data Subject's interests, rights, and freedoms. SVAYZ shall inform the Customer of any upheld objection that affects the Customer's use of the Platform.

4.4.3 Where the Joint Controller Processing involves special category data (as defined in Article 9 of the UK/EU GDPR), including any biometric data derived from AI interview recordings, such processing shall only be carried out with the explicit consent of the Data Subject or where another Article 9 condition applies (Article 22B UK GDPR, as amended).

4.4.4 For candidates located in the European Economic Area, the stricter requirements of Article 22 of the EU GDPR shall continue to apply.

4.5 EU AI Act Compliance

4.5.1 The parties acknowledge that AI systems used in recruitment are classified as high-risk AI systems under Annex III, Category 4 of the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), with obligations becoming enforceable from 2 August 2026.

4.5.2 In respect of the Joint Controller Processing involving AI, the parties' respective obligations under the EU AI Act are as follows:

(a) SVAYZ, as the provider of the AI system, shall comply with the obligations applicable to providers of high-risk AI systems, including risk management (Article 9), data governance (Article 10), technical documentation (Article 11), transparency (Article 13), human oversight measures (Article 14), and accuracy and robustness testing (Article 15).

(b) The Customer, as a deployer of the AI system, shall comply with the obligations applicable to deployers, including ensuring human oversight (Article 26(2)), monitoring AI operation (Article 26(5)), and maintaining logs for a minimum of six months (Article 26(6)).

4.5.3 The Platform's AI features do not perform emotion recognition, social scoring, real-time biometric identification, or any other practice prohibited under Article 5 of the EU AI Act.

4.5.4 SVAYZ shall ensure that all employers and recruitment agencies using the Platform's AI features have a sufficient level of AI literacy, in accordance with Article 4 of the EU AI Act.

4.6 Bias Monitoring and Equality Act 2010

4.6.1 SVAYZ is committed to conducting regular bias audits of its AI systems across protected characteristic proxies (as defined in the Equality Act 2010) to identify and mitigate potential disparate impact.

4.6.2 SVAYZ has completed a Data Protection Impact Assessment (DPIA) for its Application Quality Intelligence system and is completing DPIAs for its remaining AI features that process Candidate Data and shall maintain these DPIAs throughout the term of the Principal Agreement. Summaries of relevant DPIAs are available to the Customer upon reasonable request.

4.6.3 The Customer shall not use AI outputs to discriminate against candidates on the basis of any protected characteristic, and shall maintain auditable records of meaningful human review for hiring decisions that relied on Platform AI outputs.

5. International Data Transfers

5.1 SVAYZ shall not transfer Candidate Data to a country outside the United Kingdom or the EEA unless:

(a) the transfer is to a country that has been deemed to provide an adequate level of data protection by the UK Secretary of State (for UK GDPR transfers) or by the European Commission (for EU GDPR transfers);

(b) appropriate safeguards have been implemented in accordance with Chapter V of the UK/EU GDPR, including:

(i) the UK IDTA or UK Addendum to the EU SCCs (for transfers governed by the UK GDPR); and/or

(ii) the EU SCCs (for transfers governed by the EU GDPR); or

(c) a derogation under Article 49 of the UK/EU GDPR applies.

5.2 The current international transfers arising from SVAYZ's use of Sub-processors are described in Annex 3. SVAYZ shall conduct and maintain a Transfer Impact Assessment (TIA) in respect of transfers to countries that do not benefit from an adequacy decision.

5.3 Where transfers are made on the basis of SCCs or the IDTA, these are incorporated by reference into this DPA. In the event of a conflict between this DPA and the transfer mechanism, the transfer mechanism shall prevail.

6. General Provisions

6.1 Liability

6.1.1 Each party's liability under this DPA shall be subject to the limitations and exclusions of liability set out in the Principal Agreement, except that:

(a) liability for breach of Applicable Data Protection Laws shall not be subject to any financial cap; and

(b) liability for regulatory fines imposed on a party shall be borne by the party whose action or omission gave rise to the fine.

6.2 Term and Survival

6.2.1 This DPA shall remain in force for the duration of the Principal Agreement and shall automatically terminate when SVAYZ ceases to process Candidate Data on behalf of or jointly with the Customer.

6.2.2 The obligations under Sections 3.6 (Breach Notification), 3.9 (Data Deletion and Return), and 6.1 (Liability) shall survive termination.

6.3 Governing Law

6.3.1 This DPA shall be governed by and construed in accordance with the law of **England and Wales**. The courts of England and Wales shall have exclusive jurisdiction.

6.4 Amendments

6.4.1 SVAYZ may update this DPA from time to time to reflect changes in Applicable Data Protection Laws, regulatory guidance, or SVAYZ's processing activities. SVAYZ shall provide the Customer with at least 30 days' notice of material amendments.

7. Data Protection by Design and by Default (Article 25)

7.1 SVAYZ implements data protection by design and by default in accordance with Article 25 of the UK/EU GDPR. The following measures are embedded in the Platform's architecture:

7.1.1 Human-in-the-loop architecture: The Platform enforces meaningful human oversight of all AI-generated outputs. No candidate is automatically rejected, excluded, or deprioritised based on AI output alone. Application status changes (shortlisted, rejected, interview) can only be triggered by explicit human action, enforced at the application layer.

7.1.2 Data minimisation: The Platform implements selective field loading and public field whitelists to ensure that AI features and public-facing views process only the data fields directly relevant to the processing purpose. Candidate data not relevant to a specific assessment (e.g., bookmark history, notification preferences) is excluded from AI processing.

7.1.3 Privacy by default: The Platform is configured to protect privacy by default. Sentry error tracking is configured with `sendDefaultPii: false` to prevent accidental collection of personally identifiable information. Web analytics (Vercel Speed Insights) are gated behind explicit user consent and are not activated until affirmative consent is obtained.

7.1.4 Pseudonymisation on erasure: When a candidate exercises their right to erasure under Article 17, personal identifiers in AI audit logs are replaced with pseudonymous identifiers. The anonymised audit record is retained for the period required by the EU AI Act (Article 12), but can no longer be linked to the individual without additional information that has been deleted.

7.1.5 Access controls: Role-based access control (RBAC) is enforced server-side in all API routes and server actions. Employers can only access candidate data for roles they have posted. Administrative access is restricted and logged. Authentication is managed by a dedicated identity provider (Clerk) with multi-factor authentication support.

7.1.6 Encryption: All data is encrypted in transit (TLS 1.2+) and at rest (AES-256). Sensitive application data (such as OAuth tokens for calendar integrations) is additionally encrypted using AES-256-GCM with authenticated encryption.

Annex 1 -- Description of Processing

A. Categories of Data Subjects

Candidates aged 18 and over who create accounts on the Platform or whose data is uploaded by the Customer. The Platform is not intended for use by persons under 18 years of age.

B. Categories of Personal Data

Category	Examples
Identity data	Full name, email address, telephone number, professional title
Professional data	CV/resume, work history, skills, qualifications, certifications, education, languages
Application data	Job applications, cover letters, responses to screening questions
AI interview data	Video/audio recordings, transcripts, AI-generated interview assessments
AI assessment data	Suitability scores, rankings, match scores, AI-generated summaries
Account data	Account credentials (managed by Clerk), last active timestamp, Platform usage events
Communication data	Messages exchanged through the Platform between candidates and employers
Video introduction data	Candidate-recorded video introductions, duration, consent timestamps
LinkedIn verification data	LinkedIn profile snapshots and comparison results (where candidate opts in to verification)

Behavioural data	Client-side engagement metrics (e.g. time on page, scroll depth) collected during application
Search and browsing data	Search queries, directory lookups, profile view events, dismissed/saved jobs
Portfolio data	Project URLs, media, and links submitted by candidates
Calendar data	OAuth tokens and calendar event data for interview scheduling integrations
Chatbot data	Conversations with the Platform's AI assistant
AI audit data	Algorithmic decision audit logs, bias audit records, quality scoring audit trails
Offer and compensation data	Salary offers, signing bonuses, equity grants, negotiation history, candidate salary expectations
Consent and preference data	Cookie consent preferences, analytics/marketing consent status, notification preferences, profile visibility settings, consent audit trail

C. Special Category Data

SVAYZ does not intentionally collect special category data (Article 9 UK/EU GDPR) through its standard processing operations. However:

(a) Candidates may voluntarily include such data in free-text fields (e.g. disability status in a CV). Where this occurs, the Customer is responsible for ensuring a lawful basis under Article 9.

(b) AI interview recordings and video introductions capture audio and/or video of candidates. SVAYZ's AI interview analysis is limited to evaluating the substantive content and relevance of responses and does not perform facial recognition, emotion detection, physiognomic inference, or voice-based personality profiling. Where any future processing of interview recordings involves analysis of biometric characteristics beyond plain content analysis, SVAYZ shall obtain the candidate's explicit consent before processing.

(c) Candidates may optionally submit LinkedIn profile data for verification purposes. This data may reveal professional affiliations that could indirectly disclose protected characteristics. SVAYZ processes LinkedIn data solely for identity and employment verification and does not infer protected characteristics from it.

D. Processing Operations

Operation	Description	Legal Basis
Collection and storage	Receiving and storing Candidate Data uploaded by candidates or the Customer	Performance of contract / legitimate interests
AI ranking and scoring	Automated analysis of	Legitimate interests

	candidate data against role requirements to generate suitability scores	
AI interviews	Recording, transcription, and AI assessment of candidate interviews	Legitimate interests (mandatory) / consent (optional)
AI matching	Automated comparison of candidate profiles with role requirements	Legitimate interests
AI content generation	Generating CV summaries, job descriptions, and preparation tips	Performance of contract
Data sharing	Making Candidate Data available to the Customer through the Platform	Performance of contract
Retention and deletion	Retaining data per retention schedule; deleting upon request or schedule expiry	Legal obligation / legitimate interests

E. Retention

Candidate Data is retained in accordance with the following schedule:

- AI interview recordings (audio/video): **12 months** from the date of the interview, automatically deleted via daily scheduled cron job (including blob storage and vector embeddings)
- AI-generated scores, transcripts, and assessment summaries: **12 months** from the date of the interview
- AI audit logs (algorithmic decision records): **5 years** from the date of the decision, in accordance with EU AI Act record-keeping obligations. Personal identifiers are anonymised upon GDPR erasure request; anonymised audit records are retained for the full period.
- CV/resume data: Duration of candidate account; deleted upon account deletion or GDPR erasure request (30-day grace period for cancellation)
- Application data: Duration of the recruitment process; deleted upon account deletion or GDPR erasure request (30-day grace period)
- Video introductions: Duration of the application process; deleted upon account deletion or GDPR erasure request
- Account data: Duration of account; anonymised upon account deletion
- Communication data: Duration of account; deleted upon account deletion
- Calendar connection tokens: Duration of the active connection; revoked and deleted upon disconnection or account deletion

All retention periods are subject to (a) any overriding legal obligation to retain data, and (b) the candidate's right to request earlier deletion. SVAYZ operates automated deletion

processes for interview recordings and GDPR erasure requests, and is extending automated deletion to all remaining data categories.

Annex 2 -- Technical and Organisational Security Measures

SVAYZ implements the following measures in accordance with Article 32 of the UK/EU GDPR:

Measure	Description
Encryption in transit	All data transmitted between users, the Platform, and Sub-processors is encrypted using TLS 1.2 or higher.
Encryption at rest	All Candidate Data stored in Neon PostgreSQL and other infrastructure is encrypted at rest using AES-256 encryption. Sensitive application data (such as OAuth tokens) is additionally encrypted using AES-256-GCM with authenticated encryption.
Authentication	User authentication is managed by Clerk with support for multi-factor authentication (MFA). Platform access requires secure credentials.
Access control	Role-based access control (RBAC) limits access to Candidate Data to authorised personnel. Server-side authorisation checks are enforced in all API routes and server actions. Administrative access is restricted and logged.
Network security	HTTPS enforced across all endpoints. HTTP Strict Transport Security (HSTS), Content Security Policy (CSP) headers, and Permissions-Policy headers are configured to mitigate common web attack vectors.
Video and recording security	AI interview recordings are stored in Vercel Blob Storage with private access controls. Access requires signed URLs with time-limited expiry, and is restricted to authorised participants (the interviewing employer and the candidate).
Rate limiting	IP-based rate limiting is implemented using Upstash Redis to prevent abuse, with tiered limits for public pages, public APIs, and AI search endpoints.
Monitoring and error tracking	Sentry is deployed for real-time error tracking and performance monitoring, with alerting on anomalous activity. Personally identifiable information (PII) is not sent to Sentry.
Data minimisation	The Platform collects only the data necessary for the specified processing purposes. Selective field loading and public field whitelists ensure that AI features and public-facing views process only relevant data fields.

Automated data deletion	A 12-month retention cron job automatically identifies and deletes expired interview recordings, transcripts, and assessment data. GDPR erasure requests are processed within 30 days, including deletion of derived scores, AI-generated assessments, and vector embeddings.
Access logging and audit trail	Access to Candidate Data is logged. Consent changes, GDPR operations, and administrative actions are recorded with timestamps for audit purposes.
Password management	All critical company infrastructure credentials are stored in Bitwarden (Team plan) with emergency access protocols.
Sub-processor security	All Sub-processors are contractually required to maintain security measures at least equivalent to those described in this Annex. Sub-processors are selected based on their security certifications and practices.
Backup and recovery	Regular automated backups of Candidate Data are maintained. Backup data is encrypted and subject to the same access controls as production data.
Incident response	SVAYZ maintains incident detection via real-time error monitoring (Sentry) and is developing a formal incident response procedure covering breach detection, escalation, and the 48-hour notification commitment in Section 3.6.
Employee training	All SVAYZ personnel with access to Candidate Data receive data protection awareness training.
Vulnerability management	Regular security assessments and vulnerability scanning of the Platform infrastructure.

Annex 3 -- Approved Sub-processors

The following Sub-processors are approved as at the date of this DPA:

Sub-processor	Purpose	Location	International Transfer	Safeguard
Neon Inc.	Database hosting and storage (PostgreSQL)	EU (Frankfurt region)	None (EU data residency)	EU SCCs; Neon DPA
Google LLC (Gemini API)	AI model inference (ranking, scoring, interviews, content generation)	EU / US	US (API processing)	EU SCCs; Google Cloud DPA; EU AI Act transparency

Clerk Inc.	User authentication and identity management	US	US	EU SCCs; Clerk DPA
Stripe Inc.	Payment processing	EU / US	US (for processing)	EU SCCs; Stripe DPA; PCI DSS compliance
Vercel Inc.	Web application hosting, edge functions, candidate interview recording storage (Blob Storage)	EU / US	US	EU SCCs; Vercel DPA
Qdrant	Vector database for candidate matching and search	EU (Cloud)	None (EU processing)	Qdrant DPA
Upstash Inc.	Redis rate limiting and caching	EU / US	US	EU SCCs; Upstash DPA
Inngest Inc.	Background job processing (application screening, notifications)	US	US	EU SCCs; Inngest DPA
Resend Inc.	Transactional email delivery	US	US	EU SCCs; Resend DPA
Sentry (Functional Software Inc.)	Error tracking and performance monitoring	EU (Frankfurt data center)	None (EU processing)	EU SCCs; Sentry DPA
Google LLC (Calendar API)	Calendar integration for interview scheduling (OAuth)	EU / US	US	EU SCCs; Google Cloud DPA
Microsoft Corporation (Graph API)	Outlook calendar integration for interview scheduling (OAuth)	EU / US	US	EU SCCs; Microsoft DPA
Vercel Inc. (Speed Insights)	Web performance analytics (consent-gated)	EU / US	US	EU SCCs; Vercel DPA