Data Processing Agreement

Socratease, Inc · Version 1.0 · July 29, 2026

This Data Processing Agreement ("DPA") forms part of the Recruiter Terms of Service (the "Agreement") between **Socratease, Inc**, a Delaware corporation at 16192 Coastal Highway, Lewes, Delaware 19958, United States ("Equip", "we", "us"), and the customer that accepted the Agreement ("Customer", "you"). It applies automatically, without signature by Customer, from the date Customer first uses the Platform.

1. Definitions

Terms not defined here have the meaning given in the Agreement or in Data Protection Law.

- **Data Protection Law** means all laws on the processing of Personal Data that apply to the processing under this DPA, including the EU General Data Protection Regulation 2016/679 ("GDPR"), the GDPR as retained in UK law ("UK GDPR") and the UK Data Protection Act 2018, the Swiss Federal Act on Data Protection ("FADP"), and the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA").
- **Customer Personal Data** means Personal Data that Equip processes on behalf of Customer in providing the Platform, chiefly candidate data: applications, resumes, assessment attempts, interview recordings and transcripts, scorecards and proctoring evidence.
- **Personal Data**, **Controller**, **Processor**, **Data Subject**, **processing** and **Supervisory Authority** have the meanings given in the GDPR; under the CCPA, Personal Data includes "personal information".
- **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.
- **Sub-processor** means a third party that Equip engages to process Customer Personal Data.
- **SCCs** means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914.

2. Scope and roles

2.1 Customer is the Controller of Customer Personal Data and Equip is its Processor. Where Customer is itself a Processor for its own client, Equip is Customer's Sub-processor and Customer warrants that its instructions are authorised by that client.

2.2 Equip is a Controller, not a Processor, for its own account, billing, security and website analytics data, as described in the Equip Privacy Policy. This DPA does not cover that data.

2.3 The subject matter, duration, nature and purpose of the processing, and the types of Personal Data and categories of Data Subjects, are set out in Annex I.

3. Customer instructions

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

3.2 Equip will tell Customer promptly if, in its opinion, an instruction infringes Data Protection Law, and may suspend that processing until the instruction is confirmed or changed.

3.3 Equip never uses Customer Personal Data to train AI models, for marketing or advertising, or for any purpose other than providing, securing and supporting the Platform for Customer.

3.4 Customer is responsible for having a lawful basis for the processing, for giving Data Subjects the notices the law requires, and for obtaining any consent it relies on, including for AI-assisted evaluation and proctoring features it chooses to use.

4. Confidentiality and personnel

Equip ensures that every person it authorises to process Customer Personal Data is bound by confidentiality and has access only as their role requires.

5. Security

5.1 Equip implements the technical and organisational measures in Annex II, which are designed to give a level of security appropriate to the risk. Equip holds SOC 2 Type 2 and ISO 27001 certifications covering the Platform.

5.2 Equip may update those measures, provided the overall level of protection is not reduced.

6. Sub-processors

6.1 Customer gives general authorisation for Equip to engage Sub-processors. The current list is the Third-Party Service Providers section of the Equip Privacy Policy at https://equip.co/privacy-policy/#third-party-providers, which forms part of this DPA.

6.2 Equip will update that list at least fourteen (14) days before a new Sub-processor starts processing Customer Personal Data. Customer is responsible for checking the list for changes.

6.3 Customer may object to a new Sub-processor on reasonable grounds relating to data protection by writing to Equip within that fourteen-day period. The parties will discuss the objection in good faith. If it cannot be resolved, Customer's sole remedy is to terminate the affected part of the Platform.

6.4 Equip imposes on each Sub-processor, by written contract, data protection obligations no less protective than those in this DPA, and remains liable to Customer for each Sub-processor's performance of those obligations.

7. Data Subject requests

7.1 Customer can access, correct, export and delete candidate data itself through the Platform. These self-service tools are the technical and organisational measures by which Equip helps Customer

respond to requests from Data Subjects to exercise their rights. Any further help Customer asks for is at Customer's cost.

7.2 If Equip receives a request directly from a Data Subject about Customer Personal Data, it will refer the Data Subject to Customer and will not respond to the request itself unless Customer instructs it to or the law requires it.

8. Personal Data Breach

8.1 Equip will notify Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach.

8.2 The notice will describe, as far as then known, the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed. Equip will supply further information as it becomes available and take reasonable steps to contain and remedy the breach.

8.3 Notifying a breach is not an admission of fault or liability.

9. Impact assessments and consultation

Equip will give Customer reasonable help, at Customer's cost and using information available to Equip, with any data protection impact assessment and prior consultation with a Supervisory Authority that Data Protection Law requires of Customer in relation to the Platform.

10. Deletion and return

10.1 During the term, Customer may delete Customer Personal Data at any time through the Platform, and Equip retains it according to the retention schedule in the Equip Privacy Policy.

10.2 Customer may export its Customer Personal Data at any time before the Agreement ends. Equip will delete it within ninety (90) days of the end of the Agreement, unless the law requires Equip to keep it. Copies in backups are deleted as the backups expire on their normal cycle and remain protected under this DPA until then.

11. Audits

11.1 Equip will make available to Customer the information reasonably necessary to demonstrate compliance with this DPA. Equip meets this obligation, and any audit request, first by providing its current SOC 2 Type 2 report and ISO 27001 certificate, under confidentiality.

11.2 Customer, or an independent auditor bound by confidentiality and not a competitor of Equip, may carry out an on-site or remote audit only where a Supervisory Authority requires it. Such an audit may take place no more than once in any twelve (12) month period, on at least thirty (30) days' written notice, during business hours, without disrupting Equip's operations, at Customer's cost, and with Customer reimbursing Equip's reasonable costs of supporting it.

11.3 Nothing in this section requires Equip to disclose other customers' data or information protected by law or confidentiality obligations to third parties.

12. International transfers

12.1 Equip stores and processes Customer Personal Data on infrastructure in the United States. Customer authorises that transfer and onward transfers to Sub-processors as permitted by this section.

12.2 **EEA.** For Customer Personal Data subject to the GDPR transferred to Equip in a country without an adequacy decision, the SCCs are incorporated into this DPA as follows: Module Two (controller to processor) applies where Customer is a Controller and Module Three (processor to processor) where Customer is a Processor; the optional docking clause in Clause 7 applies; under Clause 9(a), Option 2 (general written authorisation) applies, with the notice period in section 6.2; the optional language in Clause 11 does not apply; under Clause 13, the supervisory authority is the one competent for Customer, or where Customer is not established in the EEA, the authority of the Member State in which Customer's Article 27 representative is established, failing which Ireland; under Clauses 17 and 18, the law and courts of Ireland apply; Annexes I and II of the SCCs are completed by Annexes I and II of this DPA, and Annex III by section 6.1.

12.3 **United Kingdom.** For transfers subject to the UK GDPR, the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner (version B1.0) is incorporated. Table 1 is completed with the parties' details in this DPA, Tables 2 and 3 by section 12.2 and the Annexes, and in Table 4 either party may end the Addendum as set out in its Section 19.

12.4 **Switzerland.** For transfers subject to the FADP, the SCCs apply as in section 12.2, with these changes: the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority; references to the GDPR are read as references to the FADP; and "Member State" is read so as not to exclude Data Subjects in Switzerland from suing for their rights in their place of habitual residence.

12.5 If the SCCs and this DPA or the Agreement conflict, the SCCs govern.

12.6 Equip's EU representative under Article 27 GDPR is Rickert Rechtsanwaltsgesellschaft mbH, Colmantstraße 15, 53115 Bonn, Germany.

13. CCPA

To the extent Customer Personal Data is personal information under the CCPA, Equip is Customer's service provider and will not: (a) sell or share it; (b) retain, use or disclose it for any purpose other than the business purposes set out in the Agreement, including for a commercial purpose other than providing the Platform; (c) retain, use or disclose it outside the direct business relationship with Customer; or (d) combine it with personal information Equip receives from others, except as the CCPA permits. Equip will comply with the CCPA's obligations that apply to it, give the same level of privacy protection the CCPA requires, notify Customer if it can no longer meet these obligations, and allow Customer to take reasonable steps to stop and remediate unauthorised use. Equip certifies that it understands and will comply with these restrictions.

14. Liability

Each party's liability arising out of or relating to this DPA, including the SCCs to the extent the law allows, is subject to the Limitation of Liability section of the Agreement, except where Data

Protection Law does not permit that liability to be limited.

15. Term, precedence and changes

15.1 This DPA lasts as long as Equip processes Customer Personal Data under the Agreement, and its obligations survive until that data is deleted under section 10.

15.2 If this DPA and the Agreement conflict on the processing of Customer Personal Data, this DPA governs, subject to section 12.5. A data processing agreement that Customer and Equip have signed separately governs instead of this standard DPA.

15.3 Equip may update this DPA by publishing a new version at https://equip.co/dpa/, to reflect changes in law, Sub-processors or the Platform. An update will not materially reduce the protection given to Customer Personal Data. Versions already issued remain available.

16. Governing law

Except where the SCCs require otherwise, this DPA is governed by the law of the State of Delaware, and disputes are resolved as set out in the Agreement.

Signed for and on behalf of **Socratease, Inc**



Jayanth Neelakanta
Chief Executive Officer
July 29, 2026

Customer accepts this DPA by accepting the Agreement and does not need to sign it.

Annex I — Description of the processing

Item	Details
Data exporter	Customer, as Controller (or Processor for its own client); contact details as given in its Equip account
Data importer	Socratease, Inc, as Processor; privacy contact hello@equip.co
Categories of Data Subjects	Job applicants and candidates; employees and other people Customer assesses or interviews; Customer's users who review them
Categories of Personal Data	Name, email, phone, location; resume and application answers; assessment responses and scores; AI interview recordings, transcripts and evaluations; scorecards and notes; proctoring evidence (photos, screenshots, audio, video, session recordings) and Trust Score events; IP address and browser data

Item	Details
Special categories	None intended. Customer should not request them; any that candidates submit are processed only as part of their application
Frequency of transfer	Continuous, while Customer uses the Platform
Nature and purpose	Hosting, parsing, scoring, evaluating, proctoring, interviewing and presenting candidate data so Customer can hire and assess people; support and security of the Platform
Duration and retention	For the term of the Agreement plus section 10. Proctoring evidence is deleted automatically after at most 3 months; other candidate data is kept until Customer deletes it or its account
Sub-processors	As listed under section 6.1, for the same nature, purpose and duration
Competent supervisory authority	As set out in section 12.2

Annex II — Technical and organisational measures

- **Certification:** SOC 2 Type 2, audited annually, and an ISO 27001 certified information security management system.
- **Encryption:** TLS for all data in transit; encryption of data at rest.
- **Hosting:** Amazon Web Services in the United States, behind firewalls.
- **Access control:** role-based access for staff.
- **Testing:** regular security scans and penetration tests.
- **Retention and deletion:** proctoring evidence deleted automatically after at most 3 months; deletion tools for Customer, as described in section 10.
- **Incident response:** notification of Personal Data Breaches within 72 hours, as described in section 8.