Data Processing Agreement

Version 1.0 · Enterprise template · Not binding until executed by both parties.
Published July 07, 2026 · StabilityLogic LLC.

This Data Processing Agreement (the 'DPA') supplements the master services or pilot agreement (the 'Agreement') entered into between StabilityLogic LLC ('StabilityLogic') and the customer identified in the Agreement or on the signature page below (the 'Customer'). It governs the processing of personal data by StabilityLogic on behalf of Customer in connection with the Household Stability Index™ platform and related services. Nothing in this DPA constitutes legal advice; Customer is expected to have counsel review this document prior to execution.

1. Controller / Processor definitions

For the purposes of this DPA: (a) 'Controller' means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data; (b) 'Processor' means a natural or legal person which processes personal data on behalf of the Controller; (c) 'Data Subject' means an identified or identifiable natural person; (d) 'Personal Data' means any information relating to a Data Subject; (e) 'Applicant Data' means Personal Data provided by Customer or a Data Subject to StabilityLogic for the purpose of producing a Household Stability Index™ recommendation; (f) 'Sub-processor' means any third party engaged by StabilityLogic to process Applicant Data on its behalf, as listed in the register published at stabilitylogic.com/subprocessors. Customer acts as Controller. StabilityLogic acts as Processor and processes Applicant Data solely on Customer's documented instructions, including as set out in the Agreement and this DPA.

2. GDPR provisions

Where the EU General Data Protection Regulation (Regulation (EU) 2016/679) or the UK GDPR applies to the processing of Applicant Data:

- StabilityLogic will process Applicant Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country, unless required to do so by Union or Member State law to which StabilityLogic is subject; in such a case, StabilityLogic will inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
- StabilityLogic will ensure that persons authorized to process Applicant Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- StabilityLogic will implement the technical and organizational measures described in Section 5 (Security measures) and reflected in the current Enterprise Security Overview.
- StabilityLogic will assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to StabilityLogic.
- StabilityLogic will make available to Customer all information necessary to demonstrate compliance with Article 28 GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, subject to reasonable notice and confidentiality obligations.
- StabilityLogic will delete or return all Applicant Data to Customer at the end of the provision of services relating to processing, per Section 6 (Data retention).

3. CCPA provisions

Where the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, 'CCPA'), applies to the processing of Applicant Data:

- StabilityLogic is a 'Service Provider' as defined in the CCPA. StabilityLogic will not (i) sell or share Applicant Data; (ii) retain, use, or disclose Applicant Data for any purpose other than the specific purpose of performing the services specified in the Agreement, including retaining, using, or disclosing Applicant Data for a commercial purpose other than providing the services; (iii) retain, use, or disclose Applicant Data outside of the direct business relationship between StabilityLogic and Customer; or (iv) combine Applicant Data received from Customer with personal information received from any other source, except as expressly permitted by the CCPA.
- StabilityLogic will comply with applicable obligations under the CCPA and provide the same level of privacy protection to Applicant Data as is required by the CCPA of a Business.
- StabilityLogic will notify Customer if it makes a determination that it can no longer meet its obligations under the CCPA, and Customer may take reasonable and appropriate steps to stop and remediate the unauthorized use of Applicant Data.
- Consumer-rights requests (access, deletion, correction, opt-out) received by StabilityLogic will be forwarded to Customer without undue delay, and StabilityLogic will provide reasonable assistance to Customer in responding.

4. Confidentiality

StabilityLogic personnel with access to Applicant Data are bound by written confidentiality obligations and receive role-appropriate data-handling training. Access to production Applicant Data is restricted to authorized personnel on a least-privilege basis, is logged, and is reviewed on a recurring cadence. StabilityLogic will keep Applicant Data confidential and will disclose it only to Sub-processors bound by written confidentiality obligations consistent with this DPA, or as otherwise required by applicable law (in which case StabilityLogic will, where legally permitted, notify Customer prior to disclosure).

5. Security measures

StabilityLogic maintains a written information-security program aligned with recognized industry frameworks and appropriate to the risks of processing Applicant Data. Current controls include:

- Encryption of Applicant Data in transit (TLS 1.2 or higher) and at rest.
- Multi-tenant logical isolation with per-organization identifiers on every record.
- Role-based access control, least-privilege personnel access, and MFA on administrative interfaces.
- Structured audit logging of scoring decisions, overrides, notes, tag changes, and pipeline transitions.
- Secrets and API keys stored outside application code and injected at runtime.
- Backup and recovery procedures with tested restore, and reproducible deployments from version-controlled infrastructure definitions.
- Documented incident-response runbook covering detection, triage, containment, notification, and post-incident review.

A more detailed description of technical and organizational measures is contained in the current StabilityLogic Enterprise Security Overview, incorporated into this DPA by reference and available at stabilitylogic.com/trust.

6. Data retention

Applicant Data is retained only for the period reasonably necessary for the purposes of the Agreement, plus any period required to defend a rental decision under applicable federal, state, and local law (including record-retention obligations under the Fair Credit Reporting Act, 15 U.S.C. § 1681, and applicable state analogs). Upon termination of the Agreement, StabilityLogic will, at Customer's written election, return or hard-delete Applicant Data within a mutually agreed timeframe, subject to ongoing legal-hold obligations. Audit-log entries associated with a rental decision may be retained beyond the general retention period to the minimum extent necessary to demonstrate the reasoning and reproducibility of that decision.

7. Subprocessors

Customer provides general written authorization for StabilityLogic to engage the Sub-processors listed in the register published at stabilitylogic.com/subprocessors. StabilityLogic will impose on each Sub-processor, by written contract, data-protection obligations no less protective than those set out in this DPA. StabilityLogic will notify Customer of any intended addition or replacement of a Sub-processor at least thirty (30) days in advance. Customer may object on reasonable grounds within that notice window; if the objection is not resolved, either party may terminate the affected portion of the Agreement without penalty.

8. International transfers

Applicant Data is processed in the United States. To the extent Applicant Data relating to Data Subjects located in the European Economic Area, the United Kingdom, or Switzerland is transferred outside their jurisdiction of origin, the parties will rely on an appropriate transfer mechanism recognized under applicable law, including (as applicable) the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), the UK International Data Transfer Addendum, or an equivalent successor mechanism. Additional safeguards will be adopted where required by an ongoing transfer impact assessment.

9. Customer obligations

Customer is responsible for the lawfulness of the collection, disclosure, and transfer to StabilityLogic of Applicant Data, and for ensuring that all necessary notices and consents are in place for the processing contemplated by this DPA. Without limiting the foregoing, Customer will:

- Provide only Applicant Data that Customer is lawfully entitled to disclose to StabilityLogic.
- Provide accurate, complete instructions in the Agreement and this DPA regarding the scope, purpose, and duration of processing.
- Respond, as Controller, to Data Subject requests received by Customer, using StabilityLogic's assistance where reasonably requested.
- Retain sole responsibility for the final rental decision and for compliance with the Fair Housing Act, the Fair Credit Reporting Act, and applicable state or local screening and fair-housing statutes.
- Maintain the security of its own account credentials and promptly notify StabilityLogic of any suspected unauthorized use of its account.

10. Personal-data breach notification

StabilityLogic will notify Customer without undue delay after becoming aware of a Personal-Data breach affecting Customer's Applicant Data, and in any event within seventy-two (72) hours of confirmation, providing

the information reasonably necessary for Customer to meet its notification obligations under applicable law. StabilityLogic will deliver a written post-incident summary describing the nature of the incident, the categories and approximate number of Data Subjects affected, and the corrective actions taken or proposed.

11. Termination

This DPA will remain in effect for the duration of the Agreement and, with respect to surviving obligations (including confidentiality, breach notification for pre-termination incidents, and data-return/deletion), for the period necessary to complete those obligations. Termination of the Agreement automatically terminates the corresponding processing under this DPA. Either party may terminate this DPA for material breach that remains uncured for thirty (30) days after written notice. Sections 4 (Confidentiality), 6 (Data retention), 10 (Breach notification), and 12 (Governing law) survive termination.

12. Governing law and order of precedence

This DPA is governed by the law of the State of California, without regard to conflict-of-laws principles, except where a mandatory rule of applicable data-protection law requires otherwise. In the event of any conflict between this DPA and the Agreement with respect to the processing of Personal Data, this DPA controls. Material changes to this DPA require written agreement by both parties.

Signature Page

This DPA is entered into by the parties identified below and takes effect on the later of the two signature dates. Each signatory represents that they are duly authorized to execute this DPA on behalf of the party they represent.

For the Customer (Controller)	
Legal entity name	
Signature	
Printed name	
Title	
Date	
Email for notices	
Address for notices	

For StabilityLogic LLC (Processor)	
Legal entity name	

Signature	
Printed name	
Title	
Date	
Email for notices	
Address for notices	

Notices to StabilityLogic under this DPA should be sent to: ***aqueelah@stabilitylogic.com***
Security incidents: ***security@stabilitylogic.com*** *· Privacy requests:* ***privacy@stabilitylogic.com***
Mailing address: StabilityLogic LLC, 3411 W Stanton Ave, Fullerton, CA 92833, United States.