**DATA PROCESSING ADDENDUM**

This Data Processing Addendum ("DPA") governs Azava Limited's ("Azava") processing of personal data on behalf of the customer ("Customer") in connection with Azava's provision of the Services. It forms part of, and is subject to, the Agreement. Where the parties have entered into a separately executed written agreement governing the Services, that agreement prevails over this DPA to the extent of any conflict.

## 1. Definitions and Interpretation

1.1 Definitions:

Agreement: the agreement under which Azava provides the Services to the Customer — for self-serve customers, Azava's Terms of Use; or any separately executed written agreement between the parties.

**Authorised Persons**: the persons or categories of persons that the Customer authorises to give Azava written personal data processing instructions as identified in ANNEX A and from whom Azava agrees to accept such instructions.

1. **Business Purposes**: the services to be provided by Azava to the Customer as described in the Agreement and any other purpose specifically identified in ANNEX A.
2. **Commissioner:** the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).
3. **Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing**: have the meanings given in the Data Protection Legislation.
4. **Controller:** has the meaning given in section 6, DPA 2018.
5. **Data Protection Legislation:**
   5.a) To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of Personal Data.
   5.b) To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Customer or Provider is subject, which relates to the protection of Personal Data.
6. **Data Subject**: the identified or identifiable living individual to whom the Personal Data relates.
7. **EU GDPR:** the General Data Protection Regulation ((EU) 2016/679).
8. **EEA:** the European Economic Area.
9. **Personal Data**: means any information relating to an identified or identifiable living individual that is processed by Azava on behalf of the Customer as a result of, or in connection with, the provision of the services under the Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
10. **Processing, processes, processed, process**: any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making

available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third parties.

11. **Personal Data Breach**: a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.
12. **Processor**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Customer.
13. **Records**: has the meaning in Clause 12.
14. **Standard Contractual Clauses (SCCs)**: the ICO's International Data Transfer Agreement for the transfer of personal data from the UK and/or the ICO's International Data Transfer Addendum to EU Commission Standard Contractual Clauses and/or the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to Commission Implementing Decision (EU) 2021/914 and/or the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (Customer-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU or such alternative clauses as may be approved by the European Commission or by the UK from time to time.
15. **Term: the term of the Agreement.**
16. **UK GDPR:** has the meaning given in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

2. This DPA is subject to the terms of the Agreement and is incorporated into the Agreement. Interpretations and defined terms set forth in the Agreement apply to the interpretation of this DPA.

1. The Annexes form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes.
2. A reference to writing or written excludes fax but not email.
3. In the case of conflict or ambiguity between:
    (a) any provision contained in the body of this DPA and any provision contained in the Annexes (excluding any executed SCC), the provision in the body of this DPA will prevail;
    (b) the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Annexes, the provision contained in the Annexes will prevail;
    (c) any of the provisions of this DPA and the provisions of the Agreement, the provisions of the Agreement will prevail; and
    (d) any of the provisions of this DPA (or any other provision contained in the Annexes or any of the documents referred to in (b) and (c) above) and any executed SCC, the provisions of the executed SCC will prevail.

**2. Personal data types and processing purposes**

1. The Customer and Azava agree and acknowledge that for the purpose of the Data Protection Legislation:
    (a) the Customer is the Controller and Azava is the Processor.
    (b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including but not limited to providing any required notices and obtaining any required consents, and for the written processing instructions it gives to Azava.

2. ANNEX A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which Azava may process the Personal Data to fulfil the Business Purposes.
3. Azava acts as an independent Controller with respect to personal data processed for billing, account management, internal analytics, security, and compliance purposes. Such processing is outside the scope of this Data Processing Addendum.

**3. Provider's obligations**

1. Azava will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions. Azava will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. Azava must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.
2. Azava must comply promptly with any Customer written instructions requiring Azava to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
3. Azava will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third parties unless the Customer or this DPA specifically authorises the disclosure, or as required by domestic law, court or regulator (including the Commissioner). If a domestic law, court or regulator (including the Commissioner) requires Azava to process or disclose the Personal Data to a third party, Azava must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.
4. Azava will reasonably assist the Customer, at no additional cost to the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of Azava's processing and the information available to Azava, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation.

**4. Provider's employees**

1. Azava will ensure that all of its employees:
    (a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;
    (b) have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and
    (c) are aware both of Azava's duties and their personal duties and obligations under the Data Protection Legislation and this DPA.

**5. Security**

1. Azava must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in ANNEX B.

**6. Personal Data Breach**

1. Azava without undue delay notify the Customer if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data.
(b) any accidental, unauthorised or unlawful processing of the Personal Data; or
(c) any Personal Data Breach.

2. Where Azava becomes aware of (a), (b) and/or (c) above, it shall, without undue delay, also provide the Customer with the following information:
   (a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;
   (b) the likely consequences; and
   (c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.
3. Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter.
4. Azava will not inform any third party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's consent, except when required to do so by domestic law.

**7. Transfers of personal data**

1. The Customer authorises Azava to transfer and process the Personal Data outside the UK and the EEA to the sub-processors listed in ANNEX A. Where such a transfer is to a country that is not the subject of UK or EU adequacy regulations, Azava ensures that the transfer is made subject to appropriate safeguards under Article 46 of the UK GDPR and/or EU GDPR — principally the UK International Data Transfer Agreement / Addendum and/or the European Commission's Standard Contractual Clauses, as incorporated into the relevant sub-processor's data processing terms. Azava will make details of the applicable safeguards available to the Customer on request.
2. Azava ensures that any such transfer satisfies at least one of the following conditions:
   (a) Azava is processing the Personal Data in a territory which is subject to adequacy regulations under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. Azava must identify in ANNEX A the territory that is subject to such adequacy regulations; or
   (b) Azava participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that Azava (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR and EU GDPR.
   (c) the transfer otherwise complies with the Data Protection Legislation for the reasons set out in ANNEX A.
3. If any Personal Data transfer between the Customer and Azava requires execution of SCCs in order to comply with the Data Protection Legislation (where the Customer is the entity exporting Personal Data to Azava outside the EEA), the parties will complete all relevant details in, and execute, the most recent version of SCCs and take all other actions required to legitimise the transfer.

**8. Subcontractors**

1. Azava may authorise any third party or subcontractor to process the Personal Data. Those subcontractors are as set out in ANNEX A. Azava must list all approved subcontractors in

Annex A and include any subcontractor's name and location and the contact information for the person responsible for privacy and data protection compliance.

2. Where the subcontractor fails to fulfil its obligations under the written agreement with Azava, Azava remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.
3. The Parties agree that Azava will be deemed to control legally any Personal Data controlled practically by or in the possession of its subcontractors.
4. For the avoidance of doubt, where the Customer chooses to enable any integration with a third party service as determined by them, such third party services will not be Azava's sub-processors, and Azava is not responsible for any processing practices carried out by such third party services.

**9. Complaints, data subject requests and third-party rights**

1. Azava must, at no additional cost to the Customer, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:
   (a) the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and
   (b) information or assessment notices served on the Customer by the Commissioner or other relevant regulator under the Data Protection Legislation.
2. Azava must notify the Customer immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.
3. Azava must notify the Customer within 7 days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.
4. Azava will give the Customer its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.
5. Azava must not disclose the Personal Data to any Data Subject or to a third party other than in accordance with the Customer's written instructions, or as required by domestic law.

**10. Term and termination**

1. This DPA will remain in full force and effect so long as:
   (a) the Agreement remains in effect; or
   (b) Azava retains any of the Personal Data related to the Agreement in its possession or control (**Term**).
2. Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect the Personal Data will remain in full force and effect.
3. If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements.

**11. Data return and destruction**

1. At the Customer's request, Azava will give the Customer a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

2. On termination of the Agreement for any reason or expiry of its term, Azava will securely delete or destroy all or any of the Personal Data related to this DPA in its possession or control, except for one copy that it may retain and use as set out in Annex A in relation to data processing activities, only.
3. If any law, regulation, or government or regulatory body requires Azava to retain any documents or materials or Personal Data that Azava would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

**12. Records**

1. Azava will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in clause 5.1 (**Records**).

**13. Audit**

1. Azava will permit the Customer to audit Azava's compliance with its Agreement obligations, on at least 30 days' notice, no more than once every 12 months.
2. The notice requirements in clause 13.1 will not apply if the Customer believes and can evidence that that a Personal Data Breach occurred or is occurring, or Azava is in breach of any of its obligations under this DPA or any Data Protection Legislation, which must be evidenced.
3. If a Personal Data Breach occurs or is occurring, or Azava becomes aware of a breach of any of its obligations under this DPA or any Data Protection Legislation, Azava will:
    (a) promptly conduct its own audit to determine the cause;
    (b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;
    (c) provide the Customer with a copy of the written audit report; and
    (d) remedy any deficiencies identified by the audit within a reasonable timeframe..

**14. Warranties**

1. Azava warrants and represents that:
    (a) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;
    (b) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:
        (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;
        (ii) the nature of the Personal Data protected; and
        (iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in clause 5.1.

2. The Customer warrants and represents that Azava's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

**15. Notice**

1. Any notice given to a party under or in connection with this DPA shall be in writing and shall be:
   (a) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or
   (b) sent by email to the following addresses (or an address substituted in writing by the party to be served):
      (i) For the Customer: [notice email provided at sign-up]
      (ii) For Azava: henry@azava.com
2. Any notice shall be deemed to have been received:
   (a) if delivered by hand, at the time the notice is left at the proper address; or
   (b) if sent by pre-paid first-class post or other next working day delivery service, at 9:00am on the second Business Day after posting; or
   (c) if sent by email, at the time of transmission, or, if this time falls outside Business Hours in the place of receipt, when Business Hours resume.
3. This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

This agreement has been entered into on the date stated at the beginning of it.

| | |
|---|---|
| Signed by Henry Stanford | |
| for and on behalf of AZAVA LIMITED | Director |
| Signed by [Customer signatory] | |
| for and on behalf of [Customer] | Director |

**A. Personal Data processing purposes and details**

**SECTION 1 - *CUSTOMER IS THE CONTROLLER AND AZAVA IS PROCESSOR;***

a) **Communication Ingestion (Email, WhatsApp, Calendars)**

| Field | Details |
|---|---|

| | |
|---|---|
| Purpose | Receive and ingest the Customer's communications and inputs for the Customer's chosen workflow (e.g. a VC firm's investment workflow, or any other use case the Customer configures) |
| Customer | The Customer (any organisation or individual using Azava — e.g. a VC firm) |
| Data Subjects | Any individuals whose personal data the Customer chooses to submit, as determined by the Customer — for example (VC context) founders, portfolio companies, employees of target companies, investors and other correspondents; more generally, the Customer's contacts and any people referenced in the records and communications it processes |
| Data | Email bodies, attachments, WhatsApp messages, Slack messages, metadata (headers, timestamps, sender/recipient), phone numbers, meeting notes from other platforms |
| Retention | Until deletion by customer; hard-delete supported; system logs retained 14 days |
| Processors/Sub-processors | Render, Postgres, Sentry |
| Transfers | Sentry to US (SCCs) |
| High-Risk? | Yes (content ingestion, unstructured, possible sensitive data) |
| Mitigations | Encryption in transit & at rest, access controls, role-based access, zero trust, strict data minimisation |

a)

b) **Data Parsing and Structuring**

| Field | Details |
|---|---|
| Purpose | Automatically extract entities, people, attributes, tags and structured records from the Customer's inputs (e.g. structured deal notes in a VC context) |
| Data | Derived and inferred insights based on communications |
| Retention | As long as the customer account exists or until deleted |

| | |
|---|---|
| Processors/Sub-processors | OpenAI, Google Document AI, Anthropic |
| High-Risk? | Medium |
| Mitigations | Deterministic parsing where possible, auditability, ability to delete derived output on request |

b)

c) **CRM / Slack / Airtable Integrations**

| Field | Details |
|---|---|
| Purpose | Send structured and raw data to customer systems as instructed |
| Data | Names, emails, phone numbers and any other personal data in the Customer's inputs, plus summaries and metadata derived from them (e.g. deal summaries in a VC context) |
| Retention | Not stored beyond transmission (except logs) |
| Recipients | Customer-specified systems |
| High-Risk? | Low |
| Mitigations | Signed webhook requests (planned), integration scoping, customer control over destinations |

c)

d) **Audit Logging and Provenance**

| Field | Details |
|---|---|
| Purpose | Record processing steps for traceability |

| | |
|---|---|
| Data | Row-level logs of processing operations, IDs, timestamps, user IDs, message IDs |
| Retention | See Retention section |
| Location | Render.com (Frankfurt) |
| High-Risk? | Medium |
| Mitigations | Log minimisation, automatic rotation, restricted access, optional customer-specific retention controls |

d)

e) **Storage and Retrieval on Customer's behalf**

| **Field** | **Details** |
|---|---|
| Purpose | Store data for customer workflows and history |
| Data | Entire communication dataset + structured outputs |
| Retention | See Retention section |
| Location | Render.com for Postgres DB, AWS S3 for raw files, both EU Frankfurt |
| High-Risk? | High |
| Mitigations | Backups encrypted, access controls, data residency in EU, deletion SLA (e.g., 7–30 days) |

e)

f) **Issue debugging and reliability (Sentry, Render Logs)**

| **Field** | **Details** |
|---|---|
| Purpose | Capture errors and events to resolve customer issues |
| Data | Stack traces, user identifiers, excerpts of content |

| | |
|---|---|
| Retention | Sentry: 90 days; Render: 14 days |
| Location | Sentry (Iowa), Render logs |
| High-Risk? | Medium |
| Mitigations | |

f)

g) **External Data Augmentation (Bright Data, Google Search API)**

| **Field** | **Details** |
|---|---|
| Purpose | Augment and verify entities (companies, people, websites) with publicly available data to improve search, deduplication, and context for customer workflows |
| Customer | The Customer (any organisation or individual using Azava — e.g. a VC firm) |
| Data Subjects | Individuals referenced in publicly available data the workflow looks up — e.g. founders, executives and public company personnel (VC context), or any publicly listed contacts relevant to the Customer's use case |
| Data | Public web page content, search result snippets and URLs, metadata (titles, descriptions), derived attributes (company domains, roles, links). No credential-based or paywalled access. Respect robots.txt and site terms. |
| Processors/Sub-processors | Bright Data (proxy network and web retrieval), Google Programmable Search / Custom Search JSON API |
| Retention | see Retention section |
| Transfers | Possible transfers to third countries by Google and Bright Data; vendor SCCs/DPF as applicable |
| High-Risk? | Medium (web data may incidentally include personal data) |
| Mitigations | Public-source only, rate limiting, content minimisation |

g)

**B. Security measures**

- **Encryption in transit and at rest** using TLS 1.2+ and AES-256.
- **Access controls**: least privilege, role-based, admin access.
- **Network security**: no public DB access.
- **Data retention policies**: See retention section
- **Incident response**: incidents documented and mitigated within 72-hours.
- **Backup controls**: encrypted, access restricted, deletion within 30 days of customer request.
- **Data subject rights support**: ability to locate, export, delete all data tied to an identity.