DATA PROCESSING AGREEMENT

Last Updated November 26, 2025

This Data Processing Agreement ("**DPA**") is governed by and hereby attached to the agreement signed between the parties ("**Agreement**") executed by and between Stage5.AI Ltd. ("**Stage5"**), and you, a customer, user or individual ("**Customer**"). Stage5 and Customer shall each be referred to as "**party**" and collectively as "**parties**".

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

WHEREAS, Stage5 offers its customers AI-driven agent coding services ("**Services**") by developing and delivering a customized software agent designed to address the specific problem or requirement as described and requested by the customer, and in accordance with the customer's specifications ("**Stage5 Technology**"), all as agreed by the parties in the applicable order form or other ordering documents that are incorporated in the Agreement (collectively the "**Service(s)**");

WHEREAS, the Services may require Stage5 to Process Personal Data (as such terms are defined below) on Customer's behalf, and subject to the terms and conditions of this DPA; and

WHEREAS, the parties desire to supplement this DPA to achieve compliance with data protection laws and agree on the following:

1. DEFINITIONS

1.1. "**Adequate Country**" is a country that received an adequacy decision from the European Commission or other applicable data protection authority.

1.2. The terms "**Business**", "**Business Purpose**", **"Consumer",** "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" (and "**Process**"), "**Processor**", "**Holder**", **"Sensitive Data", "Service Provider", "Sale" (or "Sell") and "Share",** "**Special Categories of Personal Data**" and "**Supervisory Authority**", shall all have the same meanings as ascribed to them under applicable Data Protection Laws. Further, under this DPA "**Data Subject**" shall also mean and refer to a "**Consumer**", and "**Personal Data**" shall also mean and refer to "**Personal Information**", and "**Special Categories of Data**" or "**Highly Sensitive Data**" shall also mean and refer to "**Sensitive Data**".

1.3. "**Customer Data**" means any Personal Data processed by Stage5 in the course of its Services provision to Customer, all as detailed in **Annex I** attached herein. Customer Data may be included in both the Input submitted and the Output generated.

1.4. "**Data Protection Law**" means any and all applicable privacy and data protection laws and regulations (including, where applicable, EU Data Protection Law, UK Data Protection Laws, Swiss Data Protection Laws, Israeli Data Protection Laws and the US Data Protection Laws, as may be amended or superseded from time to time.

1.5. "**EEA**" means the European Economic Area.

1.6. "**European Data Protection Laws**" means collectively, the laws and regulations of the European Union, the EEA, their member states, and the United Kingdom,

applicable to the Processing of Personal Data, including (where applicable): (i) EU General Data Protection Regulation (Regulation 2016/679) ("**EU GDPR**"); Regulation 2018/1725; and the e-Privacy Directive (Directive 2002/58/EC), as amended (**e-Privacy Law**); (ii) "**UK Data Protection Laws**" - the Data Protection Act 2018 (DPA 2018), as amended, and EU GDPR as incorporated into UK law as amended ("**UK GDPR**" and collectively with the EU GDPR shall be referred to herein as the "**GDPR**"); (iii) "**Swiss Data Protection Laws**" or "**FADP**" - the Swiss Federal Act on Data Protection of September 25, 2020 (as amended from time to time), and its implementing ordinances (including the Ordinance on the Federal Act on Data Protection ("**FODP**"); (iv) any national data protection laws made under, pursuant to, replacing or succeeding the EU GDPR or the e-Privacy Law; (v) any amendment or legislation replacing or updating any of the foregoing; and (vi) any judicial or administrative interpretation of any of the above, including any binding judicial or administrative interpretation of any of the above, or approved certification mechanisms issued by any relevant Supervisory Authority.

1.7. "**Input**" means any content, data, material, or instructions – whether in textual, visual, audio, code-based, or other format – that is used by the Customer to generate Output through an artificial intelligence system provided by Stage5.

1.8. "**Instructions**" means the written, documented instructions issued by the Customer to Stage5 directing Stage5 to perform a specific or general action with regard to Customer Data (including, but not limited to, instructions to provide the Services under the Agreement and instructions under this DPA).

1.9. "**Israeli Data Protection Laws**" means, collectedly, the: (i) Israeli Privacy Protection Law, 5741-1981, (as amended under Amendment 13); (ii) the regulations promulgated pursuant thereto, including the Israeli Privacy Protection Regulations (Data Security), 5777-2017 and the Israeli Protection of Privacy (Transfer of Data to Databases Abroad) Regulations, 5761-2001; (iii) any amendments or legislation replacing or updating any of the foregoing, and; (iv) any judicial or administrative interpretation of any of the above, including any binding guidance, guidelines, codes of practice, approved codes of conduct or certification mechanisms approved by the Israeli Privacy Protection Authority.

1.10. "**Output**" means any content, code, text, image, audio, or other form of information generated by an artificial intelligence system provided by Stage5 in response to Input submitted by the Customer.

1.11. "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data. Any Personal Data Breach will comprise a Security Incident.

1.12. "**Standard Contractual Clauses**" or "**SCCs**" means (i) the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by the European Commission Decision 2021/914 of 4 June 2021, which may be found here; (ii) the UK "International Data Transfer Addendum to the European Commission Standard Contractual Clauses" available at: available at: https://ico.org.uk/media2/migrated/4019538/international-data-transfer-agreement.pdf and incorporated herein by reference ("**UK SCC**"); or (iii) the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner ("**Swiss SCC"**).

1.13. "**US Data Protection Laws**" means any U.S. federal and state privacy laws and regulations effective as of the Effective Date of this DPA and applies to Stage5 Processing of Customer Data, and any implementing regulations and amendment thereto.

Any other terms that are not defined herein shall have the meaning provided under the Agreement or applicable Data Protection Laws. A reference to any term or section of the Data Protection Laws means the version as amended. Any references to the GDPR in this DPA shall mean the GDPR or UK GDPR depending on the applicable Law.

2. ROLES AND DETAILS OF PROCESSING

2.1. The parties agree and acknowledge that under the performance of their obligations set forth in the Agreement, and with respect to the Processing of Customer Data, and according to the applicable Data Protection Law, Stage5 is acting as a Data Processor and Customer is acting as a Data Controller.

2.2. Each party shall be individually and separately responsible for complying with the obligations that apply to such party under applicable Data Protection Law. The Customer shall be exclusively responsible to ensure its Instructions are compliant with applicable Data Protection Laws and enable a lawful Processing of Customer Data, including by obtaining any required consent and providing any required disclosures under applicable Data Protection Law.

2.3. Customer warrants that it has all the necessary rights to provide the Personal Data to Stage5 for the Processing to be performed in relation to the Services, and that one or more lawful bases set forth in the applicable Data Protection Laws support the lawfulness of the Processing. To the extent required by the applicable Data Protection Law, Customer is responsible for ensuring that all necessary privacy notices are provided to Data Subjects, and unless another legal basis set forth in the applicable Data Protection Law supports the lawfulness of the Processing, that any necessary Data Subject consents to the Processing are obtained, and for ensuring that a record of such consent is maintained. Should such consent be revoked by a Data Subject, Customer is responsible for communicating the fact of such revocation to Stage5, and Stage5 will act pursuant to Customer's instructions as seems appropriate.

2.4. The subject matter and duration of the Processing carried out by the Processor on behalf of the Controller, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are described in **Annex I** attached hereto.

2.5. If any Sensitive Data or Special Categories of Personal Data or Highly Sensitive Data is processed (as those terms are defined under Data Protection Laws), including, any information that constitutes "consumer health data" under the Connecticut Data Privacy Actor the Washington and Nevada Consumer Health Data Laws or any information that constitutes "protected health information" under the Health Insurance Portability and Accountability Act of 1996, 5 U.S.C. § 553 et seq., together with any amending legislation and any regulations promulgated thereunder, or any Personal Data that is deemed by US regulatory authorities as meriting sensitive treatment under US Data Protection Laws or U.S. state or federal consumer protection laws such as financial information, demographic information, credit

scores, etc., it is Customer's responsibility to inform Stage5 of such processing, and ensure additional contractual obligations are met, if needed and applicable. For avoidance of doubt, Stage5 does not monitor, and review Customer Data processed according to this DPA, and may not be aware of any sensitivity within Customer Data.

3. PROCESSING OF PERSONAL DATA

3.1. Stage5 represents and warrants that it shall Process Customer Data, on behalf of the Customer, solely for the purpose of providing the Services, all in accordance with Customer's written instructions under the Agreement and this DPA. Notwithstanding the above, in the event Stage5 is required under applicable laws, including Data Protection Law or any union or member state regulation, to Process Customer Data other than as instructed by Customer, Stage5 shall make reasonable efforts to inform the Customer of such requirement prior to Processing such Customer Data, unless prohibited under applicable law.

3.2. Stage5 hereby certifies it understands the rules, requirements and definitions under applicable Data Protection Law, and shall not: (i) Sell or Share the Customer Data; (ii) retain, use or disclose the Customer Data for any purpose other than for a Business Purpose specified in the Agreement; (iii) receive or Process any Personal Information as consideration for any Services it provides to the Customer; or (iv) combine the Customer Data with other Personal Data that it receives from, or on behalf of another customer.

3.3. Stage5 shall comply with the requirements set forth under applicable Data Protection Law with regards to processing of de-identified data.

3.4. Stage5 shall inform Customer without undue delay in the event that, according to Stage5's reasonable discretion, any of Customer's Instructions infringes applicable laws, and Stage5 shall have the right to immediately cease and suspend any such Processing activity related to the infringing Instruction.

3.5. Stage5 shall notify the Customer if it determines that it can no longer meet its obligations under this DPA or applicable Data Protection Law.

3.6. Stage5 shall provide reasonable cooperation and assistance to the Customer in ensuring compliance with its obligation to carry out data protection impact assessments and prior consultations with Supervisory Authorities or other competent data privacy authorities to the extent required under applicable Data Protection Law (including data protection impact assessments and consultations with regulatory authorities), provided that Stage5 shall only be required to assist as for information which is reasonably available to Stage5.

3.7. Where applicable, Stage5 shall assist the Customer in ensuring that Customer Data Processed is accurate and up to date, by informing the Customer without delay if it becomes aware of the fact that the Customer Data it is processing is inaccurate or has become outdated.

3.8. Stage5 shall ensure: (i) the reliability of its staff and any other person acting under its supervision who may come into contact with or otherwise have access to and Process Customer Data; and (ii) that persons authorized to Process the Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. DATA SUBJECTS RIGHTS AND LEGAL REQUEST

4.1. It is agreed that where Stage5 receives a request from a Data Subject for exercising a data subject's rights or an applicable authority in respect of Customer Data, where applicable, Stage5 will notify the Customer of such request promptly and direct the Data Subject or the applicable authority to the Customer in order to enable the Customer to respond directly to the Data Subject's or the applicable authority's request, unless otherwise required under applicable laws.

4.2. Parties shall provide each other with commercially reasonable cooperation and assistance in relation to the handling of and responding to Data Subject's or applicable authority's request, to the extent permitted under Data Protection Law. Stage5 shall provide Customer with cooperation and assistance mentioned above provided that the Customer cannot reasonably fulfill such obligations independently with the help of information available in the documentation, the website or any other self-service feature provided by Stage5.

5. SUB-PROCESSING

5.1. The Customer provides general authorization for Stage5 to engage third party data Processors ("**Sub-Processor**") to Process Customer Data. The Customer specifically authorizes Stage5 to engage and appoint such Sub-Processors as listed in **Annex III**, to Process Customer Data, as well as permits each Sub-Processor to appoint a Sub-Processor on its behalf.

5.2. Stage5 may engage an additional or replace an existing Sub-Processors to Process Customer Data, subject to the provision of a fourteen (14) days prior notice of its intention to do so to the Customer (such notice can be provided through an email correspondence) ("**Notice**" and "**Notice Period**" respectively). In case the Customer has not objected to the adding or replacing of a Sub-Processor within Notice Period, such Sub-Processor shall be deemed approved by the Customer. In the event the Customer objects to the adding or replacing of a Sub-Processor, within such Notice Period, Stage5 may, under Stage5' sole discretion, suggest the engagement of a different Sub-Processor for the same course of services, or otherwise enable the Customer to terminate the Agreement where the Services cannot be reasonably provided under such circumstances, without liability to Customer.

5.3. Stage5 shall, where it engages any Sub-Processor, impose, through a legally binding contract between Stage5 and the Sub-Processor, data protection obligations that are no less onerous than, and provide at least the same level of protection as, those set out in this DPA. Stage5 shall ensure that such contract will require the Sub-Processor to provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Data Protection Laws. Sub-processors shall be obligated, contractually, to reasonably cooperate with Stage5, the Customer or an applicable regulatory authority in the event of an investigation or Security Incident.

5.4. Stage5 shall remain responsible to the Customer for the performance of the Sub-Processor's obligations in accordance with this DPA.

6. TECHNICAL AND ORGANIZATIONAL MEASURES

6.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and without prejudice to any other security standards agreed upon by the parties, Stage5 shall protect the security, confidentiality, integrity and availability of Customer Data and protect it against Security Incident.

6.2. Current technical and organizational measures implemented and maintained by Stage5 are further detailed in **Annex II** to this DPA, as updated from time to time (provided that any such amendments will not have a material negative effect on the level of protection provided to Customer Data).

7. SECURITY INCIDENT

7.1. Stage5 will notify the Customer without undue delay, no later than 72 hours, upon becoming aware of any Security Incident involving the Customer Data. Stage5's notification regarding or response to a Security Incident under this Section 7 shall not be construed as an acknowledgment by Stage5 of any fault or liability with respect to the Security Incident.

7.2. Stage5 will: (i) take reasonably necessary steps to remediate, minimize any effects of and investigate any Security Incident and to identify its cause; (ii) upon Customer request, co-operate with the Customer and provide the Customer with such reasonable assistance and information in connection with the containment, investigation, remediation or mitigation of the Security Incident, if applicable, and obligation to notify the affected Data Subjects. Upon Customer's request and taking into account the nature of the Processing and the information available to Stage5, Stage5 will provide a report or written notice detailing the Security Incident, the affected Personal Data and Data Subjects.

8. AUDIT RIGHTS

8.1. Stage5 shall maintain accurate written records of any and all the Processing activities of any Customer Data carried out under this DPA its compliance with its obligations under this DPA, and shall make such records available to the Customer upon Customer's thirty (30) days prior written request, however no more than once per twelve (12) months of engagement ("**Audit Reports**"). Information provided through Customer's questionnaire shall be defined as a sufficient Audit Report. The Audit Report provided shall be considered Stage5's Confidential Information and shall be subject to the corresponding confidentiality obligations under the Agreement or require signed a non-disclosure agreement.

8.2. In the event the Audit Report is reasonably determined as not sufficient for the purpose of demonstrating compliance, Stage5 shall make available, solely upon prior reasonable written notice and no more than once per calendar year, to a reputable auditor nominated by the Customer, information necessary to reasonably demonstrate compliance with this DPA or where required by Applicable Data Protection Law or an applicable authority, and shall allow for audits, including inspections, by such reputable auditor solely in relation to the Processing of the Customer Data ("**Audit**") in accordance with the terms and conditions hereunder. The auditor shall be subject to standard confidentiality obligations (including

towards third parties). Stage5 may object to an auditor appointed by the Customer in the event Stage5 reasonably believes the auditor is not suitably qualified or is a competitor of Stage5. Customer shall bear all expenses related to the Audit and shall (and ensure that each of its auditors shall) over the course of such Audit, ensure that the Audit is conducted during regular business hours, and avoid causing any damage, injury or disruption to Stage5's premises, equipment, personnel and business while its personnel are on those premises in the course of such Audit. Stage5 shall agree to an Audit solely under the following terms: (i) a thirty (30) day prior written notice was provided; and (ii) restrict its findings to only to information relevant to Customer Data or an applicable Security Incident.

8.3. Nothing in this DPA will require Stage5 to either disclose to Customer or its third-party auditor, or to allow Customer or its third-party auditor to access: (i) any data of any other Stage5's customer or Stage5's internal data including without limitation data processed in Stage5's role as a Controller; (ii) Stage5's internal accounting or financial information; (iii) any trade secret of a Stage5 or its affiliates; (iv) any information that, in Stage5's reasonable opinion, could compromise the security of any Stage5's systems or cause any breach of its obligations under applicable law or its security, privacy or confidentiality obligations to any third party; or (v) any information that Customer or its third-party auditor seeks to access for any reason other than the good faith fulfillment of Customer's obligations under the Data Protection Law. No access to any part of Stage5's IT systems or infrastructure (including, without limitation, any hands-on or intrusive testing) will be permitted.

9. CROSS BORDER PERSONAL DATA TRANSFERS

9.1. Customer acknowledges and agrees that for the provisions of the Services, Stage5 may Process, including transfer, Customer Data to various jurisdictions where Stage5, its affiliates or Sub-Processors operate. Stage5 will ensure that transfers are made in compliance with Data Protection Law.

9.2. Where European Data Protection Laws apply:

9.2.1. Stage5 will not transfer Customer Data originating from the EEA, the UK or Switzerland, to any country or recipient not recognized as providing an adequate level of protection for such Personal Data (within the meaning of the European Data Protection Law), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Laws. Such measures may include (without limitation) (i) transferring such Customer Data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including to an Adequate Country or data privacy and transfer frameworks; (ii) to a recipient that has achieved binding corporate rules authorization in accordance with applicable Data Protection Law; or (iii) to a recipient that has executed the Standard Contractual Clauses.

9.2.2. When Customer and Stage5, or Stage5 and or its Sub-Processor rely on the Standard Contractual Clauses to facilitate a transfer to a third country, the following shall apply:

1. For Transfer of Customer Data from the EEA the EU SCC shall apply and completed as follows: **(1)** Module II (Controller to Processors) will apply; **(2)** In Clause 7 the optional docking clause will not apply; **(3)** In Clause 9, option 2 (general written authorization) shall apply for the Sub-Processors listed under **Annex III** and the method for appointing Sub-Processor shall be as set forth in the Sub-Processing Section of the DPA; **(4)** In Clause 11, the optional language will not apply, and Data Subjects shall not be able to lodge a complaint with an independent dispute resolution body; **(5)** In Clause 17, option 1 shall apply, and the EU SCC shall be governed by the law of the Republic of Ireland; **(6)** In Clause 18(b) the parties choose the competent courts of the Republic of Ireland, as their choice of forum and jurisdiction; **(7) Annex I(A) of the EU SCC** is completed as follows: Customer is the Data Exporter, Stage5 is the Data Importer, the parties' contact details are as completed under the Agreement; **Annex I(B) of the EU SCC** is completed as set out in Annex I of this DPA; **Annex I(C) of the EU SCC** shall identify the competent supervisory authority/ies as the supervisory authority Republic of Ireland; **(8) Annex II of the EU SCC** is deemed completed with the information set out in Annex II of this DPA; **(9) Annex III of the EU SCC** shall be completed with the list of Sub-Processors set out in Annex III of this DPA.
2. For transfer of Customer Data from the UK, the UK SCC shall apply and completed as follows: **(1) Table 1** shall be completed as set forth in section (i)(7) above; **(2) Table 2** shall be completed as set forth in Section (i)(1) – (i)(4) above; **(3) Tables 3** shall be completed as follows: **Annex 1A** shall be completed with relevant information as set out in Section (i)(7) above; **Annex 1B** shall be completed with relevant information as set out in **Annex I** of this DPA; , **Annex II** shall be completed with relevant information as set out in Annex II of this DPA; **Annex III** shall be completed with the list of sub-processors set out in Annex III of this DPA; **(4) Table 4** shall be completed with the "neither party" option; and **(5)** Any conflict between the terms of the EU SCC and the UK SCC will be resolved in accordance with Section 10 and Section 11 of the UK SCC.
3. For transfer of Customer Data from Switzerland, the Swiss SCC shall apply in with following modifications (i) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" will be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" will be replaced with the "the Swiss Federal Data Protection and Information Commissioner " and the "relevant courts in Switzerland".

10. TERM, TERMINATION AND CONFLICT

10.1. This DPA shall be effective as of the Effective Date (as defined in the Agreement) and shall remain in force until the Agreement terminates or as long as Stage5 Processes Customer Data.

10.2. Stage5 shall be entitled to terminate this DPA or cease the Processing of Customer Data in the event that Processing of Customer Data under the Customer's Instructions or this DPA infringe applicable legal requirements, provided Customer did not provide updated Instructions to cure such infringement within ten (10) days from receiving applicable notice from Stage5. Alternately, Stage5 may, in its sole discretion, suspend the Processing of the Customer Data until such infringement is cured without liability to the Customer and without prejudice to any fees incurred by Customer prior to suspension date.

10.3. Following the termination or expiration of this DPA, Stage5 shall, at the choice of the Customer, delete or return all Customer Data Processed on behalf of the Customer and certify to the Customer that it has done so. Until the Customer Data is deleted or returned, the parties shall continue to ensure compliance with this DPA. Customer's choice shall be provided in writing to Stage5, following effect of termination. Notwithstanding the foregoing, Stage5 may retain Customer Data (i) as required by applicable laws; or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Stage5 will maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to retained Customer Data and not further Process it except as required by Data Protection Law.

10.4. In the event of a conflict between the terms and conditions of this DPA and the Agreement, this DPA shall prevail. For the avoidance of doubt, in the event Standard Contractual Clauses have been executed between the parties, the terms of the Standard Contractual Clauses shall prevail over those of this DPA.

ANNEX I

DETAILS OF PROCESSING

This Annex includes certain details of the Processing of Customer Data as required under the Data Protection Law.

Service model	BYOA	All inclusive
Categories of Data Subjects	As uploaded by Customer while using the Services.	
Categories of Personal Data processed:	Input, Output	All data as uploaded by Customer while using the Services, including Input, Output, data retrieved from integrated systems, agent activities, prompts, instructions, etc.
Special Categories of Personal Data:	As shall be determined by the Customer.	
Nature of the processing:	Collection, storage, organization, communication, transfer, host and other types of Processing for the purpose of providing the Services as set out in the Agreement.	
Purpose(s) of Processing:	To provide the Service.	
Retention Period:	For as long as is necessary to provide the Service by Stage5; provided there is no legal obligation to retain the Customer Data post termination or unless otherwise requested by the Customer.	
Process Frequency:	Continuous basis	

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES

Stage5 implements, and throughout the term of this DPA will maintain, a comprehensive information security program which shall take into account the nature, scope and purposes of Processing, the risks to the rights and freedoms of natural persons, the establishment and maintenance technical, physical, and administrative safeguards to: (i) ensure the security, availability, and confidentiality of Customer Data; (ii) protect against any foreseeable threats or hazards to the security or integrity of Customer Data; (iii) protect against any willful, negligent, accidental or unlawful access, acquisition, use, alteration, disclosure, loss or destruction of Customer Data; and (iv) ensure secure and appropriate disposal of Customer Data ("**Information Security Program**"). Stage5 further represents that it implements the following security measures as a part of Information Security Program:

a. Stage5 shall establish a procedure for allowing access to Personal Data and restriction of such access. Stage5 shall ensure that access to Personal Data is strictly limited to those individuals who "need to know" or need to access the Personal Data and as strictly necessary for the purpose of providing the Services and shall keep record of the persons authorized to access the Personal Data subject of the Agreement.
b. Stage5 shall take all steps reasonably necessary to ensure the reliability of the individuals who may have access to Personal Data and shall ensure that each such individual (i) is informed of the confidential nature of the Personal Data; (ii) has received appropriate training on his/her responsibilities; and (iii) is subject to written confidentiality undertakings and written security protocols.
c. Stage5 shall implement physical measures to ensure that access to the Personal Data is granted only to authorized users.
d. Stage5 shall maintain and implement sufficient and appropriate (based on the type of Personal Data and its sensitivity) environmental, physical and logical security measures with respect to the Personal Data and to Stage5's system's infrastructure, data processing system, communication means, terminals, system architecture, hardware and software, in order to prevent penetration and unauthorized access to Customer Data or to Customer's systems.
e. Stage5 shall act in accordance with an appropriate written information security policy and working procedures that comply with the security requirements under this Annex and Data Protection Law, including with respect to backup and recovery procedures. Stage5 shall review its security policies and operating procedures periodically, and when material changes to the systems or Processing are made, all in order to amend them, if required.
f. Stage5 shall take measures to record the access to the Personal Data, including monitoring the entry into the facilities where the Personal Data is Processed, as well as any equipment brought in or taken out of such facilities.

g. Stage5 shall implement automatic control mechanism for verifying access to systems containing Personal Data, which shall include, inter alia, the user identity, date and time of access attempt, the system component attempted to be accessed, type and scope of access and if access was granted or denied. Stage5 shall periodically monitor the information from the control mechanism, list issues and irregularities and the measures taken to handle them. Control records shall be maintained for a minimum of 24 months.
h. Stage5 will perform periodic security risk surveys to systems containing Personal Data.
i. Stage5 will not disclose Personal Data through a public communications network or via the internet, without using industry-standard encryption methods.

ANNEX III

LIST OF SUB-PROCESSORS

As of the effective date above, Stage5 uses the following sub-processors:

Name	Description of the processing
Anthropic (Claude API)	AI language model inference for conversational agents - processes user messages, conversation history, system prompts, interaction context
OpenAI	AI language model inference (alternative provider) - processes user messages, conversation history, interaction context
XAI (Grok)	AI language model inference (default provider) - processes user messages, conversation history, interaction context
Google (Gemini)	AI language model inference (alternative provider) - processes user messages, conversation history, interaction context
Traceloop	LLM observability and performance monitoring - processes LLM call metadata, token usage, latency metrics, conversation traces
Laminar (LMNR)	LLM monitoring and evaluation - processes LLM call parameters, outputs, evaluation metrics
Descope	Authentication and identity management - processes user credentials, email addresses, names, phone numbers, authentication events
Slack	Messaging channel integration - processes user messages, conversation metadata, user identifiers
Telegram	Messaging channel integration - processes user messages, chat identifiers, media files, user IDs
Twilio	WhatsApp messaging services - processes phone numbers, messages, media content, conversation metadata
Forgejo	Git repository management - processes repository content, file changes, user credentials, organization and team data. Run in our local environment.
Temporal.io	Distributed workflow orchestration - processes workflow state, execution data, conversation context, activity inputs/outputs. Run in our local environment.
ConfigCat	Feature flag management - processes tenant/user context for feature evaluation
Composio	Third-party integration platform - processes API credentials, integration metadata, action parameters

Exa	AI-powered web search and content extraction - processes search queries, URLs
Tavily	Web search services - processes search queries
Brave Search	Privacy-focused web search - processes search queries
Firecrawl	Web scraping and content extraction - processes URLs, scraping parameters
CurrencyAPI	Currency conversion services - processes currency conversion requests (no personal data)
Amazon Web Services (AWS)	Cloud infrastructure (Secrets Manager, S3, Lambda) - processes application secrets, PDF files, processing data
Browserbase	Cloud browser automation - processes URLs, web interaction parameters
Google Analytics	Events about how customers interact with the marketing website.
Sentry	Monitoring for the Stage5.ai ui. We use that to monitor errors that happen in Stage5.ai ui so we can improve the product and increase its quality.
Heap	User monitoring for Stage5.ai ui. The idea is to see how users are using the system, where they click, which pages they view, etc.