Last Updated: March 27, 2026

# HiThrive: Data Processing Addendum

**THIS DATA PROCESSING ADDENDUM ("DPA")** forms part of and is incorporated into the HiThrive Master Subscription Agreement or other written or electronic agreement governing Customer's use of the Service ("**Main Agreement**") between Customer and HiThrive (each a "**party**" and together the "**parties**").

In the course of providing the Service to Customer, HiThrive may process Customer Data (defined below) and the parties agree to comply with the following provisions with respect to any processing of Customer Data by HiThrive as a processor or service provider to Customer.

1. **Definitions**. Capitalized terms used in this DPA shall have the meanings given to them in the Main Agreement unless otherwise defined herein. The following definitions are used in this DPA:

   1.1. "**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

   1.2. "**Authorized Affiliate**" means any Customer Affiliate permitted to use the Service pursuant to the Main Agreement but have not signed their own "Main Agreement" and are not a "Customer" as defined under the Main Agreement.

   1.3. "**CCPA**" means Sections 1798.100 et seq. of the California Civil Code and any attendant regulations issued thereunder as may be amended from time to time, including but not limited to the California Privacy Rights Act of 2020 (the "CPRA") and its implementing regulations.

   1.4. "**Customer Data**" means any Customer Content that is Personal Data and that HiThrive processes on behalf of Customer in the course of providing the Service, as more particularly described in Schedule A of this DPA.

   1.5. "**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests (as measured on a fully-diluted basis) then outstanding of the entity in question. The term "Controlled" will be construed accordingly.

   1.6. "**Data Protection Laws**" means all data protection and privacy laws regulations applicable to a party and its processing of Personal Data under the Main Agreement, including, where applicable: (a) the GDPR, (b) all applicable implementations of the GDPR into national law, (c) in respect of the United Kingdom, the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**"), (d) the Swiss Federal Data Protection Act ("**Swiss DPA**"), and (e) the CCPA; in each case, as may be amended, superseded or replaced.

   1.7. "**Europe**" means for the purposes of this DPA the European Economic Area ("EEA"), United Kingdom and Switzerland.

   1.8. "**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

   1.9. "**Personal Data**" means any information protected as "personal data", "personal information" or "personally identifiable information" under Data Protection Laws.

   1.10. "**Restricted Transfer**" means: (i) where the GDPR applies, a transfer of Customer Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission **("EEA Restricted Transfer")**; (ii) where the UK GDPR applies, a transfer of Customer Data from the United Kingdom to any other country which is

not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018 **("UK Restricted Transfer")**; and (iii) where the Swiss DPA applies, a transfer of Customer Data from Switzerland to any other country which is not determined to provide adequate protection for personal data by the Federal Data Protection and Information Commission or Federal Council (as applicable) **("Swiss Restricted Transfer")**.

1.11. "**Standard Contractual Clauses**" means (i) the standard contractual clauses between controllers and processors adopted by European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021 and currently located at: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf, as amended, superseded or replaced from time to time.

1.12. "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data, stored or otherwise processed by HiThrive in connection with the provision of the Service. "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful login attempts, pings, port scans, denial of services attacks, and other network attacks on firewalls or networked systems.

1.13. "**Subprocessor**" means any Processor having access to Customer Data and engaged by HiThrive to assist in fulfilling its obligations with respect to providing the Service pursuant to the Main Agreement (excluding any employee, consultant or independent contractor of HiThrive).

1.14. The terms "**controller**", "**data subject**", "**processor**", "**processing**", "**personal data**" and "**sensitive data**" shall have the meanings given to them in Data Protection Laws or if not defined therein, the GDPR, and terms "**service provider**", "**business**", "**collects**" (and "**collected**" and "**collection**"), "**consumer**", "**business purpose**", "**sell**" (and "**selling**", "**sale**", and "**sold**") and "**service provider**" have the meanings given to them in §1798.140 of the CCPA, as applicable.

1.15. "**UK Addendum**" means the International Data Transfer Addendum (version B1.0) to the EU Commission Standard Contractual Clauses issued by UK Information Commissioners Office under S.119(A) of the UK Data Protection Act 2018, as amended, superseded or replaced from time to time.

2. Roles and Scope of Processing

2.1. **Data Processing Roles**. HiThrive shall process Customer Data for the Permitted Purpose as a processor on behalf of Customer as the controller. For the purposes of the CCPA (where applicable), HiThrive shall process Customer Data as a service provider for the Customer as a business.

2.2. **Compliance with Laws**. Each party shall comply with its obligations under Data Protection Laws in respect of any Customer Data it processes under this DPA. For the avoidance of doubt, HiThrive is not responsible for complying with Data Protection Laws uniquely applicable to Customer by virtue of its business or industry, such as those generally applicable to online service providers.

2.3. **Processing Instructions**. HiThrive shall process Customer Data in accordance with Customer's documented lawful instructions, unless obligated to do otherwise by applicable law, in which case HiThrive will notify Customer (unless that law prohibits HiThrive from doing so on important grounds of public interest). For these purposes, Customer instructs HiThrive to process Customer Data for the purposes described in Schedule A (the "**Permitted Purpose**", which, where CCPA applies, is a business purpose). The DPA and Main Agreement are Customer's complete and final instructions. Any additional or alternate instructions must be consistent with the terms of the DPA and the Agreement. Without prejudice to Section 2.4 (Customer Responsibilities), HiThrive shall promptly notify Customer in writing, unless prohibited from doing so under Data Protection Laws, if it becomes aware or believes that any processing instructions from Customer violates Data Protection Laws (but without obligation to actively monitor Customer's compliance with Data Protection Law) and in such event, HiThrive shall not be obligated to undertake such processing until such time as the Customer has

updated its processing instructions and HiThrive has determined that the incidence of non-compliance has been resolved.

2.4. **Customer Responsibilities**. Customer shall, in its use of the Service and provision of instructions, process Customer Data in accordance with Data Protection Laws. Customer is solely responsible for: (i) the accuracy, quality, and legality of the Customer Data, (ii) the means by which Customer acquired such Customer Data; and (iii) the instructions it provides to HiThrive regarding the processing of such Customer Data. Customer shall ensure (i) that it has provided notice and obtained (or will obtain) all consents and rights necessary for HiThrive to process Customer Data pursuant to the Main Agreement and this DPA, (ii) its instructions are lawful and that the processing of Customer Data in accordance with such instructions will not violate applicable Data Protection Laws, and (iii) where the CCPA applies, that the Customer Data is provided to HiThrive in order to perform the Service for a valid business purpose only.

**3. Subprocessing**

3.1. Authorized Subprocessors. Customer provides a general prior authorization for HiThrive to engage Subprocessors and, where CCPA applies, other third party service providers (hereinafter referred to as Subprocessors) in order to provide the Service. A list of Subprocessors currently engaged by HiThrive is available to Customer upon written request to privacy@hithrive.com ("**Subprocessor List**"). HiThrive will remain responsible for any acts or omissions of any Subprocessor that cause HiThrive to breach any of its obligations under this HiThrive DPA.

3.2. Notification of New Subprocessors. At least ten (10) days prior to authorizing any new Subprocessor to process Customer Data, HiThrive will provide written notice to Customer of the intended change.

**4. Security Measures and Security Incident Response**

4.1. Security Measures. HiThrive will implement and maintain appropriate and reasonable technical and organizational security measures designed to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data in accordance with the security measures described in Schedule B ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that HiThrive may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service provided to Customer.

4.2. Personnel. HiThrive restricts its personnel from processing Customer Data without authorization by HiThrive as set forth in the Security Measures and shall ensure that any person who is authorized by HiThrive to process Customer Data is under an appropriate obligation of confidentiality. HiThrive requires all personnel with access to Customer Data to complete security awareness training within fourteen (14) days of hire and at least annually thereafter.

4.3. Customer Responsibilities. Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Data transmitted via the systems it administers and maintains (i.e. email encryption), and taking any appropriate steps to securely encrypt or back up any Customer Data uploaded to the Service.

4.4. Security Incident Response. Upon becoming aware of a Security Incident, HiThrive will notify Customer without undue delay and, in any case within seventy-two (72) hours after becoming aware. HiThrive will provide information relating to the Security Incident to Customer promptly as it becomes known or as is reasonably requested by Customer to fulfil Customer's obligations as controller. HiThrive will also take appropriate and reasonable steps to contain, investigate, and mitigate any Security Incident.

5. **Audit and Records.**

5.1. Audit Rights. HiThrive shall make available to Customer all information in HiThrive's possession or control and provide all assistance in connection with audits of HiThrive's premises, systems, and documentation as Customer may reasonably request to enable Customer to assess HiThrive's compliance with this DPA. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including this Section 5 and where applicable, the Standard Contractual Clauses) by instructing HiThrive to comply with the audit measures described in the Security Measures and Section 5.2 below.

5.2. Audit Procedures. Where required under Data Protection Laws or where a data protection authority requires , Customer may, on giving at least thirty (30) days prior written notice, request that Customer's personnel or a third party (at Customer's expense) conduct an audit of HiThrive's facilities, equipment, documents and electronic data relating to the processing of Customer Data under the Main Agreement to the extent necessary to inspect and/or audit HiThrive's compliance with this DPA, provided that: (i) Customer shall not exercise this right more than once per calendar year; (ii) such additional audit enquiries shall not unreasonably impact in an adverse manner HiThrive's regular operations and do not prove to be incompatible with applicable Data Protection Laws or with the instructions of the relevant data protection authority; (iii) before the commencement of such additional audit, the parties shall mutually agree upon the scope, timing, and duration of the audit, and (iv) at all times during the scope of the audit, Customer and any appointed third party will comply with HiThrive's policies, procedures, and reasonable instructions governing access to its systems and facilities, including limiting or prohibiting access to information that is confidential information. Without prejudice to the foregoing, HiThrive will provide all assistance reasonably requested by Customer to accommodate Customer's request.

6. **Data Transfers**. Customer acknowledges and agrees that HiThrive may transfer and process Customer Data to and in the United States and other locations in which HiThrive, its Affiliates, or its Subprocessors maintain data processing operations as more particularly described in the Subprocessor List (available upon written request). HiThrive shall ensure that such transfers are made in compliance with Data Protection Laws and this DPA.

7. **Return or Deletion of Data**. Promptly upon Customer's request, or within one hundred eighty (180) days after the termination or expiration of the Main Agreement, HiThrive shall delete or return Customer Data in its possession or control. This requirement shall not apply to the extent HiThrive is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data HiThrive shall securely isolate and protect from any further processing, except to the extent required by such laws.

**8. Cooperation**

8.1. Data Subject and Consumer Rights Requests. HiThrive shall, taking into account the nature of the processing, reasonably assist Customer in responding to any requests from individuals or applicable data protection authorities relating to the processing of Customer Data for the Permitted Purposes.

(a) In the event that any such request is made to HiThrive directly, HiThrive will not respond to such communication directly (except to direct the data subject to contact Customer) without Customer's prior authorization, unless legally compelled to do so. If HiThrive is required to respond to such a request, HiThrive will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

(b) If Customer is unable to respond to the request with regard to personal data processed by HiThrive in its capacity as either a processor or service provider to Customer (as applicable), upon Customer's reasonable request, and subject to any applicable restrictions or exemptions under applicable law, HiThrive will use reasonable efforts to assist Customer in responding to verified individual requests received by Customer as it relates to the processing of personal data by HiThrive as a processor or service provider to Customer.

8.2. Data Protection Impact Assessments (DPIAs). To the extent required under Data Protection Laws applicable to Europe, HiThrive will provide requested information regarding the Service necessary to enable Customer to carry out data protection impact assessments and prior consultations with data protection authorities.

9. Europe

9.1. Scope. The terms in this Section 9 apply only if and to the extent Customer is established in Europe or the Customer Data is otherwise subject to Data Protection Laws applicable to Europe.

9.2. Subprocessor Obligations. HiThrive will enter into a written agreement with each Subprocessor imposing data protection obligations no less protective of Customer Data as this DPA or the Data Protection Laws to the extent applicable to the nature of the services provided by such Subprocessor.

9.3. Subprocessor Objection Right. If Customer objects on reasonable grounds relating to data protection to HiThrive's use of a new Subprocessor, then Customer shall promptly, and within ten (10) days following HiThrive's notification pursuant to Section 3.2 (Notification of new Subprocessors) above, provide written notice of such objection to HiThrive. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties cannot agree to a mutually acceptable resolution, Customer shall as its sole and exclusive remedy have the right to terminate the relevant affected portion(s) of the Service without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination). Upon termination by Customer pursuant to this Section, HiThrive shall refund Customer any prepaid fees for the terminated portion(s) of the Service that were provided after the effective date of the termination.

9.4. Transfer Mechanism. To the extent the transfer of Customer Data from Customer to HiThrive is a Restricted Transfer and Data Protection Laws applicable to Europe require that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses, which shall be incorporated by reference into and form an integral part of this DPA, as follows:

(a) In connection with an EEA Restricted Transfer: (i) Module Two (*controller to processor transfers*) shall apply and all other modules are deleted; (ii) in Clause 7, the optional docking clause will apply; (ii) in Clause 9 of Module Two, Option 2 will apply and the time period for prior notice of Sub-processor changes is identified in Section 3.2 of this DPA; (iii) in Clause 11, the optional language will not apply; (iv) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Irish law; (v) in Clause 18(b), disputes shall be resolved before the courts of Ireland; (vi) Annex I shall be deemed completed with the information set out in Schedule A (Description of Processing/ Transfer) of this DPA; and (vii) Annex II shall be deemed completed with the information set out in Schedule B (Security Measures) (as applicable) of this DPA.

(b) In connection with a UK Restricted Transfer, the Standard Contractual Clauses shall apply in accordance with Section 9.4(a) above, but as modified and interpreted by the Part 2: Mandatory Clauses of the UK Addendum, which shall be incorporated into and form an integral part of this DPA. Any conflict between the terms of the Standard Contractual Clauses and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Schedule A and Schedule B of this DPA and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

(c) In connection with a Swiss Restricted Transfer, the Standard Contractual Clauses shall apply in accordance with Section 9.4(a) above, but with the following modifications: (i) any references in the Standard Contractual Clauses to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA and the equivalent articles or sections therein; (ii) any references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; (iii) any references to the "competent supervisory

authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in Switzerland; and (iv) the Standard Contractual Clauses shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts.

(d) The rights and obligations afforded by Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

9.5. Data Transfer Arrangements. To the extent HiThrive adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to Data Protection Laws) for the transfer of Personal Data ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Data Protection Laws applicable to Europe and extends to territories to which Personal Data is transferred).

9.6. Notification of Government Access Requests. For the purposes of Clause 15(1)(a) of Standard Contractual Clauses, HiThrive shall notify Customer and not the data subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the data subject, as necessary.

**10. Authorized Affiliates**

10.1. Affiliate Communications. Customer is responsible for coordinating all communications with HiThrive on behalf of its Authorized Affiliates with regard to this DPA. Customer represents that it is authorized to issue instructions as well as make and receive any communications in relation to this DPA on behalf of its Authorized Affiliates.

10.2. Affiliate Enforcement. Authorized Affiliates may enforce the terms of this DPA directly against HiThrive, subject to the following provisions:

(a) Customer will bring any legal action, suit, claim, or proceeding which the Affiliate would otherwise have if it were a party to the Main Agreement (each an "Affiliate Claim") directly against HiThrive on behalf of such Affiliate, except where Data Protection Laws to which the relevant Affiliate is subject require that the Affiliate bring or be a party to such Affiliate Claim; and

(b) for the purpose of any Affiliate Claim brought directly against HiThrive by Customer on behalf of such Affiliate in accordance with this Section, any losses suffered by the relevant Affiliate may be deemed to be losses suffered by Customer.

**11. Limitation of Liability**

11.1. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

11.2. Any claim or remedies Customer or its Affiliates may have against HiThrive and its respective employees, agents, or Subprocessors arising under or in connection with this DPA including: (i) for breach of this DPA (including the Standard Contractual Clauses or the UK Addendum); (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; (iii) under Data Protection Laws, including but not limited to CCPA, GDPR, UK GDPR or Swiss DPA, including any claims relating to damages paid to a data subject, consumer, or other individual; and (iv) breach of its obligations under the Standard Contractual Clauses or UK Addendum, will, to the maximum extent permitted by law, be subject to any limitation and exclusion of liability provisions (including any agreed aggregate financial cap) that apply under the Main Agreement.

11.3. For the avoidance of doubt, HiThrive and its Affiliates' total overall liability for all claims from Customer and its Affiliates arising out of or related to the Main Agreement and each DPA shall apply in the aggregate for all claims under the Main Agreement and this DPA together, including by Customer and its Affiliates.

**12. CCPA**

12.1. Scope. The terms in this Section 12 apply only if and to the extent the Customer Data is subject to Data Protection Laws applicable to the state of California.

12.2. For the purposes of the CCPA, HiThrive is prohibited from:

(a) selling Customer Data;

(b) sharing Customer Data (as the term "share" is defined under the CCPA);

(c) processing Customer Data for targeted and/or cross context behavioral advertising;

(d) retaining, using, or disclosing Customer Data for any purposes other than the specific purposes of performing the Service or as otherwise permitted under Main Agreement and this DPA;

(e) retaining, using, or disclosing Customer Data outside the direct business relationship between HiThrive and Customer.

(f) combining Customer Data with any other data if and to the extent doing so would be inconsistent with the Business Purpose or the limitations on service providers under the CCPA or other Data Protection Laws.

12.3. HiThrive hereby certifies that it understands the restrictions set out in Section 12.1 and will comply with them, and that it will notify Customer if HiThrive becomes unable to comply with the CCPA.

12.4. Notwithstanding the foregoing and anything to the contrary in the Main Agreement (including this DPA), Customer acknowledges that HiThrive shall have a right to process Customer Data for the purposes of creating anonymized, aggregate and/or de-identified information for its own legitimate business purposes, including where Customer has requested a HiThrive Service that includes the provision of benchmarking reports, compiling anonymized benchmarking reports and statistics.

12.5. HiThrive maintains, and will continue to maintain during the term of the Main Agreement, tools and resources for consumers to exercise their rights under the CCPA. If HiThrive, directly or indirectly, receives a request submitted by a consumer who is an employee of Customer to exercise a right it has under the CCPA in relation to that Consumer's Customer Data, HiThrive will follow the procedures described in Section 8 of this DPA.

**13. General**

13.1. The parties agree that this DPA shall replace any existing DPA the parties have previously entered into in connection with the Service.

13.2. As between Customer and HiThrive, this DPA is incorporated into and subject to the terms of the Main Agreement and shall be effective and remain in force for the term of the Main Agreement or the duration of the Service. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Customer Data.

13.3. Except as described in Section 10 (Authorized Affiliates), in no event shall this DPA benefit or create any right or cause of action on behalf of a third party, but without prejudice to the rights or remedies available to data subjects under Data Protection Laws or this DPA (including the Standard Contractual Clauses).

13.4. Each party acknowledges that the other party may disclose the Standard Contractual Clauses, this DPA, and any privacy related provisions in the Main Agreement to any regulator or supervisory authority upon request.

13.5. Notwithstanding anything to the contrary in the Main Agreement and without prejudice to Section 2.3, HiThrive may periodically make modifications to this DPA as may be required to comply with Data Protection Laws.

13.6. Other than as required by applicable Data Protection Laws or the Standard Contractual Clauses, the dispute mechanisms, including those related to venue and jurisdiction, set forth in the Main Agreement govern any dispute pertaining to this DPA.

**SIGNATURE PAGE TO DATA PROCESSING ADDENDUM**

This Data Processing Addendum has been entered into and become a binding and effective part of the Main Agreement with effect as of the date last executed below.

| | | | |
|---|---|---|---|
| _____ (Customer Legal Name) | | **HiThrive Inc.** | |
| **Name** (fully written out): | _____ | **Name** (fully written out): | Joshua Zacharias |
| **Email:** | _____ | | |
| **Title:** | _____ | **Title:** | CEO |
| **Signature:** | _____ | **Signature:** | _____ |
| **Date:** | _____ | **Date:** | _____ |

**SCHEDULE A:** Description of Processing / Transfer

**Annex 1(A) List of Parties:**

| Data Exporter | Data Importer |
|---|---|
| **Name:** The party named as the 'Customer" in the Main Agreement. | **Name:** HiThrive Inc. ("HiThrive") |
| **Address:** The address for the Customer associated with its HiThrive account or as otherwise specified in the Order Form or Main Agreement. | **Address:** 8 The Green #4000, Dover, DE 19901 |
| **Contact Person's Name, position and contact details:** The contact details associated with the Customer's HiThrive account or as otherwise specified in the Order Form or Main agreement. | **Contact Person's Name, position and contact details:** Joshua Zacharias, CEO, privacy@hithrive.com |
| **Activities relevant to the transfer:** See Annex 1(B) below. | **Activities relevant to the transfer:** See Annex 1(B) below |
| **Signature and Date:** By using the Service to transfer Customer Data to HiThrive located in a non-adequate country, the data exporter will be deemed to have signed this Annex 1. | **Signature and Date:** By transferring Customer Data to non-adequate country on Customer's instructions, the data importer will be deemed to have signed this Annex 1. |
| **Role:** Controller | **Role:** Processor |

**Annex 1(B) Description of Transfer:**

| Data Exporter | Data Importer |
|---|---|

| | |
|---|---|
| **Categories of Data Subjects:** | Depending on the nature of the Service, Personal Data transferred may concern the following categories of data subjects:<br>• Customer's current and former employees, agents, advisors, contractors and other personnel (who are natural persons) ("**Customer Personnel**')<br>• Users of the Service who are customer's current and former employees, agents, advisors, contractors and other personnel (who are natural persons) ("**Users**") |
| **Categories of Personal Data:** | **<u>Customer Personnel:</u>**<br>The types of Personal Data processed by HiThrive are determined and controlled by Customer in its sole discretion and may include, but are not limited to the following categories of Personal Data:<br>• general employee information including name, email, phone number, job title, department, and direct manager;<br>• specific information related to the employees' professional accomplishments, awards and performance.<br>**<u>Users:</u>**<br>Depending on the nature of the Services, the Personal Data may include:<br>• Account log-in credentials such as email, username and password, and unique user or team ID;<br>• Business contact information such as name, phone number, email address and mailing address;<br>• Employment information, such as employer, job title, |
| **Special category data (if appropriate):** | HiThrive does not intentionally collect or process special category data. However, Customer may submit special category data to the Service, the extent of which is determined and controlled by Customer in its sole discretion. |

| | |
|---|---|
| **Frequency of the transfer (one-off or continuous):** | Continuous basis depending on the nature of the Service. |
| **Nature of processing:** | The nature of the processing is the performance of the Service in accordance with the Main Agreement. |
| **Purpose(s) of the data transfer and further processing:** | The transfer is made for the following purposes: (i) to provide and improve the Service provided to Customer in accordance with the Main Agreement; (ii) processing initiated by Users in their use of the Service; (iii) to comply with other reasonable instructions provided by Customer (e.g. via email or support tickets) that are consistent with the terms of the Main Agreement and this DPA, and (iv) to comply with any legal obligation under applicable law, including Data Protection Law.<br><br>Where HiThrive benchmarking is provided as part of the Service requested by Customer, Customer Data may also be aggregated with other customer's Customer Data for the purposes analyzing overall trends to compile anonymized benchmarking reports and statistics requested by Customer in connection with its use of the Service, in accordance with the Main Agreement.<br><br>Where Customer chooses to use a HiThrive AI feature, Customer authorizes, instructs, and warrants that it has obtained any necessary consents required for HiThrive and its Subprocessors to process Customer Data for the purpose of providing HiThrive AI output and functionality, and as necessary to comply with applicable law or regulation. |
| **Retention period (or, if not possible to determine, the criteria used to determine that period):** | The duration of the processing is the term of Main Agreement or any applicable Order Form plus the period from expiration of the Main Agreement or Order Form (as applicable) until the return or deletion of the personal data by HiThrive in accordance with the DPA. |

| | |
|---|---|
| **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:** | As above |

**Annex 1(C): Competent supervisory authority**

The competent supervisory authority shall be determined in accordance with Clause 13 of 2021 Controller-to-Processor Clauses and the GDPR.

**SCHEDULE B:** Technical and Organizational Security Measures

HiThrive maintains the following technical and organizational security measures with respect to Customer Data. HiThrive may update these measures from time to time, provided that such updates do not materially degrade the overall security of the Service.

**1. Infrastructure and Hosting**

HiThrive operates on a platform-as-a-service (PaaS) architecture hosted on Google Cloud Platform ("GCP"). Physical and environmental security controls for GCP data center facilities—including perimeter security, badge and biometric access controls, continuous video surveillance, and visitor escort requirements—are the responsibility of GCP and are addressed via GCP's own certifications, which HiThrive reviews at least annually. HiThrive's production infrastructure includes Cloud Run container services, GCP Datastore, Pub/Sub messaging, Memory Store, Cloud Buckets, and VPC private networking. All application containers are deployed behind a managed firewall with inbound traffic restricted to HTTPS connections through designated frontend endpoints.

**2. Encryption**

All Customer Data is encrypted at rest using industry-standard encryption protocols. All Customer Data transmitted over public networks is encrypted in transit using HTTPS/TLS 1.2 or higher. Cryptographic keys are managed through GCP Key Management Service (KMS), providing key generation, rotation, and secure storage. Access to encryption keys is restricted to authorized personnel with a documented business need. Customer Data backups are encrypted, with access restricted to key personnel.

**3. Access Controls**

HiThrive controls access to production systems and Customer Data through a role-based access control (RBAC) system applying the principle of least privilege. User access rights are provisioned based on job role and function and require documented manager approval. Production system access requires unique usernames and passwords or SSH keys, and multi-factor authentication (MFA). Remote access is permitted only via approved encrypted connections. Access to production networks, databases, operating systems, and firewalls is restricted to authorized personnel with a documented business need. User access rights are reviewed at least quarterly, and access for terminated employees is revoked within three business days of termination. HiThrive maintains a formal production system asset inventory and a data classification policy ensuring confidential data is properly secured and restricted to authorized personnel.

**4. Network Security**

HiThrive's network is segmented to prevent unauthorized access to Customer Data. Firewalls are configured to prevent unauthorized access, with firewall rulesets reviewed at least annually and required changes tracked to completion. Network and system hardening standards are documented based on industry best practices and reviewed at least annually. HiThrive employs GCP Security Command Center for automated intrusion detection and continuous network threat monitoring. HiThrive conducts annual network penetration testing using an independent external security firm; identified issues are triaged and remediated through HiThrive's incident response and change management processes. Upon reasonable written request, HiThrive will provide Customer with the executive summary of the most recent penetration test report, subject to confidentiality obligations.

**5. Vulnerability Management**

HiThrive employs continuous automated vulnerability scanning on production servers, including source code scanning for common security issues and known vulnerabilities in open-source dependencies. HiThrive maintains an internal SLA for responding to and remediating identified vulnerabilities based on severity. External-facing systems are subject to host-based vulnerability scans at least quarterly, with critical and high vulnerabilities tracked to remediation. Infrastructure is patched routinely and in response to identified vulnerabilities to maintain production system hardening.

**6. Incident Response and Availability**

HiThrive maintains a documented incident response plan covering identification, containment, eradication, recovery, and notification for security and data privacy events. HiThrive performs continuous internal monitoring of applications, databases, and cloud infrastructure. Failed application containers are automatically replaced to minimize downtime. Customer Data is backed up regularly within GCP with daily backups and seven-day point-in-time recovery (PITR), monitored by the CTO and engineering team. A risk management program is maintained covering threat identification, risk rating by likelihood and impact, and documented mitigation strategies.

**7. Change Management and Development Practices**

HiThrive maintains documented SDLC policies governing development, acquisition, implementation, and maintenance of information systems. All changes to software and infrastructure are required to be authorized, documented, tested, reviewed, and approved before production deployment. Development and testing environments are logically separated from production. Version control software maintains source code history and supports rollback. A CI/CD pipeline automates build, test, and deployment of container images. Management approvals for production changes are documented in HiThrive's ticketing system.

**8. Data Retention and Disposal**

HiThrive maintains formal retention and disposal procedures for Company and Customer Data. Customer Data is purged or removed from the application environment upon Customer's departure from the Service in accordance with best practices and the Main Agreement. Electronic media containing confidential information is purged or destroyed in accordance with best practices, with certificates of destruction issued for each device destroyed.

**9. Personnel Security**

HiThrive conducts background checks on all new employees as part of the hiring process. New employees are required to acknowledge HiThrive's code of conduct and sign a confidentiality agreement during onboarding. Contractors are required to sign a confidentiality agreement at engagement, and contractor agreements incorporate or reference HiThrive's code of conduct. All personnel with access to Customer Data are required to complete security awareness training within fourteen (14) days of hire and at least annually thereafter. Information security policies and procedures are reviewed at least annually. Roles and responsibilities for information security controls are formally assigned in job descriptions and a Roles and Responsibilities policy.

**10. Vendor Management**

HiThrive maintains a vendor management program that includes a critical third-party vendor inventory, documented security and privacy requirements for vendors, and at least annual review of critical third-party vendors. HiThrive reviews attestation reports (including SOC 2 and equivalent) from subservice organizations and monitors for relevant security incidents reported by those vendors.

**11. SOC 2 Certification**

HiThrive maintains a SOC 2 certification relevant to Security. HiThrive will make its most recent SOC 2 report available to Customer upon reasonable written request, subject to confidentiality obligations.