LEANPATH DATA PROCESSING ADDENDUM

This Leanpath Data Processing Addendum, including its Annexes and the Standard Contractual Clauses and UK Addendum ("**DPA**"), is supplemental to and forms part of the electronic terms of service or written agreement for the provision of the Leanpath Services ("**Agreement**") entered into between Leanpath, Inc. ("**Leanpath**") and the entity referred to as "**Customer**" in the Agreement.

Customer enters into the DPA on behalf of itself and, to the extent required under Applicable Data Protection Law, in the name and on behalf of any Authorized Affiliate (defined below). Capitalized terms used herein and not otherwise defined in this DPA shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of this DPA and the Agreement, this DPA shall prevail.

This DPA applies solely to processing of Customer Personal Data within environments controlled by Leanpath or its Subprocessors and describes the parties' obligations with respect to the processing of such Customer Personal Data to ensure compliance with Applicable Data Protection Law.

The parties agree as follows:

1. Definitions

1.1 "**Affiliate**" means an entity that directly or indirectly controls, is controlled by, or is under common control with a party where "control" means either (a) direct or indirect ownership or control of greater than 50% of the voting securities of such entity; or (b) the ability to control the activities of the entity through contractual rights.

1.2 "**Applicable Data Protection Law**" means data protection and privacy laws and regulations applicable to a party and its respective processing of Customer Personal Data under the Agreement, including where applicable (a) the General Data Protection Regulation 2016/679 ("**GDPR**"); (b) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the Data Protection Act 2018 (together, "**UK GDPR**"); and (c) the Swiss Federal Data Protection Act and its implementing regulations and ordinance ("**Swiss Data Protection Act**"); the California Consumer Privacy Act ("**CCPA**"), the Virginia Consumer Data Protection Act ("**VCDPA**") and other similar U.S. state data protection laws in effect; in each case, as amended, superseded or replaced from time to time.

1.3 "**Authorized Affiliate**" means a Customer Affiliate that is authorized to use the Services under the Agreement and has not signed their own separate Agreement with Leanpath.

1.4 "**Authorized Person**" means any person authorized by Leanpath to process Customer Personal Data, including Leanpath employees, officers, contractors and consultants.

1.5 "**Customer Personal Data**" means any personal data contained within Customer Content and processed by Leanpath on behalf of Customer to perform the Services under the Agreement.

1.6 "**Europe**" means for the purposes of this DPA, the European Economic Area, Switzerland and the United Kingdom.

1.7 "**Restricted Transfer**" means: (i) where the GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the UK to any other country which is not based on adequacy regulations pursuant to section 17A of the Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner, in each case whether such transfer is a direct or onward transfer.

1.8 "**Personal Data Breach**" means a confirmed breach of security leading to any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data processed in environments controlled by Leanpath or its Subprocessors. A "Personal Data Breach" does not include activity that does not compromise Customer Personal Data, including (but not limited to) any unsuccessful attempt to access Customer Personal Data or Leanpath equipment or facilities storing Customer Personal Data, including without limitation pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

1.9 "**Security Addendum**" means the Leanpath Security Addendum attached here as Annex C as may be updated from time to time in accordance with this DPA.

1.10 "**Services**" means those services and activities to be supplied to or carried out by or on behalf of Leanpath for Customer pursuant to the Agreement.

1.11 "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, as amended, superseded or replaced from time to time.

1.12 "**Subprocessor**" means any third party processor used by Leanpath to process Customer Personal Data, including any Leanpath Affiliate. A "Subprocessor" does not include any employee, contractor or consultant of Leanpath or its Affiliates.

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

The lower case terms "**controller**," "**processor**," "**personal data**," "**data subject**," "**process**," and "**processing**" have the meanings given to them by the GDPR. The term "controller" includes "business", the term "data subject" includes "consumers", and the term "processor" includes "service provider" (in each case, as defined by the CCPA).

2. Scope and Role of the Parties

2.1 Scope and details of processing. This DPA applies solely to the extent that Leanpath processes Customer Personal Data subject to Applicable Data Protection Law as a processor. The subject matter, nature, purpose, and duration of the processing, as well as the types of personal data processed and categories of data subjects involved, are described in Annex A.

2.2 Leanpath's role and processing instructions. Leanpath shall process Customer Personal Data as a processor on Customer's behalf and solely in accordance with Customer's lawful documented instructions, which instructions shall include processing initiated by Customer in the use of and configuring of the Services. For these purposes, Customer instructs Leanpath to process Customer Personal Data to perform the Services in accordance with the Agreement, including this DPA (the "Permitted Purposes"). The parties agree that the Agreement (including this DPA) sets out Customer's complete and final instructions to Leanpath in relation to the processing of Customer Personal Data and processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.

2.3 Customer's responsibilities. Customer shall be responsible for complying with its obligations under Applicable Data Protection Law in its processing of Customer Personal Data. In particular, Customer agrees that it shall (a) be responsible for determining whether the Services are appropriate for processing Customer Personal Data consistent with Customer's legal and regulatory obligations; (b) comply with its obligations under Applicable Data Protection Law in its use of the Services and any processing instructions it issues to Leanpath; and (c) ensure it has the right make available Customer Personal Data to Leanpath, including providing notice and obtaining all consents necessary under Applicable Data Protection Law for Leanpath (and its Subprocessors) to lawfully process Customer Personal Data for the Permitted Purposes. Leanpath is not responsible for determining whether Customer's instructions are compliant with applicable law; however, Leanpath shall inform Customer if, in its opinion, Customer's processing instructions infringe Applicable Data Protection Law, in which case Leanpath shall not be required to comply with such instruction. Taking into account the nature of the processing, Customer agrees that it is unlikely that Leanpath would become aware that any Customer Personal Data processed by Leanpath is inaccurate or outdated. To the extent Leanpath becomes aware of such inaccurate or outdated data, Leanpath will inform the Customer.

2.4 Third-party controllers. Where Customer is itself a processor of Customer Personal Data acting on behalf of a third party controller (or other intermediaries), Customer represents and warrants that (a) it is authorized to provide Customer Personal Data to Leanpath and that Customer's processing instructions reflect and do not conflict with the instructions of such third party controller; and (b) it will act as the sole point of contact for Leanpath with regard to such third party controller and Leanpath need not interact directly with (including seeking authorizations directly from or providing notifications directly to) such third party controller other than through the regular provision of the Services.

3. Leanpath Data Processing Obligations

3.1 Confidentiality. Leanpath shall ensure that any Authorized Person is subject to a duty of confidentiality (whether contractual or statutory) and that they shall only process Customer Personal Data for the Permitted Purposes.

3.2 Security. Leanpath shall implement and maintain appropriate technical and organizational measures designed to (a) protect Customer Personal Data from Personal Data Breaches and (b) preserve the security, confidentiality and integrity of Customer Personal Data, as further described in the Security Addendum.

3.3 Security Updates.Leanpath may update the Security Addendum from time to time, provided that any updates shall not materially diminish the overall security of Customer Personal Data. Customer shall be responsible for reviewing the Security Addendum and any other information made available by Leanpath relating to data security and making an independent determination as to whether the Security Addendum meets the Customer's requirements and obligations under Applicable Data Protection Law.

3.4 Personal Data Breaches.Leanpath shall inform Customer without undue delay upon becoming aware of a Personal Data Breach and take such measures as Leanpath may deem necessary and reasonable to remediate the Personal Data Breach. Leanpath shall provide Customer with timely information about the nature of the Personal Data Breach as such information becomes known or available to Leanpath, and provide reasonable cooperation and assistance to enable Customer to comply with its obligations under Applicable Data Protection Law with respect to notifying the relevant supervisory authority and/or affected data subjects. The obligations described in this Section 3.4 shall not apply to Personal Data Breaches that result from Customer's actions or omissions, and any obligation to report or respond to a Personal Data Breach will not be construed as an acknowledgement by Leanpath of any fault or liability with respect to such Personal Data Breach or the Customer Personal Data concerned.

3.5 Audits.

(a) Upon Customer's request, and no more than once per calendar year, Leanpath shall (a) make available for Customer's review summary copies (on a confidential basis) of existing audit reports and certifications (each, an "**Audit Report**") to help Customer assess Leanpath's compliance with this DPA and Applicable Data Protection Law; and (b) only to the extent a supervisory authority determines that Leanpath's provision of such Audit Reports does not provide sufficient information to allow Customer to assess Leanpath's compliance with this DPA or Applicable Data Protection Law, Customer shall have the right, at Customer's expense, to conduct an audit or assessment of reasonable scope and duration to a mutually agreed-upon audit or assessment plan with Leanpath that is consistent with the Audit Parameters ("**Audit**").

(b) Each Audit must conform to the following parameters ("**Audit Parameters**"): (i) be reasonable in scope taking into account the architecture of and use by Customer of the Services

(ii) be conducted by an independent third party that will enter into a confidentiality agreement with Leanpath; (iii) occur at a mutually agreed date and time and only during Leanpath's regular business hours; (iv) occur no more than once annually with at least three weeks' advance written notice; (v) cover only facilities controlled by Leanpath; (vi) not violate any obligation between Leanpath and its service providers or third-party, (vii) restrict findings to only Customer Personal Data relevant to Customer; and (viii) obligate Customer, to the extent permitted by law or regulation, to keep confidential any information gathered that, by its nature, should be confidential.

(c) The parties agree that the audit rights granted under the Standard Contractual Clauses shall be exercised in accordance with this Section 3.5.

3.6 Subprocessors.

(a) Customer provides a general authorization for Leanpath to appoint Subprocessors, including the Subprocessors listed at Annex D ("**Subprocessor List**").

(b) Leanpath will: (i) ensure that each Subprocessor shall be bound by a written agreement, including data protection terms and security measures, no less protective of Customer Personal Data than the Agreement and this DPA; and (ii) be liable for any breach of this DPA caused by an act, error or omission of its Subprocessors to the extent Leanpath would have been liable had such breach been caused by Leanpath.

(c) Leanpath shall notify Customer if it engages a new Subprocessor at least thirty (30) days prior to any such change if Customer opts-in to receive such notifications in the manner made available on the Subprocessor List.

(d) Customer may object in writing to Leanpath's appointment of a new Subprocessor based on reasonable data protection concerns by emailing dpo@leanpath.com within ten (10) days of notice of a new Subprocessor from Leanpath and the parties will discuss such concerns in good faith. If the parties are unable to reach a mutually agreeable resolution within ten (10) days, Customer, as its sole and exclusive remedy, may terminate the Services with only respect to the portions of the Services which cannot be provided by Leanpath without the use of the new Subprocessor.

3.7 Cooperation.

(a) Data Subject Rights. Leanpath shall, taking into account the nature of the processing, provide Customer with reasonable assistance (including by appropriate technical and organization measures, in so far as this is possible) to enable Customer to respond to (i) any requests from a data subject seeking to exercise any of its rights under Applicable Data Protection Law (including its right of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Customer Personal Data (collectively "**Correspondence**"). In the event the Correspondence is made directly to Leanpath,

it shall where the Customer is identified or identifiable from the Correspondence, promptly notify Customer and shall not, unless legally compelled to do so, respond directly to the Correspondence except to refer the requestor to Customer to allow Customer to respond as appropriate. Any assistance provided shall be relevant to the Services that support the processing of Customer Personal Data and commercially reasonable and proportionate to the objective of the exercise with which Leanpath is requested to assist.

(b) Law Enforcement Requests. If Leanpath receives a subpoena, court order, warrant or other legal demand from law enforcement or public or judicial authorities seeking the disclosure of Customer Personal Data, Leanpath shall, where the Customer is identified or identifiable from such disclosure request and to the extent required and permitted by applicable law, promptly notify Customer of such request and reasonably cooperate with Customer to limit, challenge or protect against such disclosure.

(c) Data Protection Assessments; Data Protection Impact Assessments. Leanpath shall provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under Applicable Data Protection Law to conduct a data protection assessment, data protection impact assessment and/or to consult with the competent supervisory authorities with respect to Leanpath's processing of Customer Personal Data. Leanpath shall comply with the foregoing by: (i) complying with Section 3.5 (Audits); (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing sub-sections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance at Customer's expense.

3.8 Deletion on Termination. Upon Customer’s request following termination or expiry of the Agreement, Leanpath shall return or delete all Customer Personal Data in its possession or control (except to the extent Leanpath is required to retain any Customer Personal Data under applicable law, in which case Leanpath shall isolate and protect such data from any further processing until it can be lawfully deleted).

4. International Transfers; CCPA Compliance

4.1 Processing Locations. Leanpath may transfer and Process Customer Personal Data in the United States and anywhere else in the world where Leanpath or Subprocessors maintain data processing operations. Leanpath shall ensure that Customer Personal Data is adequately protected in accordance with the requirements of Applicable Data Protection Law and this DPA.

4.2 Restricted Transfers. Where the transfer of Customer Personal Data from Customer to Leanpath is a Restricted Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses, which shall be deemed incorporated into and form an integral part of this DPA in accordance **with Annex B.**

4.3 Alternative Transfer Mechanism. To the extent that Leanpath adopts an alternative data transfer mechanism (including, but not limited to, any new version of or successor to the Standard Contractual Clauses or participation in the EU-U.S. Data Privacy Framework) ("**Alternative Transfer Mechanism**"), such Alternative Transfer Mechanism shall automatically apply instead of the Standard Contractual Clauses described in this DPA, but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Law and extends to territories to which Customer Personal Data is transferred.

4.4CCPA Compliance. To the extent that Leanpath's Processing of Customer Personal Data is subject to the CCPA, this Section 4.4 will also apply. Customer discloses or otherwise makes available Customer Personal Data to Leanpath for the Permitted Purposes. Leanpath shall: (a) comply with its applicable obligations under the CCPA; (b) provide the same level of protection as required under the CCPA; (c) notify Customer if it can no longer meet its obligations under the CCPA; (d) not "sell" or "share" (as such terms are defined by the CCPA) Customer Personal Data; (e) not retain, use, or disclose Customer Personal Data for any purpose (including any commercial purpose) other than the Permitted Purposes or as otherwise permitted under the CCPA; (f) unless otherwise permitted by the CCPA, not retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and Leanpath; and (g) unless otherwise permitted by the CCPA, not combine Customer Personal Data with personal data that Leanpath (i) receives from, or on behalf of, another person, or (ii) collects from its own, independent consumer interaction. Leanpath will permit Customer, upon reasonable request, to take reasonable and appropriate steps to ensure that Leanpath Processes Customer Personal Data in a manner consistent with the obligations applicable to a "Business" under the CCPA by requesting that Leanpath attest to its compliance with this Section 4.4. Following any such request, Leanpath will promptly provide that attestation or notice about why it cannot provide it. If Customer reasonably believes that Leanpath is engaged in unauthorized Processing of Customer Personal Data that is subject to this Section 4.4, Customer will immediately notify Leanpath of such belief, and the parties will work together in good faith to remediate the allegedly violative Processing activities, if necessary.

5. General

5.1 Governing law. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law.

5.2 Modifications. This DPA may not be modified except by a subsequent written instrument signed by both parties. If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

5.3 Survival. The obligations placed upon the parties under this DPA shall survive so long as Leanpath and its Subprocessors processes Customer Personal Data on Customer's behalf.

5.4 Authorized Affiliates. Leanpath's obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions: (a) Customer is solely responsible for communicating any processing instructions on behalf of its Authorized Affiliates; (b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations under this DPA; and (c) if an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against Leanpath ("**Authorized Affiliate Claim**"), Customer must bring such Authorized Affiliate Claim directly against Leanpath on behalf of such Authorized Affiliate, unless Applicable Data Protection Laws require the Authorized Affiliate be a party to such claim, and all Authorized Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set forth in the Agreement, including any aggregate limitation of liability.

5.5 Limitation of Liability. The total and combined liability of each of the parties (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this DPA (including the Standard Contractual Clauses), whether in contract, tort (including negligence), or any other theory of liability, shall be subject to the exclusions and limitations of liability set forth in the Agreement.

5.6 Third Party Rights. In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a third party controller), but without prejudice to the rights or remedies available to data subjects under Applicable Data Protection Law or the Standard Contractual Clauses.

ANNEX A – SCOPE AND DETAILS OF PROCESSING

ANNEX 1(A): LIST OF PARTIES

Data exporter:	*Name of data exporter:*	The entity referred to as "Customer" in the Agreement
	Contact person's details:	If a Customer has signed an Order Form, the contact person's details are those set forth therein; if not, the Customer's administrative users shall be deemed the contact(s).
	Activities relevant to data transfer:	See Annex 1.B below
	Signature and date:	Execution of the Agreement shall be deemed valid execution of the DPA (including the SCCs)
	Role (controller/processor):	Controller (for Module 2) or processor (for Module 3)
Data importer:	*Name of the data importer:*	Leanpath, Inc.
	Contact person's details:	Marc Demarest, VP Corporate Development, dpo@leanpath.com
	Activities relevant to data transfer:	See Annex 1.B below

	Signature and date:	Execution of the Agreement shall be deemed valid execution of the DPA (including the SCCs)
	Role (controller/processor):	Processor

ANNEX 1(B): DESCRIPTION OF THE TRANSFER AND PROCESSING

Categories of data subjects:	Authorized users of the Services, who are employees, agents or contractors of Customer and its Affiliates.
Categories of personal data:	Name and work email address of authorized users (account data). The Services also process photographs of food waste in waste receptacles; camera fields of view are configured to capture waste receptacles and their contents, images are not intended to capture individuals, and incidental capture of individuals is minimized. Waste-tracking events are not attributed by Leanpath to identified individuals.
Sensitive data (if applicable):	None. The Services are not intended to process special categories of personal data, and do not include biometric identification or categorisation, emotion recognition, or audio recording functionality.
Frequency of the transfer:	Continuous or one-off depending on the nature of the Services being provided by Leanpath.
Nature, subject matter and duration of processing:	The nature of the processing is the provision of the Services as further described in the Agreement, and the subject matter is Customer Personal Data. The processing duration is the period for which Leanpath processes Customer Personal Data as determined by the Customer through its processing instructions.
Purpose of processing:	Leanpath shall process Customer Personal Data for the Permitted Purposes, as described in the Agreement and this DPA.
Retention period:	Leanpath will retain Customer Personal Data as instructed by Customer and in accordance with the Agreement, including this DPA.

ANNEX 1(C): COMPETENT SUPERVISORY AUTHORITY

Competent supervisory authority	The data exporter's competent supervisory authority shall be determined in accordance with the GDPR.

ANNEX B – STANDARD CONTRACTUAL CLAUSES (MODULES 2 AND 3)

1.1 To the extent the Standard Contractual Clauses are deemed incorporated into and form an integral part of the DPA pursuant to Section 4.2 of the DPA, they shall apply as follows:

(a) In relation to transfers of Customer Personal Data protected by the GDPR, the SCCs shall apply as follows:

(1) the Module Two terms shall apply where Customer is the controller of Customer Personal Data and the Module Three terms shall apply where Customer is a processor of Customer Personal Data;

(2) in Clause 7, the optional docking clause shall apply and Affiliates may accede to the SCCs subject to mutual agreement of the parties;

(3) in Clause 9, option 2 ("general authorization") is selected and the process and time period for prior notice of Sub-processor changes is set out in Section 3.6 of the DPA;

(4) in Clause 11, the optional language shall not apply;

(5) in Clause 17, option 1 shall apply and the SCCs will be governed by the laws of the Republic of Ireland;

(6) in Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland;

(7) Annex I shall be deemed completed with the information set out in Annex A of the DPA;

(8) Annex II shall be deemed completed with the Security Measures (as described in Section 3.2 of the DPA).

(b) In relation to transfers of Customer Personal Data protected by the UK GDPR, the SCCs as implemented by Section 1.1(a) above shall apply with the following modifications:

(1) the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of the DPA;

(2) Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in the DPA (including its Annexes) and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "importer"; and

(3) any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with section 10 and section 11 of the UK Addendum.

(c) In relation to transfers of Customer Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented by Section 1.1(a) above shall apply with the following modifications:

(1) references to “Regulation (EU) 2016/679” and specific articles therein shall be interpreted as references to the Swiss Data Protection Act and the equivalent articles or sections therein;

(2) references to “EU”, “Union”, “Member State” and “Member State law” shall be replaced with references to “Switzerland” and “Swiss law” and references to the “competent supervisory authority” and “competent courts” shall be replaced with references to the “Swiss Federal Data Protection Information Commissioner” and “competent Swiss courts”; and

(3) the SCCs shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts.

ANNEX C – SECURITY MEASURES

Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

Overview

This annex provides an overall listing of the controls in place at Leanpath to maintain the security of our office and data. These controls form the backbone of our SOC 2 processes. Leanpath is not currently SOC 2 certified, but is working towards that goal in 2026.

Management

Leanpath management is ultimately responsible for overseeing these controls. On a semi-annual basis, each control owner is required to review the controls under their jurisdiction. Management observes the controls in action over the course of the year to ensure functionality and to recommend changes where needed.

Definitions

1. **Company** - Company is defined as **Leanpath**, Inc.
2. **Client** - Client is defined as any user of **Leanpath** systems.

Integrity and Ethical Values

Control Description
The Company's views on personal and corporate integrity and ethical values, along with guidelines for employee conduct are contained within the Code of Conduct. The Code of Conduct provides a framework for how employees conduct business and perform their duties.
The Company maintains a Contractor Agreement, which outlines the Company's associated standards of conduct. Third-party contractors working on behalf of the Company are required to read, accept, and abide by the Agreement before commencing work.
Background checks are performed on all new employees. The results are reviewed by HR for appropriateness and appropriate action is taken, as deemed necessary.

According to the Code of Conduct, Company personnel witnessing any improper behavior should report such incidents promptly to management and/or HR.
On an annual basis, all relevant employees are subject to a formal performance review to assess the employee's performance in their current roles and to identify opportunities for growth and job performance improvement.
The Code of Conduct reiterates that employees who violate company policies are subject to appropriate disciplinary action up to and including termination.

Board Oversight and Development of Controls

Control Description
The Company is managed by a Board composed of key investors who are independent of day-to-day management of the Company and the founders/executives. The Board is governed by a charter, meets in executive session on a quarterly basis, and retains full and free access to officers, employees, and the books and records of the Company.
The Board and its committees have authority to hire independent legal, financial, or other advisors as deemed necessary or appropriate in the discharge of their duties, including oversight of the development and performance of internal control.
Quarterly, the Board meets with members of executive management to discuss operational and financial results and significant matters, risks, and issues facing the Company.

Management Reporting Lines & Responsibility Over Objectives

Control Description

HR maintains formal organizational charts to clearly identify positions of authority and the lines of communication and escalation.
Employee duties and responsibilities are defined and communicated through job descriptions and policies and procedures. Job descriptions exist for common positions and are periodically reviewed by HR and management for accuracy and updated as needed.
The Company maintains a compliance policy which outlines management's responsibility regarding internal controls, frameworks, audit observations (from internal and external sources), and remediation of findings. The policy is reviewed and approved on an annual basis.
The responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving relevant system controls is assigned to appropriate personnel with authority to perform their related duties.
The Company maintains a third-party (vendor) risk management policy, which outlines the policies, procedures, and responsibilities associated with onboarding new vendors and monitoring existing vendors who will have access to Company's customers' personal information. The policy is reviewed and approved by a member of InfoSec on an annual basis.

Employee Recruitment, Retention, and Training

Control Description
Internal policy and procedure documents relating to security and availability are maintained and made available on the Company's site. The policies are reviewed and approved by a member of IT management on an annual basis.
Prior to fulfilling positions, management evaluates a candidate's abilities and background (experience, education, etc.) to meet the requirements of the formal job description.

IT provides company-wide security awareness training to all new employees upon hire, and to all company personnel at least once per calendar year.
Company personnel are instructed to notify IT immediately of any abnormal system behavior or suspicion of a threat.
The Company provides on-the-job training and/or external training of new hires and/or existing employees, as deemed necessary, to empower them with the skills needed to carry out job responsibilities.

Vendor Management & Risk Assessment

Control Description
Before engaging relevant vendors, the Company requests and reviews supporting documentation (e.g., business licenses, industry standard assurance/attestation reports, questionnaires). Entities found to be non-compliant with security or availability requirements are refused.
Formal agreements are in place with relevant vendors, establishing commitments, product specifications, roles, responsibilities, and control requirements. Agreements require vendors to notify Company personnel of security incidents involving PRM data.
The Company evaluates relevant service providers (e.g., colocation facility, cloud providers) annually in accordance with its vendor management process. Documentation such as SOC 2 reports are obtained and assessed to identify new risks.
The Executive Team maintains an annual and three year strategic plan and meets at least quarterly to monitor progress against objectives and discuss business risks.

A Security Council, consisting of IT Operations, Development, Dev/Ops, and Security teams, meets regularly to align security initiatives with operational risks.
At least annually, the Company performs a formal risk assessment, which includes the identification of internal and external threats and the determination of appropriate risk mitigation strategies. This will be completed as part of our on-going SOC 2 process.

Protection of Information Assets

Control Description
Firewalls are implemented at external points of connectivity and network segment boundaries (DMZ, internal) and are configured to be restrictive by default.
Traffic flowing to Leanpath passes through a web application firewall (WAF) designed to inspect for malicious content and prevent denial-of-service attacks.
Customers do not have direct access to the Leanpath database. All data access is provided through Leanpath Online which provides appropriate RBAC to segment access to customer data.
Multi-factor authentication (MFA) is required for access to all corporate accounts. Users must also authenticate at the system or device layer using a separate username and password.
Encryption at Rest: The Leanpath database and file backups are encrypted at rest using full-disk encryption.
Encryption in Transit: External access to Leanpath Online is restricted through a minimum of TLS 1.2 encryption throughout customer sessions.

Endpoint Security: Software is implemented exclusively in Google Cloud Platform and leverages all available security controls including Google's minimized container os to ensure security.

Incident and Change Management

Control Description
An Information Security and Incident Management Policy defines protocols for identifying, investigating, and mitigating security incidents. In the event of an incident, a Security Incident Response Team is activated.
Tabletop simulations are performed periodically to test the Incident Response Plan.
Change Management: Separate development, test, and production environments exist. Application changes are tested by QA and approved before implementation.
Patch Management: IT monitors the availability of patches daily. Patches are applied in a timely manner, starting with non-production environments to assess for service disruptions.
Disaster Recovery: Leanpath utilizes geographically distinct colocation facilities and mirrors production technology to permit resumption of operations in the event of a disaster.
Backups: Incremental or full backups of Leanpath data and configurations are generated daily. The ability to restore database data is tested quarterly.

ANNEX D – SUBPROCESSOR LIST

Third-party Subprocessors

Leanpath's list of subprocessors is always available, in up-to-date form, at:

https://www.leanpath.com/subprocessors/

Leanpath Affiliates

The following affiliates of Leanpath may function as Subprocessors to provide technical and operational support for the Leanpath Services.

Affiliate Name	Purpose	Entity Country
Leanpath Ltd	Oversee Leanpath's operations in Europe, the Middle East and Africa	United Kingdom
Leanpath Pte. LTD.	Oversee Leanpath's operations in Asia, exclusive of China, Australia and New Zealand	Singapore
Leanpath Australia PTY, Ltd.	Oversee Leanpath's operations in Australia and New Zealand	Australia