Data Processing Agreement

This Data Processing Agreement ("Agreement") is made between Heidi Health Ltd, a company registered in England and Wales under the Companies Act 2006 with company number 15878893 ("**Data Processor**") and Lister House Surgery (C81072) & Lister House Chellaston (Y05286), GP Surgeries in England in Wales which are part of PCCO PCN ("**Company**", "**Data Controller**"), collectively referred to as the "**Parties**".

This Agreement supplements the Terms of Use ("**Principal Agreement**") entered into between the parties and applies to the provision of the Heidi services. For the purposes of the UK Addendum, Lister House Surgery (C81072) & Lister House Chellaston (Y05286) are the Data Exporters and Heidi Health Trading Pty Ltd is the Data Importer.

This Agreement will commence on the date it is executed between the parties and will continue for as long as the Principal Agreement remains in effect, or the Data Processor retains any of the Personal Data in its possession or control (whichever is longer) ("**Term**"). The purpose of this Agreement is to outline the conditions under which the Data Processor is permitted to collect, use, disclose, and store personal data on behalf of the Data Controller in compliance with the UK Data Protection Act 2018 and the General Data Protection Regulation (**GDPR**).

Capitalised terms in this Agreement have the meaning given in the Principal Agreement and as set out below:

"**Personal Data**" is as defined under the GDPR and pertains to any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier.

"**Personal Data Breach**" is defined under the GDPR.

"**UK Addendum**" is the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers approved by the Information Commissioner's Office under section 119A of the Data Protection Act 2018 on 21 March 2022 (version B.1.0), and as updated from time to time.

"**Restricted Transfer**" is the transfer of personal data from the United Kingdom to any other country which is not subject to adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"**Transferred Data**" is any Personal Data Processed by the Data Processor or their Personnel on behalf of the Data Controller in connection with the Principal Agreement (and where the Data Processor is also acting as a controller, any Personal Data they process in connection with the Principal Agreement).

"**Data Protection Laws**" are the laws and regulations applicable to the processing of Personal Data by the parties in connection with the Principal Agreement, including, without limitation, the Data Protection Act 2018.

1. Obligations of both parties

Each party agrees to comply with Data Protection Laws in the processing of Transferred Data.

The Data Controller instructs the Data Processor to process Transferred Data in accordance with the Principal Agreement (including in accordance with Annex 1 to this Agreement).

The Data Processor agrees not to process the Transferred Data other than on the Data Controller's documented instructions.

2. Obligations of the Data Processor

The Data Processor agrees to:

- Only process Transferred Data as specified by the Data Controller and in compliance with GDPR.
- Implement appropriate technical and organizational measures to ensure the security and confidentiality of Personal Data in accordance with Data Protection Laws and as further particularised in Annex 2 of this Agreement. In assessing the appropriate level of security, the Data Processor agrees to take into account the risks that are presented by processing, in particular from a Personal Data Breach.
- Not disclose or transfer Personal Data to third parties without the Data Controller's consent except as required by law.
- Assist the Data Controller in handling any requests from data subjects under the GDPR including access to and correction of Personal Data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the

purposes of the Principal Agreement, and to comply with Data Protection Laws in the context of that individual's duties to the Data Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Sub-Processing

The Data Controller authorises the engagement of Sub-Processors already engaged by the Data Processor at the date of this Agreement that are set out in Annex 3 of this Agreement.

The Data Processor agrees not to appoint (or disclose any Transferred Data to) any additional sub-processors unless required or authorised by the Data Controller in writing.

Where the Data Processor engages a sub-processor to process the Transferred Data, the Data Processor agrees to enter into a written agreement with the sub-processor containing data protection obligations no less protective than those in this Agreement with respect to the Transferred Data (including in relation to Restricted Transfers), and to remain responsible to the Data Controller for the performance of the sub-processor's data protection obligations under such terms.

5. Data Breach Notification

The Data Processor shall notify the Data Controller without undue delay (and in any event, within 24 hours) upon becoming aware of any data breach affecting Personal Data. The notification will include all relevant information about the breach as required by the GDPR. The Data Processor shall cooperate with the Data Controller and take reasonable commercial steps as directed by the Data Controller to assist in the investigation, mitigation, and remediation of each Personal Data Breach.

6. General Terms

Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

a) disclosure is required by law; or

b) the relevant information is already in the public domain.

Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address at such other address as notified from time to time by the Parties changing address.

7. Restricted Transfers

Both parties agree that where the transfer of Transferred Data between the parties is a Restricted Transfer, it will be subject to the UK Addendum (and documents or legislation referred to within it) which shall be deemed to be incorporated into this Agreement; and:

a) the tables in part 1 of the UK Addendum shall be populated with the relevant information set out in the Annexes to this Agreement; and

b) the UK Addendum is considered an appropriate safeguard.

8. Audit and Compliance

The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the GDPR and allow for and contribute to audits conducted by the Data Controller or another auditor mandated by the Data Controller.

The Data Processor shall promptly notify the Company if it receives a request from a Data Subject under the GDPR in respect of Company

Personal Data, and ensure that it does not respond to that request except on the documented instructions of the Company or as required by Data Protection Laws to which the Data Processor is subject, in which case Data Processor shall to the extent permitted by Data Protection Laws inform the Data Controller of that legal requirement before the Data Processor responds to the request

9. Data Protection Impact Assessments and Prior Consultation

The Data Processor agrees to provide the Data Controller with reasonable assistance with any data protection impact assessments, and prior consultations with the Information Commissioner or other competent data privacy authorities, which the Data Processor reasonably considers to be required by article 35 or 26 of the UK GDPR or equivalent provisions of any other Data Protection Laws (to the extent the Data Processor does not otherwise have access to the relevant information and such information is in the Data Controller's control).

10. Term and Termination

This Agreement is effective upon the date of the last signature and continues until terminated by either party with notice. Upon termination, the Data Processor will return or destroy all Transferred Data, unless required to be retained by law.

Each party agrees that a failure or inability to comply with the terms of this Agreement and/or the GDPR or Data Protection Laws constitutes a material breach of the Principal Agreement, In such event, the Data Controller, may, without penalty:

(a) Require that the Data Processor suspends processing of the Transferred Data until such compliance is restored; or

(b) Terminate the Principal Agreement effective immediately on written notice to the Data Processor.

Notwithstanding the termination or expiry of the Principal Agreement, this Agreement will remain in effect until, and will terminate automatically upon, deletion by the Data Processor of all the Transferred Data covered by this Agreement. In the case of such termination, the Data Processor shall provide a prompt pro-rata refund to the Data Controller of all sums paid in advance under the Principal Agreement.

11. Deletion or return of Personal Data

Subject to this clause and subject to any document retention requirements at law, the Data Processor agrees to promptly, and in any event within 10 business days of the date of cessation of any Heidi services involving the processing of Transferred Data ("Cessation Date"), delete and procure the deletion of all copies of that Transferred Data.

The Data Processor agrees to provide written certification to the Data Controller that they have fully complied with this clause within 21 business days of the Cessation Date.

12. Liability

Any exclusion or limitation of the Data Processor's liability in connection with the Principal Agreement does not apply to this Agreement.

Despite anything to the contrary, to the maximum extent permitted by law, the Data Processor is liable for and agrees to indemnify the Data Controller and hold the Data Controller harmless in respect of any liability that the Data Controller may suffer, incur or otherwise become liable for, arising from or in connection with the Data Processor's breach of any provision of this Agreement or any Data Protection Laws.

13. Governing Law and Jurisdiction

This Agreement is governed by the laws of England and Wales.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below:

Signature	**Signature**
Name:	**Name:**
Email:	**Email:**
Date Signed:	**Date Signed:**

ANNEX 1

PART A: DESCRIPTION OF TRANSFER

Description of Service	Heidi processes and transcribes clinical conversations, capturing details like different speakers, medical terminology, and symptomatology. From this, a clinical note is generated. The clinician can also generate clinical documents, such as referral letters and patient explainer documents. These documents will follow templates already defined by Heidi, or the clinician can create their own template. This system is designed to alleviate the administrative burden on healthcare professionals, allowing them to focus more on patient care rather than paperwork. The Heidi Scribe will leverage natural language processing (NLP), speech recognition technology, and machine learning algorithms to understand and interpret complex medical dialogue, identify key health information, and categorise data into the appropriate sections of an EHR.
Personal Data Transferred	● Identity Data including first name, middle name, last name, title, date of birth, gender, phone number, address, relationship status, and family/social history of our client's customers. ● Contact Data including billing addresses, email addresses and telephone numbers (users of the Heidi platform). ● Financial Data including bank account and payment card details (users of the Heidi platform). ● Technical and Usage Data including internet protocol (IP) address, login data, browser session and geo-location data, device and network information, statistics on page views and sessions, acquisition sources, search queries and/or browsing behaviour, information about user access and use of our website, including through the use of Internet cookies, communications with our website, the type of browser used by users, the type of operating system used by users and the domain name of users' Internet service provider (users of the Heidi platform).
Special Categories of Personal Data and criminal convictions and offences	The transferred data may include data relating to: ● Physical or mental health data ● Racial or ethnic origin ● Sexual life and sexual orientation
Relevant Data Subjects	● Users of the Heidi platform (our customers) ● Clients of our customers
Frequency of the transfer	Continuous
Nature of the transfer	As specified in the Principal Agreement, this Agreement, and as instructed by the Data Controller, including without limitation: Collection, organisation, storage (hosting), retrieval, use and other processing of Personal Data by the Data Processor necessary to provide, maintain and improve the Heidi services. Heidi is a healthcare IT system, specifically a cloud-based artificial intelligence medical scribe platform. It is a standalone software that is used to generate comprehensive clinical documentation using a combination of speech-to-text software, note taking and artificial intelligence models. Heidi is accessible via desktop and mobile browser to registered users, with servers and data hosted locally in the UK for all UK users. Heidi works by transcribing speech into text from a healthcare encounter such as conversations between clinicians and patients or by clinicians dictating their clinical findings, impression and/or management plans before, during and after the healthcare encounter. The clinician can also add additional contextual notes about the healthcare encounter which they may not wish to verbalise during the healthcare encounter. The clinician is also able to set and modify various settings within the Heidi platform in order to customise their Heidi experience as well as how their clinical documentation is structured and written. To generate the requested clinical documentation, the transcribed text and contextual notes along with the various user controlled settings are then through an artificial

	intelligence model which then generates the requested clinical documentation based on the data that has been given to the AI model. The comprehensive clinical documentation generated by Heidi can then be copied or integrated into an electronic medical record system or used with other word processing or communication tools to provide other clinicians and/or the patient with relevant information related to the healthcare encounter and the patient's care. The intended use and recommendations for Heidi are as follows: ● Heidi should be used by qualified and registered clinicians to assist them in writing their clinical documentation. ● Heidi should not be used as a clinical decision making tool and is not a substitute for medical assessment. ● Heidi's generated clinical documentation is intended to reduce the amount of time it takes clinicians to complete their medical records; however the clinician is ultimately responsible for their clinical documentation, and must ensure that the content of the notes and documents accurately reflects the healthcare encounter for which the documentation has been generated. Heidi is noted to have the following limitations that users must be aware of: ● Heidi's generated clinical documentation is based on the clarity and quality of the speech & text data that is provided in the healthcare encounter. Users must review all clinical documentation generated to confirm their accuracy before capturing it in their electronic medical records or distributing documentation to other clinicians and/or patients. ● Hardware issues such as poor microphone quality may cause sub-par audio being captured, resulting in an inaccurate text transcript which does not adequately reflect the healthcare encounter information. Users are recommended to test the quality of their microphones prior to and while using Heidi. ● An unstable or slow internet connection may result in delays in information processing and potentially not capturing some or all of the healthcare encounter information. Therefore it is vital that users ensure they have a stable and fast internet connection when using Heidi. ● Heidi's AI models occasionally make mistakes which may not accurately reflect the information discussed in the healthcare encounter. Users must ensure they have reviewed all clinical documentation generated by Heidi to confirm their accuracy before importing it in their electronic medical records or distributing documentation to other clinicians and/or patients.
Purpose of processing	The primary purposes include improving clinical documentation, aiding healthcare professionals in note-taking, and generating consult summaries. Our technology enables clinicians to focus on patients during the consultation, contributing to improved patient care. It also acts as a valuable tool for medical practitioners, saving them hours of administrative time per week. To ensure the highest level of accuracy and reliability in our models, we implement rigorous processes for eliminating biases from our outputs. This involves continuous monitoring and evaluation of our algorithms to detect and mitigate any potential biases that may arise. Our approach includes diverse and representative data sets, regular audits, and feedback loops from clinicians to refine and enhance the system. Furthermore, we employ robust governance principles to maintain the integrity and trustworthiness of our technology. This includes sophisticated encryption protocols, de-identification of data, real-time safety monitoring, regular system audits, and penetration tests. By upholding these governance standards, we ensure that our technology not only meets but exceeds industry expectations, providing a safe and effective tool for healthcare professionals.

Duration of the Processing	The scope includes recording, transcribing, and generating summaries of clinical consultations. It encompasses the entire duration of the consultation, covering various medical details, additional clinician notes, and dynamic command line inputs that are inputted by the clinician. This processing will occur every time a clinician performs a session on Heidi - in other words, every time they click 'start transcribing'. This data will cover both data from the patient themselves (though it is de-identified) and the clinician too - such as their templates, note-taking style, clinician type, email address etc. No identifiable recordings are stored, or will be accessible. Clinicians retain ownership of all transcripts, clinical notes, and clinical documents and can decide how long this data is stored. Additionally, the patient information contained in these transcripts and clinical notes/documents will only be accessed externally for the purpose of troubleshooting with the express permission of clinicians.

PART B: INFORMATION REQUIRED FOR THE UK ADDENDUM

Information required for Table 2 of the UK Addendum						
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	✗	N/A	N/A			
2	✓	Incorporated	Not incorporated	General authorisation	28 days	
3	✗	N/A	N/A	N/A	N/A	
4	✗	N/A	N/A			N/A

Information required for Table 4 of the UK Addendum	
Ending this Addendum when the Approved UK Addendum changes	Which Parties may end this Addendum as set out in Section 19 of Part 2 of the UK Addendum: ☐ Importer ☐ Exporter ☒ Neither Party

ANNEX 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

TECHNICAL AND ORGANISATIONAL MEASURES	DETAILS
Designated data protection officer	● Yassin Omar - Data Protection Officer
Security certifications	● ISO27001:2022, Cyber Essentials, SOC2
Internal policies e.g. security policy, data retention and deletion policies	**Heidi's Data Management Policy** ensures that information is classified, protected, retained and securely disposed of in accordance with its importance to the organization. Data is classified based on legal requirements, sensitivity, and business criticality, and is protected accordingly. Key data categories include customer data, PII, financial data, and strategic plans, with access restricted to necessary personnel following the principle of least privilege. Confidential data must be encrypted with TLS v1.2 in transit and AES-256 at rest, with strict access controls and documented approvals for non-pre approved roles. Data retention periods are determined by data owners in consultation with legal counsel, and data is securely deleted when no longer needed. An annual review of data retention requirements is conducted, and compliance is measured through reports and audits. To protect the company's information, employees, partners, and assets from illegal or damaging actions. **Heidi's Information Security Policy** mandates the use of company systems solely for business purposes, emphasizing a collective effort for security by all employees, contractors, and third-party personnel. Key elements include the prohibition of USB devices, stringent remote access and mobile device policies, and adherence to acceptable use standards. Incident reporting, clean desk protocols, and whistleblower protection are integral to the policy. Compliance is enforced through regular audits, with violations subject to disciplinary actions, including termination.
Pseudonymisation and encryption of personal data	● At Heidi Health, all privacy data is encrypted in transit using TLS 1.2 or higher and at rest with AES-256. We manage encryption keys via AWS Key Management Service to ensure secure key lifecycle management. For processing such data, we run through de-identification and pseudonymization models to ensure no occurrence of re-identification.
Product security features	Our solution supports federated authentication, utilising Kinde as our third-party authentication provider which offers a robust suite of authentication capabilities designed to ensure secure and versatile user access management. The key features include: ● Single Sign-On (SSO): Enables users to access multiple services with a single set of credentials, improving user experience and security. ● Multi-Factor Authentication (MFA): Enhances security by requiring multiple forms of verification from users,

	significantly reducing the risk of unauthorised access. (launching August 2024) ● Support for Multiple Protocols: Kinde supports a range of authentication protocols, including SAML, OAuth2, OpenID Connect, and Kerberos. This compatibility allows for seamless integration with your existing identity providers and ensures that our solution can accommodate your IT environments
Network security	Heidi Health Trading Pty Ltd provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and reportable user provisioning and deprovisioning processes. Heidi also employs technical controls to prevent unauthorized access to our systems. Heidi manages its own cloud infrastructure on AWS including all network, router, firewall, server and storage equipment. This shared infrastructure is used to provide dedicated virtual machines to customers with enforced segregation between all servers. **Data Isolation:** ● We utilise AWS's multi-tenant architecture, which provides logical isolation of data using unique identifier. **Access Control:** ● Each user is assigned unique credentials and specific roles that determine their access rights. **Encryption:** ● All data is encrypted at rest using AWS-managed keys, and in transit using TLS protocols. ● We utilise AWS Key Management Service (KMS) for key management, ensuring that encryption keys are properly secured and managed. **Network Security:** ● Our AWS Virtual Private Cloud (VPC) configuration, along with security groups and network ACLs, ensures that customer-specific data is isolated from other network traffic. ● We use AWS WAF and Network Firewall to provide additional protection against unauthorised access attempts. **Intrusion Detection:** ● AWS security services for automated monitoring and detection ● Dedicated team for 24/7 intrusion monitoring and response. ● AWS Network Firewall as our stateful packet inspection (SPI) firewall is being utilised to provide advanced internal network protection. Heidi Health Trading Pty Ltd maintains a robust patch management process to ensure that all systems are up to date and secure. This process includes: **Identification:** ● Regular vulnerability scans and updates from software vendors are used to identify available patches and updates. ● We utilise MDM for workstation patching and monitoring

	Application: ● Patches are applied using automation, wherever possible. ● In a complex situation, patches are applied in a controlled manner, starting with testing in a non-production environment. ● Upon successful testing, patches are scheduled for deployment in the production environment during predefined maintenance windows to minimise disruptions. **Verification:** ● After applying patches, systems are monitored to ensure they are functioning correctly and securely. ● Logs are reviewed to confirm that patches have been applied successfully and that no issues have arisen post-deployment. Heidi Health Trading Pty Ltd maintains comprehensive audit logs to ensure accountability and traceability of all system activities. The logging process includes: **Types of Logs:** ● Logs are maintained for user access, system changes, data access, and security events. ● Specific logs include authentication attempts, changes to user permissions, and access to sensitive data. **Retention Periods:** ● Logs are retained for a minimum of one year to comply with regulatory and operational requirements. ● Critical logs, such as those related to security incidents, are retained for longer periods as needed. **Log Review Procedures:** ● Logs are reviewed regularly by the compliance and security teams to identify and address any anomalies or potential security threats. ● Automated tools are used to assist in the analysis and alerting of suspicious activities.
Physical security and disaster recovery	**Physical Security:** Heidi Health Trading Pty Ltd's production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Heidi Health Trading Pty Ltd reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis. To prevent unauthorized physical access or damage to the organization's information and processing facilities, Heidi employs strict physical security controls; these controls apply to all employees and external parties with physical access to company-owned or leased facilities. Physical security measures include secure construction materials, restricted access to secure areas, and appropriate entry controls. Secure areas are protected by FOB keys, cameras, and intrusion detection systems, with access logged and reviewed. Environmental protections, such as fire-suppression systems and climate control, are in place, and maintenance of equipment follows manufacturer recommendations. Visitors and third-parties are escorted in secure areas, and their access is logged and monitored. Delivery and loading areas are controlled to prevent unauthorized access. Suppliers and vendors must comply with the company's physical security requirements, assessed during vendor management.

	Exceptions to the policy require approval from the Compliance Lead, and violations may result in disciplinary action. **Disaster Recovery:** To ensure Heidi Health Trading Pty Ltd's can effectively manage and respond to adverse events, a Business Continuity and Disaster Recovery Policy has been employed. This policy outlines Heidi's preparedness and response plan for extended service outages caused by unforeseen events. It covers all business-critical IT systems and employees, outlining specific scenarios and response strategies for various disruptions, including the unavailability of office facilities and service outages. Key procedures include the activation of remote work, communication via Slack and email and maintaining critical services using alternative resources and locations. Key roles, such as the CTO and the executive team, are designated to lead recovery efforts and maintain operational and information security continuity.Continuity strategies rely on vendor-hosted SaaS applications, AWS commitments, and redundant systems. The policy mandates annual disaster recovery tests and emphasizes maintaining both operational and information security continuity.
Human resources security	The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Heidi Health Trading Pty Ltd's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Heidi Health Trading Pty Ltd's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example. Specific control activities that the service organization has implemented in this area are described below: ● Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel. ● Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual. ● Annual security awareness training for all employees, which is enforced and monitored by our Compliance Team. ● A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook. ● Background checks are performed for employees as a component of the hiring process. Heidi Health Trading Pty Ltd employs a structured process for managing user accounts to ensure secure and efficient access to our systems. This process includes: **Provisioning:** ● User accounts are provisioned based on role-based access control (RBAC). Each user is assigned unique credentials and specific roles that determine their access rights.

	● New users must review and acknowledge Heidi Health's policies and complete mandatory security training within 70 days of hire. **De-provisioning:** ● Upon termination of employment, user accounts are deactivated within 72 hours. Compliance and Operations are responsible for ensuring that access to all in-scope systems is revoked promptly. ● A formal offboarding checklist is used to ensure all steps are followed. **Access Reviews:** ● User access and roles are reviewed on a quarterly basis to ensure least privilege access and to make necessary adjustments based on role changes. Multi-Factor Authentication (MFA) Heidi Health mandates the internal use of multi-factor authentication (MFA) for accessing critical systems and sensitive data. The MFA process includes: ● Implementation: MFA is implemented these systems: ○ Internal Users ■ AWS: IAM Identity Center ■ GitHub ■ Google Workspace ■ Slack ■ JumpCloud (MDM) ○ External Users (e.g. Heidi Scribe app users) use 3rd party authentication service where MFA is implemented when required. A mandated solution is currently being developed and will be deployed by August 2024. ● Verification: Internal users must provide a second form of identification, such as a mobile app authentication code, in addition to their password. ● Monitoring: Our monitoring tool, Vanta, monitors MFA compliance and prompts users to update their authentication methods as needed.

ANNEX 3

LIST OF SUB-PROCESSORS

SUB-PROCESSOR	LOCATION	PURPOSE/ SERVICES	WEBSITE & CONTACT DETAILS
Google LLC	EU (Ireland)	Google Workspace: ● Employee email ● Google Drive ● Google Meets	https://workspace.google.com/
AWS	United Kingdom/ EU	Cloud hosting provider	https://aws.amazon.com/
Kinde	EU (Ireland)	User authentication	https://kinde.com/
Stripe	United Kingdom	Payment Processing	https://stripe.com/
Intercom	EU (Ireland)	Customer Support	https://intercom.com
Posthog	EU (Ireland)	Analytics	https://posthog.com/