Data Processing Agreement

This Personal Data Processing Agreement ("Processing Agreement" or "DPA") entered by and between Customer and Service Provider, sets forth the terms and conditions relating to the privacy, confidentiality and security of Personal Data (as defined below) associated with services to be rendered by Service Provider ("we", "our" or "us") to Customer pursuant to the accepted Order Form or Service Provider Agreement (the "Agreement").

If you have questions regarding this Processing Agreement you can send them by email to dpo@wearexams.com.

For the avoidance of doubt, any capitalized terms not defined in this Processing Agreement shall have the meanings set forth for such terms elsewhere in the Agreement.

In consideration of the mutual covenants and agreements in this Processing Agreement, in the Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, Customer and Service Provider agree as follows:

I. DEFINITIONS

1.1. "Applicable Data Protection Laws" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, as well as the CCPA (as defined below) and any other state or national laws or regulation applicable to the Processing of Personal Data under the Agreement.

1.2. "CCPA" or "California Consumer Privacy Act of 2018" means Assembly Bill 375 of the California House of Representatives, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy and approved by the California Governor on June 28, 2018.

1.3. "Customer Security Incident", has the meaning attributed to this term in article 5.4 (Security Incidents and Personal Data Breach Management and notifications) below.

1.4. "Data Controller" or "Controller" means the Customer provided that it determines the purposes and means of the processing of Personal Data in relation and in connection to the Agreement.

1.5. "Data Processor" or "Processor" means the Service which processes Personal Data on behalf of the Data Controller, and in compliance with the terms and conditions provided hereto.

1.6. "Data Subject" means the physical person to whom the Personal Data refers.

1.7. "Data Transfer" means any transfer of personal data from the USA to any third country or international organization.

1.8. "GDPR" means the 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), and its relevant national implementation.

1.9. "Personal Data" means any information relating to an identified or identifiable natural person such as name, last name, email address, postal address, telephone number, date of birth, Social Security number (or its equivalent), driver's license number, account number, credit or debit card number, location data, identification number, any other unique identifier or one or more factors specific to an individual's physical, economic, cultural or social identity or that is defined as "Personal Information," "Personally Identifiable Information," "Personal Data," or any similar designation by Applicable Data Protection Laws, in any form and any media, that Service Provider receives, accesses, collects, processes, generates, compiles or creates in connection with this Processing Agreement and the Agreement.

1.10. "Process" or "Processing" means any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as creation, collection, procuration, obtaining, accession, recording, organisation, storage, adaption or alteration, retrieval, consultation, dissemination or otherwise making available, use, disclosure by transmission, restriction, erasure or destruction.

1.11. "Service Provider" & "Service Provider Group" means Labchanges Unlimited SL. dba WeAreExams and its affiliates and subsidiaries.

1.12. "Subcontractors" has the meaning attributed to it in article 3.1 (*Appointment of Subcontractor*) below.

1.13. "Technical and Organisational Security Measures" means those measures aimed at protecting personal data against unlawful destruction or accidental destruction or loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of Processing.

1.14. "USA", means the United States of America.

II. DATA PROTECTION

2.1. **Compliance with Laws**. Both parties will comply with all requirements of the Applicable Data Protection Laws.

2.2. **Role of the Parties**. This DPA applies when Customer Personal Data is Processed by the Service Provider. The Customer acts as Controller with respect to Customer Personal Data and the Service Provider acts as Processor.

2.3. **Scope of the DPA and Processing Instructions**. The present Processing Agreement sets forth the terms and conditions pursuant to which the Service Provider as Processor will Process Personal Data provided by the Customer as Controller for the purpose of providing the Services included in the Agreement, as well as when performing its obligations under this DPA and the Agreement. Provided that, the Service Provider shall not Process Customer's Personal Data for any other purposes.

It is in any case understood that Service Provider will only Process Personal Data only on the written instructions of Customer, and Service Provider agrees to act in accordance with the instructions of Customer. Service Provider shall inform Customer in writing as soon as is commercially and reasonably practicable if it cannot comply with Customer's instructions. If Service Provider cannot comply with Customer's instructions, Customer can suspend the transfer or disclosure to or access by Service Provider of Personal Data and terminate any further Processing of Personal Data by Service Provider, if doing so is necessary to comply with Applicable Data Protection Laws.

2.4. **Duration**. The present Processing Agreement shall be valid and effective from the date of entry into force of the Agreement until the termination of the Agreement, unless agreed in writing otherwise.

2.5. **Description of the Personal Data Processing by Service Provider.** A list regarding the scope and duration of Processing, categories of Data Subjects, and types of Personal Data Processed, is set out in Exhibit 1 of the Processing Agreement attached hereto.

2.6. **Inquiries on Processing.** Service Provider shall deal promptly and appropriately with any inquiries from Customer relating to the Processing of Personal Data subject to this Processing Agreement or the Agreement.

2.7. **Service Provider Personnel.**

2.7.1. Confidentiality Obligations. Service Provider warrants that except and solely as permitted in the applicable section in the Agreement, Service Provider and its employees, agents, consultants and contractors shall hold in strict confidence (i) the existence and terms of this DPA, the Agreement and any related agreement; (ii) any and all Personal Data (whether in individual or aggregate form and regardless of the media in which it is contained) that may be disclosed at any time to Service Provider or its employees, agents, consultants or contractors by Customer, Customer's Affiliates or their respective employees, agents, consultants or contractors in anticipation of, in connection with or incidental to the performance of services for or on behalf of Customer or Customer's Affiliates; (iii) any and all Personal Data (whether in individual or aggregate form and regardless of the media in which it is contained) that may be Processed at any time by Service Provider or its employees, agents, consultants or contractors in connection with or incidental to the performance of services for or on behalf of Customer or Customer's Affiliates; and (iv) any information derived from the information described in (ii) and (iii) above; ((ii), (iii) and (iv) designate collectively: Personal Data; provided, however, that the Parties agree that any materials or information used in or resulting from any activities that Service Provider is allowed to engage in pursuant to the applicable Section in the Service Provider Agreement shall be deemed to not constitute "Personal Data" even if such information or materials used in such activities might constitute or include "Personal Data" in other contexts).

2.7.2. Limitation of Access. Service Provider shall ensure that Service Provider's access to the Personal Data is limited to those personnel who require such access to perform the Agreement and are obliged to keep the Personal Data confidential, pursuant to the principle of the "need to know".

2.7.3. Supervision and Awareness. Service Provider shall exercise the necessary and appropriate supervision over its relevant employees, contractors, consultants, agents, vendors and partners to maintain appropriate privacy, confidentiality and security of Personal Data. Service Provider shall provide training, as appropriate, regarding the privacy, confidentiality and information security requirements set forth in this Processing Agreement to employees, contractors, consultants, agents, vendors and partners with access to Personal Data.

2.7.4. Data Protection Officer. Members of the Service Provider Group will appoint a Data Protection Officer where such appointment is required by Applicable Data Protection Laws and Regulations. The appointed person may be reached at dpo@wearexams.com.

2.8. **Return and Deletion of Customer Data.** Promptly upon the expiration or earlier termination of the Agreement, or such earlier time as Customer requests, Service Provider shall, at the choice of Customer, securely return to Customer or its designee, or, securely destroy or render unreadable or undecipherable if return is not reasonably feasible or desirable to Customer (which decision shall be based solely on Customer's written statement), each and every original and copy in every media of all Personal Data in Service Provider's possession, custody or control. Service Provider shall comply with all directions provided

by Customer with respect to the return or disposal of all Personal Data unless otherwise required by Applicable Data Protection Laws.

2.9. **Transfer of Personal Data**. By entering into this Data Processing Agreement and the Agreement, Customer hereby authorizes Service Provider to share, transfer, disclose or otherwise provide access to Personal Data to the Subcontractors (as defined below in article 3.1 (*Appointment of Subcontractors*) identified in Exhibit 3. In general terms, the Data Transfers envisaged in Exhibit 3 are made in favor of Subcontractors belonging to the Service Provider Group, and therefore necessary to provide the Services included in the Agreement; or because the relevant Subcontractor provides specific additional services to the Service Provider (e.g. cloud provider).

In any case, Service Provider takes reasonable and appropriate steps to ensure that the relevant Subcontractor effectively processes the Personal Data transferred in a manner consistent with the Applicable Data Protection Law and requires the relevant Subcontractor to notify Service Provider if it can no longer meet its obligation to provide the same level of protection as is required by the Applicable Data Protection Law.

For the sake of clarity, it is in any case understood that Service Provider before performing any Data Transfer will comply with the Applicable Data Protection Laws, identifying the most appropriate legal requirement.

III. SUBCONTRACTORS

3.1. **Appointment of Subcontractors.** Customer consents to Service Provider subcontracting its obligations under this Processing Agreement and the Agreement to affiliated companies or third-party processors to perform and fulfil the Service Provider's commitments and obligations under this Processing Agreement and the Agreement ("Subcontractors"). Service Provider confirms that it has entered or (as the case may be) will enter with (each of) the third-party processor(s) into a written agreement incorporating terms which are substantially similar to those set out in this Processing Agreement as between Customer and Service Provider and, such third-party processor has given sufficient guarantees that they will implement measures to ensure that Processing the Personal Data it carries out will meet the requirements of the Applicable Data Protection Law and protect the rights of data subjects.

3.2. **Subcontractors List.** As of today, an updated list of authorized Subcontractors is provided in Exhibit 3. It is in any case understood that when applicable, Service Provider shall maintain an up-to-date list of Subcontractors, specifying (i) their name and details, as well as (ii) the nature of the tasks entrusted to them, and (iii) the location of the Processing.

3.3. **New Subcontractors.** Service Provider shall give Customer prior written notice of the appointment of any new Subcontractor, including full details of the Processing to be undertaken by the Subcontractor.

3.4. **Objection Rights.** To avoid doubt, it shall be reasonable for Customer to withhold or deny such consent if Customer has reasonable doubts that a Subcontractor is able to perform and fulfil the Service Provider's commitments and obligations under this DPA. The objection must be based on reasonable grounds (e.g. if Customer proves that significant risks for the protection of its Personal Data exist at the subcontractor).

3.5. **Agreements with Subcontractors.** Customer hereby authorizes Service Provider, to agree in the name and on behalf of Customer with a Subcontractor which Processes or uses Personal Data of Customer outside the USA, to enter into any relevant agreement or into any other legal document (e.g. a data processing agreement pursuant GDPR, or CCPA, or any USA local, state, federal law, data transfer agreement pursuant to article GDPR, etc.) necessary to comply with the Applicable Data Protection Law.

3.6. **Liability.** Service Provider shall remain fully liable for all acts or omissions of any Subcontractors appointed by it pursuant to this section.

IV. RIGHTS OF DATA SUBJECTS AND ASSISTANCE

4.1. **Data Subject Request.** To the extent permitted by law, Service Provider will inform Customer as soon as is commercially and reasonably practicable, in writing of any requests with respect to Personal Data received from Customer's customers, consumers, employees or others ("Data Subject") to exercise the following Data Subject rights: access, rectification, restriction of Processing, erasure ("Right to be Forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making. Service Provider shall assist Customer, at Customer's cost (Customer will be informed of costs before they are incurred and shall be approved by the Customer in advance), in responding to any request from a data subject and in ensuring compliance with its obligations under Applicable Data Protection Laws with respect to security, breach notifications, impact assessments and consultation with supervisory authorities or

regulators, Service Provider shall cooperate with Customer if any individual seeks to exercise his/her rights (right to rectification, right to object, right to erasure, right to restrict Processing, right to data portability).

V. SECURITY

5.1. **Data Property.** All Personal Data shall at all times be and remain the sole property of Customer, and Service Provider shall not have or obtain any rights therein.

5.2. **Technical and Organizational Measures.** Service Provider shall take appropriate Technical and Organizational Security Measures against unauthorized or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, the Personal Data provided by Customer appropriate to the harm that might result from the unauthorized or unlawful Processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of the technological development and the cost of implementing any measures where appropriate, for example, pseudonymisation and encryption of Personal Data.
In this respect, Customer agrees and acknowledges as appropriate the Technical and Organizational Measures provided in Exhibit 2 attached hereto.

5.3. **Controls for the Protection of Customer Data.** Service Provider shall develop, maintain and implement a comprehensive written information security program that includes appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Personal Data, (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Data, and (iii) protect against any Information Security Incident. Service Provider regularly monitors compliance with these measures.

5.4. **Security Incident and Personal Data Breach Management and notifications.** Service Provider will notify Customer without undue delay in writing after becoming aware of any violation of any provision of this Processing Agreement or any actual or suspected theft or unauthorized Processing, loss, use, disclosure or acquisition of, or access to, any Personal Data (hereinafter "Customer Security Incident") of which Service Provider becomes aware and which may require a notification to be made to the competent Supervisory Authority or Data Subject under Applicable Data Protection Law or which Service Provider is required to notify to Customer under Applicable Data Protection Law. Service Provider shall provide commercially reasonable cooperation and assistance in identifying the cause of such Customer Security Incident and take commercially reasonable steps to remediate the cause to the extent the remediation is within Service Provider's control. The obligations herein shall not apply to incidents that are caused by Customer, Authorized Users, any Non Service Provider-related Service or Force Majeure.

5.5. **Audits.** Service Provider shall maintain complete and accurate records and information to demonstrate its compliance with its obligations under this Agreement and also for audits conducted by or on behalf of Customer. Customer may contact Service Provider in accordance with the "Notice" Section of the Agreement to request an on-site audit of Service Provider' procedures relevant to the protection of Personal Data, but only to the extent required under applicable Data Protection Law. Before the commencement of any such onsite audit, Customer and Service Provider shall mutually agree in writing upon the scope, timing, and duration of the audit. Customer will restrict its audit activity to the departments and locations agreed upon in writing. A schedule of meetings and audit activities will be detailed in writing with the nominated single point of contact for the audit and the identified business areas. Customer must provide Service Provider with a notice of fifteen (15) days. Customer can perform a new audit within three years following the former scheduled audit. Customer is responsible for the cost and expenses of the audit. Customer must sign a NDA before each audit. Customer's audit team is legally bound by Service Provider's NDA which prohibits Customer from knowingly and recklessly disclose any confidential information pertaining to the audit or to the Service Provider or to Service Provider Group. Customer shall promptly notify Service Provider with information regarding any noncompliance discovered during the course of an audit, and Service Provider shall use commercially reasonable efforts to address any confirmed non-compliance.

5.6. **Judicial Access.** Subject to applicable law, Service Provider shall notify Customer as soon as is commercially and reasonably practicable in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data. Customer shall have the right to defend such action in lieu of and behalf of Service Provider. Customer may, if it so chooses, seek a protective order. Service Provider shall reasonably cooperate with Customer in such defense.

VI. LIMITATION OF LIABILITIES

For the purposes of the Agreement, Customer represents and warrants that all the Personal Data made available to, communicated to, accessed by the Service Provider, have been previously Processed by Customer in full compliance with the Applicable Data Protection Laws.

Consequently, Customer will hold harmless Service Provider from any claims, request of indemnifications or compensation of damages regarding the Processing operations previously performed by Customer on the Personal Data that will then be Processed by Service Provider for the purpose of the Agreement.

VII. SEVERANCE

Should any provision of this Processing Agreement be invalid or unenforceable, then the remainder of this Processing Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

VIII. AMENDMENT(S) OF THE DPA

This Processing Agreement may be amended in the light of developments, laws and regulations, of the Applicable Data Protection Law as they exist to date and as they could be amended and, to any other rule, law, recommendation, regulation of the relevant data protection authority or any competent European or USA supervisory authority.

Any other change or amendment not connected or related to the necessity to comply to any change in laws or regulations, shall be agreed in writing between Customer and Service Provider.

IX. APPLICABLE LAWS AND JURISDICTIONS

This Data Processing Agreement shall be regulated and interpreted by the same law regulating the Agreement. The court identified within the Agreement shall have the exclusive jurisdiction over any disputes or claims related or connected to this Processing Agreement.

EXHIBIT 1

Details of the Processing

The details of the Processing by the Service Provider under this Agreement are as follows:

Scope of Processing

Service Provider will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Schedule detailing the subscribed Services. For further information regarding the Processing related to a particular Service, please see the online Privacy Policy (User Policy) applicable to the Service.

Nature and Purpose of Processing

Service Provider will only Process Personal Data to perform the Services pursuant to the Agreement, and as further instructed by Customer in its use of the Services.

Duration of Processing

Service Provider will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing or legally required.

Types of Personal Data Processed: Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer and the setup of each assessment in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and Last name
- Email
- Connection data (login)
- Official ID document
- Personal life data. Birthdate, ID number, Gender and other information connected to the official ID OCR
- Frames of video stream with individual participant
- Assessment metadata
- Assessment feedback data
- Payment data
- Localisation data

Categories of data subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customer itself (e.g. organization data, invoicing data, etc.);
- Individuals or organizations in a relationship with Customer (roles within the organization, etc.).

EXHIBIT 2

Description of the technical and organisational security measures implemented

1. **Application Level**.
   - **1.1.** Regularly scheduled security audits, both internal and external
   - **1.2.** External security audits and vulnerability scans performed by QoBox. The results of these audits are available to Customer on request.
   - **1.3.** Use of Secure Sockets Layer (SSL/TLS)
   - **1.4.** Strong cryptographic standards, including advanced password hashing techniques
   - **1.5.** Strong incident management, change control and asset management policies.
   - **1.6.** Access to applications is restricted only to whitelisted IP addresses (if requested by Customer): customers can choose to have their data and application be accessible only from IP addresses that they specify during the setup.
   - **1.7.** Password Authentication for all users: only Authorised Users have access to the application. In addition, there are different levels of authorisation. For example, users not authorised for administrator access cannot add or remove users.
   - **1.8.** Support for different roles and permissions for each role. Only roles or user authorised to access a protected resource can do so.
   - **1.9.** All User activity is logged: In the event of unauthorised activity, we can review the log to investigate the events and provide the log to Customer if requested.
   - **1.10.** Use one-time password authentication for critical systems. AWS, Gmail, Github, applications are all secured with the second layer of OTP system where the user is required to input username and password as well as the code shown on the authenticator application.
   - **1.11.** If identity validation is selected for a specific assessment, the original and processed ID and related data will remain in secured encrypted S3 servers. There are different regulatory policies for how long that data and results from that data need to be kept for the legitimacy of the assessment. Part or all of that data can be programmatically removed based on Customer/regional specific requirements.
   - **1.12.** Support for granular exam settings. Providing full control to the customer on the level of data requests and requirements to fully utilize the services (eg. recording, face recognition, id validation, etc)
   - **1.13.** The optional face detection and AI runs as a Javascript library embedded in a web page executed in the browser of the host device. It carries an instant and volatile processing of personal data, while scanning the images read by the video stream (for example a camera) provided by the browser API. Each image of the video stream remains in the volatile memory of the device, smartphone, tablet, PC etc., accessible from the software within the browser sandbox, only for the time strictly necessary for processing the result, estimated at about 100ms, after which it is overwritten by the next image. The last frame of the stream is destroyed as soon as it is processed.

2. **Disaster Recovery**.
   - **2.1.** Full Data backups every 24 hours.
   - **2.2.** All servers are secured and distributed behind load balancers. Service Provider is able to detect the traffic and do maintenance in the servers without affecting Customer service.
   - **2.3.** Backups are kept at a remote location on S3.
   - **2.4.** Thirty (7) days of data backups retained.
   - **2.5.** In case of disaster, Customer can be set up immediately using the latest available backup.

3. **Hosting.**
   - **3.1.** Servers are hosted in several state-of-the-art Data centres certified SSAE and ISO 27001.
   - **3.2.** Equipment is behind multiple layers of physical security and supported by redundant power and HSRP/VRRP Internet access. The Data Centre is located at heavily protected buildings where the security personnel are on guard 24x7. Other security features include biometric fingerprint readers on door locks, strategically placed cameras and motion detection, and doors equipped with alarm system.

3.3. Remote access to Service Provider network within the AWS Data centre is only allowed to authorised employees over a secure VPN connection.

4. Office Network.

4.1. The office network is protected by Google Workspace Firewall. Only authorised access is permitted.

4.2. Documents are shared only among authorised employees. Documents on the office network are encrypted in the cloud not public and can only be accessed by authorised employees or consultants.

4.3. Access to the building is not granted unless the visitor is pre-authorised or a current employee allows access.

5. Updates.

Service Provider is constantly improving its Services and platform. Service Provider's latest Technical and Organisational Security Measures updates are available on request. Customer may write to Service Provider using the following email address support@wearexams.com.

EXHIBIT3

List of Subcontractors

Infrastructure Subcontractors – Service Data Storage & Processing

Entity name	Service provided	Entity Country
Amazon Web Services, Inc.	Cloud Service Provider	United States of America
Salesforce Inc (Heroku)	Cloud Service Provider - App Server provider	United States of America
Intercom Group	Cloud support and user onboarding	United States of America
Checkin Group (GetId)	Cloud Identity Verification Service	Estonia
Agora Lab Inc.	Broadcast and Video Streaming platform	United States of America
Cynny S.p.A (DBA Morphcast)	Facial Analysis libraries	Italy
Github Inc.	Software Development & version control	United States of America

Service Provider Group – LabChanges Unlimited SL Group

Entity name	Service provided	Country
EDT Partners SL	Affiliate to the Service Provider (support, marketing, sale)	Spain
EDT Partners PTE Ltd	Affiliate to the Service Provider (support, marketing, sale)	Singapore
The Lab Ventures	Affiliate to the Service Provider (support, marketing, sale)	Spain

Service Provider Specific Subcontractors

Entity name	Entity Type	Entity Country
Pipedrive	CRM	United States of America
Jira	Ticketing & Support	United States of America
Confluence	Knowledge Base	United States of America
Slack	Internal instant messaging and collaboration	United States of America
QoBox	Stress and security testing	India
Google Workspace	Mail, Doc and related services	United States of America