DATA PROCESSING TERMS

Effective on April 2025

THESE TERMS ARE ENTERED INTO BETWEEN

(1) **Controller** - as identified in the Agreement;

(2) **Processor** - as identified in the Agreement;

both referred to individually as the "**Party**" or jointly as the "**Parties**".

The Parties signed a main agreement for services, referred to as the "**Agreement**"

THE PARTIES AGREE THE FOLLOWING:

1. Definitions and interpretations

1.1. A term will have the meaning from the Agreement unless otherwise defined here.

1.2. In these Terms:
"**ALX**" means ALX Holdings Limited, a company limited by shares, incorporated in Mauritius under company number 213364.

"**ALX Affiliate**" means any legal entity that directly or indirectly controls, is controlled by, or is under common control with ALX. The ALX Affiliates are located, inter alia, in Africa: South Africa, Ethiopia, Nigeria, Egypt, Morocco, Kenya, Ghana, Rwanda and in the United States of America: Delaware, California.

"**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

"**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

"**Data Protection Legislation**" means all laws in any relevant jurisdiction that relate to data protection, privacy, the use of information relating to individuals, and/or the information rights of individuals including, all applicable formal and informal guidance, rules, requirements, directions, guidelines, recommendations, advice, codes of practice, policies, measures or publications of the authority, and the equivalent in any other relevant jurisdictions, all as amended or replaced from time to time;

"**Data Protection Authority**" means any national data protection supervisory authority in the relevant jurisdiction;

"**Data Subject**" an identified or identifiable natural person, meaning the one who can be identified, directly or indirectly, in particular, as identified in Annex 1 - Data Processing and Data Transfer Particulars;

"**Personal Information**" means any information relating to an identified or identifiable Data Subject. Personal Information should be understood to include any related definitions used in Data Protection Legislation and is provided in Annex 1 - Data Processing and Data Transfer Particulars.

"**Processing Activities**" mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and, in particular, the processing activities described in is provided in Annex 1 - the Data Processing and Data Transfer Particulars;

"**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to the Personal Information processed for the Agreement;

"**Sensitive Personal Information**" means Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation, or Personal Information relating to criminal convictions or offenses. Sensitive Personal Information should be understood to include any related definitions used in Data Protection Legislation.

1.3. In the event of any conflict or inconsistency between the provisions of the Agreement and these Terms, the provisions of the Agreement will prevail.

2. Subject of the Terms and Role of the Parties

2.1. These Terms define the Parties' obligations regarding Personal Information that they process for the services in the Agreement.

2.2. The Parties identified the roles (Controller vs. Processor) in the Agreement.

2.3. The processing activities, including the subject matter of the processing, the nature and purpose of the processing and the categories of Data Subjects are set out in the Annex 1 to the Terms.

2.4. As regards the Customer Relationship Management data (invoicing, contact details, internal reporting), the Parties are independent Controllers. This Personal Information are usually details on the contact persons/representatives which the Parties need to process for the legal obligations and the administrative function.

3. Duration of the processing

3.1. The processing will be carried out for the duration of the Agreement.

4. Data Privacy obligations

4.1. The Controller agrees to provide only Personal Information that is strictly required by the Processor for the Agreement. So, the Controller will minimize the Personal Information transferred to the Processor, including by anonymizing and/or pseudonymizing any Personal Information.

4.2. The Processor will do the following while providing the services:

4.2.1. Process the Personal Information only on the basis of documented instructions from the Controller, which may be sent in writing or by e-mail, unless the Processor is required to do so by the law applicable to the Agreement;

4.2.2. Ensure that personnel required to access the Personal Information are subject to a binding duty of confidentiality;

4.2.3. Comply with the Data Protection Legislation and assist the Controller with completing data protection impact assessments, notifying Security Breach incidents to the competent Data Protection Authority or to the affected data subjects, and with prior consultation with Data Protection Authority if needed and related to the Agreement;

4.2.4. Implement appropriate technical and organisational measures to protect the Personal Information against unauthorised or unlawful processing and against accidental loss, destruction, damage. The minimum measures are set out in Annex 2.

4.2.5. The Processor can engage other sub-processors for the performance of the Agreement. The Processor will sign an agreement with the sub-processors which will substantially follow these Terms. Upon request, the Processor will provide the Controller with a copy of such agreement. The Processor remains liable under these Terms for any failure of the sub-processor;

4.2.6. Notify the Controller if the Processor receives any requests from a Data Subject exercising its rights under Data Protection Legislation regarding Personal Information under the Agreement. The Controller is responsible for replying to such requests, and the Processor will assist.

4.2.7. Inform the Controller of complaints/requests etc. from supervisory authorities, regulatory authorities, prosecuting authorities and/or individuals received directly by the Processor or any of its subcontractors in relation to the Agreement. The Controller is responsible for replying to such requests and the Processor will assist;

4.2.8. Allow the Controller and/or independent auditors to conduct audits (including inspections), once per year during the term of the Agreement, and provide reasonable assistance for this. The Processor can provide certificates or audit reports as evidence of compliance. The Controller bears the audit cost; and

4.2.9. stop any use of the Personal Information upon termination or expiry of the Agreement and will destroy all the Personal Information or transfer all Personal Information to the Controller, at the Controller's choice. In case of no choice in 30 days after termination, the Processer may chose;

4.3. In the event of a Security Breach, the Processor will:

4.3.1. Promptly take action to investigate the Security Breach and to identify, prevent and mitigate the effects of the Security Breach and to remedy the Security Breach;

4.3.2. Notify the Controller without undue delay and provide a description of the Security Breach including:

a) the categories and approximate number of Data Subjects affected, their country of residence and the categories and approximate number of records affected;

b) the likely consequences of the Security Breach and the risk posed by the Security Breach to Data Subjects; and

c) the measures taken or proposed to be taken by the Processor to address the Security Breach, to mitigate its adverse effects and provide timely updates to this information;

4.3.3. Not release or publish any filing, communication, notice, press release, or report concerning the Security Breach without the Controller's prior approval (except where required to do so by law or governmental authority). Such approval not to be unreasonably withheld.

4.4. If ALX is a Processor, ALX is entitled to process or have Personal Information processed within as well as outside the country of origin, provided that the requirements of applicable Data Protection Legislation are fulfilled. So, ALX may transfer Personal Information to ALX Affiliates and sub-contractors located outside the country of origin on the basis of the EU Standard Contractual Clauses (Controller to Processor: as approved by the European Commission in June 2021, as detailed here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj). Where specific model clauses (controller-processor) are required by local Data Protection Legislation, the parties agree to incorporate such model clauses to these Terms as an adequate transfer mechanism for the cross-border transfer of Personal Information. As regards transfer details please see Annex 1.

5. OTHER ASPECTS

5.1. The liability arising out of breach of these Terms is limited to the amount of the damage caused by the Party, as evidenced in a court of law.

5.2. Neither Party will be liable, to the extent any failure or delay is caused by or results from acts or circumstances beyond that Party's reasonable control.

5.3. If any part of these Terms is found to be invalid or unenforceable, the validity and enforceability of the rest of the Terms will not be affected.

5.4. Each Party can assign or transfer the rights or obligations of these Terms with prior notification of the other Party.

5.5. These Terms and any dispute or claim arising out of or in connection with it will be governed by and construed in accordance with laws mentioned in the Agreement.

ANNEX 1
Data Processing and Data Transfer Particulars

1. **Subject matter, Purpose & Nature of Processing**

   The Processor will process Personal Information made available by the Controller during the Agreement, as needed for providing the services, e.g. data available in the systems and applications.
   The Processor will act upon the Personal Information only as the Controller instructs it to perform the Services.

2. **Categories of Data Subjects**
   - Controller's employees
   - Controller's candidates
   - Controller's contractors (if individuals)
   - Controller's customers (if individuals)
   - Controller's online visitors
   - any other individual related to the Controller.

3. **Location of Data Subjects**
   As per the Agreement and as per Controller's operations.

4. **Types of Personal Information**
   - Identification data (e.g. names, addresses, dates of birth, domicile)
   - Contact data (e.g. telephone numbers, emails, job titles)
   - Employment data (e.g. employment history, certifications and other performance data)
   - other, as per the business activity of the Controller.

5. **Sensitive or Special Personal Information**
   Generally, the Processor will not receive any sensitive or special Personal Information.

6. **Transfer particulars for the transfer of Personal Information from the Controller, as data exporter to the Processor, as data importer:**
   - the frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): on a continuous basis.
   - purpose(s) of the data transfer and further processing: to allow the Processor to perform the Services;
   - retention: as long as the Agreement is in force;
   - other elements of the transfer are provided at sections 1-5 above.

ANNEX 2
Technical and Organisational Measures

1. ACCESS CONTROL TO SYSTEMS

Measures are taken to prevent unauthorized access to IT systems, including the following technical and organizational measures for user identification and authentication:

- Multi-Factor Authentication (MFA) and complex passwords with quarterly password updates for all user accounts with access to systems containing covered data
-
- No access for guest users or anonymous accounts
- Central management of system and hardware access using principle of least privilege
- Access to IT systems subject to approval from HR management and IT system administrators

2. ACCESS CONTROL TO DATA

Measures are taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorised modification or disclosure of data. These measures include:

- Role-based access control that limits access based on a user's role in the organization, implemented following the principle of least privilege
- Automated logging of user access via IT systems
- Security tools and procedures to detect and prevent unauthorized access to systems

3. DISCLOSURE CONTROL

Measures are taken to prevent the unauthorized access to data, alteration or removal of data during transfer, and to ensure that transfers are secure.

4. INPUT CONTROL

Where feasible, measures are in place to ensure data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained.

5. JOB CONTROL

Measures are in place to ensure that data are processed strictly in compliance with the data exporter's instructions.

6. AVAILABILITY CONTROL

Measures are in place to ensure that data are protected against accidental destruction or loss and include:

- Ensuring that systems or data may be restored in the event of interruption or loss
- Ensure systems are functioning and that faults are reported
- Use of uninterruptible power supplies (UPS) and other business continuity technologies and procedures
- Data backup procedures including use of remote storage where necessary.

7. SYSTEM PROTECTION AND MONITORING

Measures are in place to ensure systems are adequately monitored and protected from a variety of potential threats including, where feasible:

- Firewall implementation including, where feasible, network perimeter protection, internal network segmentation, and application-level firewalls
- Anti-virus / Anti-malware software, including email filtering and threat detection
- Advanced endpoint protection software
- System logging and monitoring
- Regular system updates including security patch deployment and vulnerability remediation timelines.

8. SYSTEMS SEGREGATION CONTROL

Measures are in place to ensure data collected for different purposes are processed separately and include:

- Restriction of access to data stored for different purposes according to staff duties.
- Logical or physical segregation of systems based on the system purpose.
- Logical or physical segregation of systems utilized for testing and production.