Contents

1. Introduction

mLab undertakes to protect the Personal Information of all employees/ stakeholders/ clients /beneficiaries of mLab in compliance with the Personal Information of Protection Act (POPIA).

2. Scope

This policy covers any personal information, which means any information that relates to a specific person. The law notes that this isn't limited to a "**natural person**" (that is, a human being) but also a "**juristic person"** which means an independent legal entity such as a company.

3. Definitions

3.1 **Child:** natural person under the age of 18, who is not legally competent to take any action or decision in respect of any matter concerning him/herself.

3.2 **Competent person:** any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

3.3 **Consent:** any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.

3.4 **Data subject:** person to whom the personal information relates.

a) **De-identify (in relation to data subject):** delete any information that:

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.

3.5 **Electronic communication:** any text, voice, sound, or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

3.6 **Information Officer:** head of a private body as contemplated in section 1, of the Promotion of Access to Information Act. In the case of mLab, this would be the Chief Executive Officer (CEO).

3.7 **Operator**: a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

3.8 **Personal information:** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or

employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

(b) **Processing:** operation or activity or any set of operations, whether by automatic means or not, concerning personal information, including:

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information

4. What personal information might we have about our data subjects

Information collected about any Data Subject (DS) will either be directly provided by the DS; by our strategic partners (for example if you are a beneficiary of another programme with which we have a legal contractual relationship); or be obtained through trusted publicly available sources. To the extent necessary, DS's provide us with consent to collect their personal data from such other persons. mLab may collect various types of personal data, including:

4.1 General and identification information (e.g., name, first name, last name, gender, email and/or postal address, fixed and/or mobile phone number).

4.2 The DS's function where applicable (e.g., title, position, name of current/previous employers; qualifications).

4.3 Payment information (e.g., bank account details, VAT or other tax identification number).

4.4 If the DS is a participant of an online platform - electronic identification data (e.g., login, access right, passwords, badge number, IP address, online identifiers/cookies, logs, access and connection times, image recording or sound such as badge pictures, CCTV or voice recordings).

4.5 Information regarding DS preferences including in terms of channels of communication and frequency.

4.6 Data provided to mLab when DS fill in forms or during events attended, or when DS answer questions in a survey.

4.7 Data which relates to our online mobile applications.

4.8 Information about the training / start-up interactions DSs have with us, including potential future interactions.

5. For which purpose does mLab use personal data and why is it justified?

5.1 mLab will only process personal data if permitted by law, including if:

- mLab has obtained prior consent.
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the DS is a party.
- The processing is necessary to comply with mLab's legal obligations.
- The processing protects the DS's legitimate interest.
- The processing is necessary for mLab's legitimate interests or the legitimate interests of a third party to whom the personal data is supplied and does not unduly affect the DS's interests or fundamental rights and freedoms.

5.2 Examples of legitimate interests may include:

- To benefit from cost-effective services (e.g., mLab may opt to use certain platforms offered by suppliers to process data).
- To offer our products and services to our clients/stakeholders.
- To prevent fraud or criminal activity, misuses of our products or services as well as the security of our IT systems, architecture, and networks.
- To meet our corporate and social responsibility objectives.
- To pay stipends or other legitimate costs to our beneficiaries.

5.3 Personal data will always be processed for a specific purpose and only data that is relevant to the achievement of that purpose will be processed. This may include:

- To manage mlab's relationship with DS's (e.g., through our databases).
- Implement tasks in preparation of or to perform existing contracts.
- Evidence transactions.
- Provide DS with adequate and updated information about mLab products and applications/services.
- Improve the quality of mLab applications/ services by adapting mLab offering to DS's specific needs.
- Answer DS requests and provision of efficient support.
- Send DS surveys.
- Manage communications and interactions with DS.
- Track mLab activities.
- Invite DS to events or promotional meetings sponsored by mLab (e.g., Hackathon events, speaker events, conferences, webinars, meetings on various digital platforms).
- Grant DS access to mLab training modules.

- Manage mLab IT resources, including infrastructure management and business continuity.
- Preserve mLab's economic interests and ensure compliance and reporting (such as complying with our policies and legal requirements, tax, and deductions, managing alleged cases of misconduct or fraud, conducting audits, and defending litigation).
- Archive and keep records.
- Invoice.
- Any other purposes imposed by law and authorities.

6. Who has access to a Data Subjects personal data and to whom can it be transferred?

Mlab will not sell, share, or otherwise transfer any personal data to third parties other than those identified in our Privacy Notice. All third parties are contractually obliged to protect the confidentiality and security of all personal data, in compliance with applicable law. Personal data can be accessed by or transferred to the following categories or recipients:

6.1 Authorised staff members on a strictly need-to-know basis. E.g., A Code Tribe Co-ordinator may require such information to manage the Code Tribe activities.

6.2 mLab's independent agents or brokers. E.g., Payroll and HR service providers, etc.

6.3 mLab's suppliers and services providers that provide services and products to mLab, if relevant.

6.4 mLab's IT systems providers, cloud service providers, database providers and consultants.

6.5 mLab's business/ stakeholders' partnerships who offer funding or services jointly with mLab.

6.6 Any third party to whom mLab assign, cede, or novate any of our rights or obligations.

6.7 mLab advisors and external lawyers.

6.8 Any national and/or international regulatory, enforcement, public body, or court where mLab is required to do so by applicable law or regulation or at their request.

7. How does mLab protect personal data?

7.1 mLab have implemented appropriate, reasonable technical and organisational measures to provide a level of security and confidentiality to all personal data. These measures take into account:

- State of the art technology.
- Costs of its implementation.
- The nature of the data.
- The risk of the processing data.

7.2 The purpose of the above is to protect personal data against accidental or unlawful destruction or alteration, loss, damage, unauthorized disclosure or access and against other unlawful forms of processing.

7.3 When handling any personal data, mLab will:

- Only collect and process personal data, which is adequate, relevant and not excessive, as required to meet the above purposes.
- Ensure that personal data remains up to date and accurate, as far as reasonably possible. To do so mLab may request DSs to confirm the personal data we hold about them. DSs are also invited to spontaneously inform mLab whenever there is a change in their personal circumstances so mLab can ensure their personal data is kept up to date.
- When processing data for research or reporting purposes mLab undertakes to "anonymise" or de-identify data so that it cannot be traced back to an individual.

8. How long will mLab store personal data?

mLab will only retain personal data for as long as necessary to fulfil the purpose for which it was collected or to comply with legal or regulatory requirements. When this period expires, personal data is removed from mLab's systems.

9. What are Data Subject's rights and how can they exercise them?

Data Subjects have the following rights, within the limits of the law:

9.1 The right to access their personal data as processed by mLab and, if s/he believes that any information relating to them is incorrect, obsolete or incomplete, to request its correction or updating.

9.2 The right to request the erasure of their personal data or the restriction thereof to specific categories of processing.

9.3 The right to withdraw their consent at any time, without affecting the lawfulness of the processing before such withdrawal.

9.4 The right to object, in whole or in part, to the processing of their personal data.

9.5 The right to object to a channel of communication used for direct marketing purposes.

9.6 The right to request its portability where applicable.

10. Relevant legislation and documentation

This policy must be read in conjunction with:

10.1   The POPI Act, implemented on 1 July 2021

10.2   mLab's Data Privacy Statement