Personal Data Protection and Privacy Policy

Injini EdTech Acceleration NPC | Version 2.0 | April 2026

Definitions

The following definitions apply throughout this policy:

Applicable Law	Means the DPA, EU GDPR, POPI/POPIA, UK GDPR, the Rwanda Law No. 058/2021 on the Protection of Personal Data and Privacy, or any one of them as the context may indicate.
Data Subject	Means a person whose personal data is processed by Injini, including programme participants, staff, contractors, funders, and visitors to our facilities.
EU GDPR	Means the European Union General Data Protection Regulation 2016/679.
DPA	Means the United Kingdom Data Protection Act 2018.
Deputy Information Officer	Means, at the publication date of this version of this policy, Mr Larry Leyden.
ICO	Means the United Kingdom Information Commissioner's Office.
Information Officer	Means, at the publication date of this version of this policy, Mrs Krista M Davidson.
Injini (or "us", "we", "our")	Means Injini EdTech Acceleration NPC (registration number 2017/193849/08).
IPO	Means an Impact Partner Organisation appointed by a funder (such as the Mastercard Foundation) to conduct data collection, sampling, or analysis in connection with programme outcomes assessments.
Personal Data Inventory	Means an inventory recording the different types of personal data held, processed, or controlled by Injini.
POPIA	Means the South African Protection of Personal Information Act 4 of 2013, as amended.
Rwanda Data Protection Law	Means Rwanda Law No. 058/2021 of 13/10/2021 on the Protection of Personal Data and Privacy, as administered by the Rwanda National Cyber Security Authority (NCSA).
Responsible Person	Means the Deputy Information Officer or, failing such person, the Information Officer, as appointed from time to time.
Regulator	Means, in the case of POPIA, the South African Information Regulator; in the case of the Rwanda Data Protection Law, the Rwanda NCSA; in the case of the DPA and UK GDPR, the ICO; and in the case of the EU GDPR, the relevant supervisory authority in the applicable member state.
Data Sharing Agreement (DSA)	Means a study-specific agreement entered into between Injini and an IPO or other third-party data processor, governing the terms under which participant data may be shared.

Purpose

Injini exists within local and international data protection and privacy environments in which effective relationships with clients and broader stakeholders are critical to our continued success.

In the course of our operations, we may receive, hold, process and transfer personal data relating to project and funding beneficiaries, including beneficiaries of skills development and enterprise development programmes, as well as personal data of our staff, stakeholders, suppliers and of visitors to our facilities.

Injini operates programmes in South Africa and Rwanda. This policy applies to all personal data processing activities in both jurisdictions and is designed to ensure compliance with POPIA, the Rwanda Data Protection Law, and other Applicable Law.

The purpose of this document is to set out our overarching data protection policy, including our obligations when sharing participant data with funders and their appointed Impact Partner Organisations.

Roles and Responsibilities

Information Officer and Deputy Information Officer

In accordance with Section 55 of POPIA, Injini is required to register an Information Officer with the South African Information Regulator. The Information Officer is responsible for ensuring Injini's compliance with this policy and with Applicable Law.

Current appointments:

- Information Officer: Mrs Krista Davidson — registered with the South African Information Regulator
- Deputy Information Officer: Mr Larry Leyden

These appointments must be kept current. Any change in the person holding either role must be updated on the Information Regulator's eServices portal without delay, and this policy updated accordingly.

Injini as Data Controller

In connection with Injini's own programme activities, Injini acts as an independent Data Controller in respect of the personal data of its programme participants, staff, and other stakeholders.

Injini as Data Processor or Joint Controller

Where Injini processes personal data on behalf of or jointly with a funder or other party (for example, in connection with a funder-led programme outcomes assessment), Injini's role — whether as independent controller, joint controller, or data processor — will be determined by the nature of the engagement and the applicable jurisdictional laws. Injini will comply with all obligations applicable to its role under Applicable Law.

Data Protection Principles

We are committed to processing personal data in accordance with our responsibilities under Applicable Law. It is therefore our policy to ensure that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Lawful Purposes and Consent

Lawful Basis for Processing

All data processed by us must be done on at least one of the following lawful bases: consent, contract, legal obligation, vital interests, public task, or legitimate interests, as contemplated by relevant Applicable Law pertaining to the Data Subjects whose personal data we process.

We shall note the appropriate lawful basis in our Personal Data Inventory as part of our internal records.

Programme Participant Consent

Where Injini collects personal data from programme participants, informed consent must be obtained prior to data collection. Consent must be:

- **Freely given** — participants must not be pressured to consent, and must be clearly informed that their eligibility to participate in the programme is not conditional on providing consent to data sharing;
- **Specific** — consent must be for a defined and clearly explained purpose;
- **Informed** — participants must be told who will collect their data, why it is being collected, who it will be shared with (including any funders and their appointed IPOs), how long it will be kept, and what their rights are; and
- **Unambiguous** — consent must be obtained through a clear opt-in mechanism such as a checkbox or signature; pre-ticked boxes are not valid.

Injini shall maintain written records of participant consent, including the date and method of consent, and shall make these available to funders upon request. Where explicit consent cannot be obtained, the relevant personal data shall not be shared with funders or IPOs.

Participants shall be informed of their right to withdraw consent at any time, and clear instructions shall be provided on how to do so. Withdrawal of consent shall not affect a participant's ability to continue participating in the programme.

Where participants are not literate or where consent forms are translated into a local language, a jurat clause must be included, signed by an interpreter.

Cross-Border Data Transfers

Injini operates in South Africa and Rwanda and may share participant data with funders and IPOs located in other jurisdictions (including Canada and other countries). Where personal data is transferred outside the country of collection, Injini shall:

- Identify and document the legal basis for the transfer under Applicable Law;
- Ensure that adequate data protection standards are in place in the receiving jurisdiction or are contractually guaranteed through a Data Sharing Agreement; and
- Record all cross-border transfers in the Personal Data Inventory.

Data Sharing with Funders and Impact Partner Organisations

Where Injini is required by a funder to share participant data with that funder or with an IPO appointed by the funder (for example, for the purpose of a programme outcomes assessment), Injini shall:

- Enter into a study-specific Data Sharing Agreement (DSA) with the IPO prior to sharing any participant data, aligned with the funder's data governance and safeguarding standards;
- Share only sampled participant identifiers and related metadata as required for the specific assessment — Injini shall retain custody of the full participant database at all times;
- Ensure that all data shared is covered by appropriate participant consent;
- Designate a focal point within Injini to coordinate with the IPO and funder on assessment-related activities; and
- Ensure that data sharing is conducted using secure transfer protocols and in accordance with Applicable Law.

Injini will not share personal data with any third party for processing other than as permitted by Applicable Law, and only where that third party has agreed to put in place adequate data protection measures.

Data Protection Governance

Regulatory Registration

Injini shall maintain valid and current registration as a Data Controller with the South African Information Regulator in terms of POPIA, and with the Rwanda NCSA in terms of the Rwanda Data Protection Law, where required. Registrations shall be renewed in accordance with applicable regulatory requirements.

Data Protection Impact Assessments

Injini shall conduct Data Protection Impact Assessments (DPIAs) prior to any processing activities that are likely to result in a high risk to the rights and freedoms of data subjects, including processing involving vulnerable populations, sensitive data categories, or large-scale participant datasets shared with third parties.

Personal Data Inventory

The Responsible Person shall maintain and regularly update a Personal Data Inventory recording the categories of personal data held, the purposes for which it is processed, the legal basis for processing, retention periods, and any third parties with whom it is shared.

Annual Review

This policy shall be reviewed at least annually by the Responsible Person, or earlier where there is a material change in Injini's processing activities, legal status, or applicable regulatory obligations.

Data Minimisation and Retention

We shall ensure that personal data processed is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Personal data shall not be retained for any longer than is necessary to achieve the purpose for which it was collected, subject to any legal or regulatory retention requirements. Injini shall document data retention periods in the Personal Data Inventory.

Once personal data is no longer required, it shall be securely deleted or anonymised such that it cannot be retrieved or attributed to an identifiable individual.

We retain a suppression list of individuals who no longer wish to be contacted by us, which we honour unless we have a lawful basis and a need to contact such individuals.

Security

We shall ensure that personal data is stored securely. Where personal data is stored in digital formats, such personal data shall be stored using modern software that is kept up-to-date.

Access to personal data shall be limited to personnel who need access and shall be role-based and least privileged. Appropriate security shall be in place to avoid unauthorised sharing of information.

Where data is shared with IPOs or other third parties, Injini shall ensure that transfer is conducted using encrypted, secure protocols (e.g. HTTPS, TLS) and that the receiving party meets minimum cybersecurity standards as required by the relevant funder.

Personal devices may only be used to process participant data if adequately secured and approved by the Responsible Person.

Appropriate backup and disaster recovery solutions shall be in place. When personal data is deleted, this shall be done safely such that the data is irrecoverable.

Data Breach Management

Injini shall maintain internal incident response procedures to detect, contain, and remediate actual or suspected personal data breaches.

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, we shall:

- Promptly assess the risk to data subjects' rights and freedoms;
- Notify the relevant Regulator as soon as reasonably possible, and where required by Applicable Law; and
- Where Injini is participating in a funder-led programme, notify the relevant funder without undue delay and cooperate fully in breach investigation, containment, remediation, and regulatory reporting.

Our Online Programmes, Website and Newsletter

Where users of our website wish to make use of our online services or sign up for our newsletters or other marketing channel communications, we shall collect such personal data in the form of names, email addresses, and other contact information where supplied. We collect such personal data solely for the purposes of supplying our online programmes, newsletters, and marketing communications as selected by a user.

Injini neither sells personal data to third parties nor uses any automated decision-making in the processing of users' personal data.

We may share users' personal data with MailChimp, ActiveCampaign, LinkedIn, or Google for the purpose of distributing our newsletter and contacting newsletter recipients. Any users who wish to have their personal data removed may unsubscribe using the link provided at the bottom of each email.

Data Subject Rights

Individuals whose personal data we process have the following rights, which Injini shall honour in a timely manner:

- Right of access — to request a copy of personal data we hold about them;
- Right to rectification — to ask us to correct inaccurate data;
- Right to erasure — to ask us to delete their data;
- Right to restriction of processing;
- Right to object to processing; and
- Right to data portability.

Any such requests shall be directed to the Responsible Person and dealt with in a timely manner in accordance with Applicable Law. Injini shall inform data subjects of their rights at the point of consent collection.

Version History

Version 1.0 — February 2022: Initial policy publication.

Version 2.0 — April 2026: Updated to reflect: registration obligations under POPIA and Rwanda Data Protection Law; participant consent requirements for funder-led programme outcomes assessments; cross-border data transfer obligations; data sharing with IPOs and funders; DPIA requirements; and cybersecurity standards for data sharing.