Group Data

Personal Data Protection and Privacy Policy

Definitions

UVU Africa	Means any and all legal entities within the definition of UVU Africa Group below.
Applicable Law	Means the DPA, EU GDPR, POPI, UK GDPR or any one of them as the context may indicate.
UVU Africa Group	Means UVU Africa NPC (registration number 1999/002647/08), Bandwidth Barn (Pty) Ltd (registration number 2000/015304/07), Injini EdTech Acceleration NPC (registration number2017/193849/08), UVU Bio NPC (registration number 2019/075897/08) and any company falling within the same "group" of companies as UVU Africa NPC provided for in section 1 of the Companies Act 71 of 2008.
Data Subject	Means a person whose personal data is processed by UVU Africa.
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 Ashley Minnaar.
ICO	Means the United Kingdom Information Commissioner's Office.
Information Officer	Means, at the publication date of this version of this Policy, Mr Ian Merrington.
UK GDPR	Means the United Kingdom General Data Protection Regulation.
Personal Data Inventory	Means an inventory recording the different types of personal data held, processed or controlled by UVU Africa.
POPI	Means the South African Protection of Personal Information Act 4 of 2013.
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 the DPA and UK GDPR, the ICO, in the case of the EU GDPR and any particular EU member state, the relevant official appointed with the responsibility for overseeing implementation of the EU GDPR in that member state and in the case of POPI, the Information Regulator established in terms of POPI.

Purpose

UVU Africa ("our", "we", "us") and its core businesses exist 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.

It is important that our relationships with all stakeholders are based on a clear understanding of our expectations and requirements in the area of data protection. These expectations and requirements must be documented in a way that leaves no doubt about the importance we place on data protection.

The purpose of this document is to set out our overarching data protection policy.

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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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, having regard to the purposes for which they are processed, 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by Applicable Law in order to safeguard the rights and freedoms of individuals; 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, using appropriate technical or organisational measures.

General Provisions

a. This policy applies to all personal data processed by us.

b. The Responsible Person shall take responsibility for our ongoing compliance with this policy. c. This policy shall be reviewed at least annually.

Lawful, Fair and Transparent Processing

Individuals have the right to access their personal data processed by us and any such requests made to us shall be dealt with in a timely manner.

Lawful Purposes

a. 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.

b. We shall note the appropriate lawful basis in an internal personal data inventory as part of our internal company records.

c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept in relation to the personal data concerned.

d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in our systems.

Data Minimisation

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

Accuracy

a. We shall take reasonable steps to ensure personal data is accurate.

b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Retention and Deletion of Personal Data

a. Where we are required by virtue of any Applicable Law, regulation or code of conduct of a reputable industry association of which we are a member, to retain any particular documents or records, including personal data, we will retain all such documents and records for not less than the minimum periods prescribed by any such law, regulation or code.

b. Outside of such legal, regulatory or code of conduct requirements, it is our policy that personal information should not be retained for any longer than is necessary to achieve the purpose for which that personal data was collected.

c. We keep personal information for as long as is reasonably necessary to enable us to provide our clients and funders with the services that they have requested or expect from us, to comply with any legal obligations that require us to keep personal information, or for as long as we reasonably require for our legitimate interests, including for example for the purposes of exercising our legal rights or defending ourselves against claims. It is our policy to look to find ways to reduce the amount of personal information that we hold and the length of time that we need to keep it.

d. We try to adopt a paperless approach wherever possible and securely destroy any paper correspondence we receive on a regular basis unless we are required to retain it for evidential or legal purposes.

e. We retain a suppression lists of individuals who no longer wish to be contacted by us indefinitely and we honour individual wishes in this regard unless we have a lawful basis and a need to contact such individuals. We need to keep this information to comply with their wishes not to be contacted by us.

f. We may also make use of data protection techniques such as personal data anonymisation (where personal data is converted to a non-personally identifiable format) and personal data pseudonymisation (the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information). Where we perform any data pseudonymisation, we keep the additional information separate from the pseudonymised data and subject to technical and organisational measures to ensure that the pseudonymised data is not attributed to an identified or identifiable natural person.

Our Online Programmes, Website and Newsletter

a. Notwithstanding anything to the contrary recorded in this policy, 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 user's personal data in the form of names, email addresses and other contact information where supplied such as mobile telephone numbers. We collect such personal data solely for the purposes of supplying our online programmes, newsletters and marketing communications as and where selected by a user.

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

c. We may share users' personal data with MailChimp, ActiveCampaigns, LinkedIn or Google, for the purpose of distributing our newsletter and contacting newsletter recipients as well as to provide offers for recruitment or participation in our programmes and events. All personal data collected by UVU Africa for such purposes is stored indefinitely for the purpose of distributing the newsletter, programmatic recruitment calls or other digital communications. Any users who wish to have their personal data removed from UVU Africa's newsletter or marketing database may unsubscribe using a link provided at the bottom of each email containing the newsletter or other marketing communication. Once unsubscribed, the user will cease receiving newsletter or marketing emails from UVU Africa and their personal data will be removed from UVU Africa's marketing database.

Security

a. 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.

b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

c. When personal data is deleted this should be done safely such that the data is irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

Third Parties

We shall not provide personal data to any third party for processing other than as permitted in terms of Applicable Law and unless that third party undertakes to put in place adequate protection measures that are no less protective of the personal data than the measures put in place by us to protect the personal data concerned.

Breach

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 people's rights and freedoms and if appropriate report this breach to the relevant Regulator.