UNIVERSITY OF LAY ADVENTISTS OF KIGALI (UNILAK)

DATA PROTECTION POLICY

February 2024

Data Protection Policy

1. Introduction

University of Lay Adventists of Kigali (UNILAK) takes its responsibilities with regard to the management of the requirements of Data Protection very seriously. This policy sets out how the UNILAK manages those responsibilities.

UNILAK obtains, uses, stores and otherwise processes personal data relating to potential members of UNILAK and students, current members and students, former members and students, consultants, contractors, website users and contacts, collectively referred to in this policy as data subjects. When processing personal data, UNILAK is obliged to fulfill individuals' reasonable expectations of privacy by complying with Policy and other relevant data protection legislation.

On October 15, 2021, Law No 058/2021 of 13/10/2021 relating to the protection of personal data and privacy was officially gazetted. This law protects personal data and ensures privacy of individuals in Rwanda.

One of the tenets of this law is the clear and unambiguous consent of an individual to the collection, storage, and processing of personal data, which is a fundamental right.

The law now brings Rwanda in line with international data protection standards, vital for modern digital economy facilitating services such as e-commerce, international financial transactions, and various online services.

The primary goals of this law are to:

- Empower citizens with the agency over their personal data
- Enable trusted and secure data flow, domestically and internationally
- Provide regulatory certainty for existing businesses and prospective investors, and an enabling environment for SME growth
- Accelerate Rwanda's ambitions toward a technology-enabled and data-driven economy

This policy therefore seeks to ensure that we:

a. are clear about how personal data must be processed and UNILAK's expectations for all those who process personal data on its behalf;
b. comply with the data protection law and with good practice;
c. protect UNILAK's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights;
d. protect the UNILAK from risks of personal data breaches and other breaches of data protection law.

2. The Scope of the Policy

This policy applies to all personal data we process regardless of the location where that personal data is stored and regardless of the data subject. All members and others processing personal data on UNILAK's behalf must read it.

A failure to comply with this policy may result in disciplinaryaction.

Application

• University faculty members (including part-time and visiting faculty)

• Staff and other employees

• Guests with electronic access, as well as any other users of the network infrastructure, including independent contractors or others (e.g., temporary agency employees) who may be given access on a temporary basis to university systems

• Third parties, including vendors, affiliates, consultants, and contractors

UNILAK Management is responsible for overseeing this policy.

3. Personal data protection principles

When you process personal data, you should be guided by the following principles, which are set out in UNILAK Data Protection Policy. The UNILAK is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

Those principles require personal data to be:

a. processed lawfully, fairly and in a transparent manner;
b. collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed;
d. accurate and where necessary kept up to date;
e. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed;
f. processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

4. Data Subjects' Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

a. where the legal basis of our processing is Consent, to withdraw that Consent at any time;
b. to ask for access to the personal data that we hold;
c. to prevent our use of the personal data for direct marketing purposes;
d. to object to our processing of personal data in limited circumstances;
e. to ask us to erase personal data without delay;
f. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
g. if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;
h. if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;
i. if the data subject has objected to our processing for direct marketing purposes;
j. if the processing is unlawful;
k. to ask us to rectify inaccurate data or to complete incomplete data;
l. to restrict processing in specific circumstances e.g. where there is a complaint about accuracy;
m. to ask us for a copy of the safeguards under which personal data is transferred outside of Rwanda;
n. the right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with the University; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards;
o. to prevent processing that is likely to cause damage or distress to the data subject or anyone else;
p. to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

q. in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights list.

5. Accountability

UNILAK is responsible for, and must be able to demonstrate compliance with, the data protection principles.

UNILAK must apply adequate resources and controls to ensure and to document Data Protection Policy compliance including:

a. appointing a suitably qualified DPO in the Directorate of ICT;
b. integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;
c. training staff on compliance and keeping a record accordingly; and
d. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

6. Responsibilities

1. UNILAK responsibilities:
   As the Data Controller, the UNILAK is responsible for establishing policies and procedures in order to comply with data protection law.

2. Data Protection Officer responsibilities: The Directorate of ICT is responsible for:
   a. advising the UNILAK and its staff of its obligations;
   b. monitoring compliance with this Policy and other relevant data protection law, UNILAK's policies with respect to this and monitoring training and audit activities relate to Data Protection compliance;
   c. to provide advice where requested on data protection impact assessments;
   d. the data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

3. Staff responsibilities
   Staff members who process personal data about students, staff, applicants, alumni or any other individual must comply with the requirements of this policy. Staff members must ensure that:
   a. all personal data is kept securely;
   b. no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
   c. personal data is kept in accordance with UNILAK's retention schedule;

   a. any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Officer;
   b. any data protection breaches are swiftly brought to the attention of the Information Compliance team and the Data Protection Officer;
   c. where there is uncertainty around a data protection matter advice is sought from the Data Protection Officer OR Director of ICT.

Where members of staff are responsible for supervising students doing work which involves the processing of personal information (for example in research projects), they must ensure that those students are aware of the Data Protection principles.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Data Protection Officer.

4. Third-Party Data Processors

Where external companies are used to process personal data on behalf of UNILAK, responsibility for the security and appropriate use of that data remains with UNILAK.

Where a third-party data processor is used:

a. a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
b. reasonable steps must be taken that such security measures are in place;
c. a written contract establishing what personal data will be processed and for what purpose must be set out; a data processing agreement, available from the Data Protection Officer, must be signed by both parties.

For further guidance about the use of third-party data processors please contact the Data Protection Officer.

5. Contractors, Short-Term and Voluntary Staff

UNILAK is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition managers should ensure that:

a. any personal data collected or processed in the course of work undertaken for UNILAK is kept securely and confidentially;
b. all personal data is returned to UNILAK on completion of the work, including any copies that may have been made. Alternatively that the data is securely destroyed and UNILAK receives notification in this regard from the contractor or short term / voluntary member of staff;
c. UNILAK receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
d. any personal data made available by UNILAK, or collected in the course of the work, is neither stored nor processed outside the Rwanda unless written consent to do so has been received from UNILAK;
e. all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

6. **Student responsibilities**

Students are responsible for:

a. familiarising themselves with the Privacy Notice provided when they register UNILAK;
b. ensuring that their personal data provided to UNILAKis accurate and up to date.

7. Data subject Access Requests

Data subjects have the right to receive copy of their personal data which is held by UNILAK. In addition, an individual is entitled to receive further information about the UNILAK's processing of their personal data as follows:

a. the purposes;
b. the categories of personal data being processed;
c. recipients/categories of recipient;
d. retention periods;
e. information about their rights;
f. the right to complain to the DPO or Director of ICT;
g. details of the relevant safeguards where personal data is transferred outside of Rwanda;
h. any third-party source of the personal data

UNILAK will not allow third parties to persuade UNILAK staff into disclosing personal data without proper authorisation. For example, students' parents do not have an automatic right to gain access to their son's or daughter's data.

The entitlement is not to documents but to such personal data as is contained in the document. The right relates to personal data held electronically and to limited manual records.

8. Reporting a personal data breach

This Policy requires that all staff and student report to the DPO or DVCF any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

If you know or suspect that a personal data breach has occurred, you should immediately contact the DPO or Director of ICT and follow the instructions in the personal data breach procedure. You must retain all evidence relating to personal data breaches in particular to enable UNILAK to maintain a record of such breaches.

9. Record Keeping

Under this Policy UNILAK will keep full and accurate records of all our data processing activities. UNILAK will keep and maintain accurate corporate records reflecting our processing, including records of data subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of processing.

These records should include, at a minimum, the name and contact details of the UNILAK as Director of ICT and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

Records of personal data breaches must also be kept, setting out:

a. the facts surrounding the breach;
b. its effects; and
c. the remedial action taken.

10. Training and Audit

UNILAK will ensure that all UNILAKstaff undergoes adequate training to enable them to comply with data protection Policy. We must also regularly test our systems and processes to assess compliance.