Are Universities Compliant? A Study of Tanzania's Person al Data Protection Act in Higher Learning Institutions

Doreen F. Mwamlangala
Lecturer, The Open University of Tanzania
mwamlangaladoreen@gmail.com

Abstract
In November 2022, the United Republic of Tanzania enacted the Personal Data Protection Law (PDPA). It established a comprehensive framework for the processing of personal data. The Act has a significant impact on higher learning institutions, which are custodians of vast amounts of personal data from students, staff, and other stakeholders. The law designates the institutions as data controllers and processors, and they are obligated to process personal data in accordance with the provisions of the Act. This article examines the compliance of higher learning institutions with the Act. Employing a doctrinal legal research approach, the article assesses Universities' compliance with the PDPA and its regulations. The findings indicate that, although the PDPA has been in place for more than two years, the compliance rate remains extremely low among higher learning institutions. This is due to a lack of data protection policies in universities and awareness training, as well as the absence of data protection officers. The article recommends that Universities appoint data protection officers and register with the Data Protection Commissioner as data controllers, which demonstrates compliance. In addition, the universities must ensure that personal data is processed in accordance with the Act and that their data protection policies and procedures are regularly updated to maintain ongoing compliance.

Keywords*: Compliance, Personal Data Protection Law, Higher Learning Institutions, Tanzania, Data Controller.*

1.0 Introduction

Over the past decade, the rapid advancement of digitalisation has significantly increased the generation and collection of personal data across various sectors, including financial institutions, telecommunications, healthcare, insurance, and education, among others. [1] This development underscored the need for a global legal framework to

[1] R. Mekovec, & D. Peras, 'Implementation of the General Data Protection Regulation: Case of Higher Education Institution,' *International Journal of e-Education, e-Business, e-Management and e-Learning*, Vol. 10 No. 1,2020, (104-112), p 105.

safeguard personal data. In addressing this need, the United Republic of Tanzania introduced its first Personal Data Protection Act (PDPA) in November 2022, which took effect in May 2023. On the one hand, the PDPA establishes rules for the collection, processing, and use of personal data within the United Republic of Tanzania. On the other hand, it establishes supervisory authority, with the Personal Data Protection Commission (PDPC) being responsible for enforcing the PDPA. The Act largely mirrors the European Union's General Data Protection Regulation (GDPR) of 2016. Since the PDPA came into effect, companies and institutions were required to revise and enact new policies not only to meet the explicit requirements of the PDPA but also to ensure the tangible proof of compliance for the supervisory authority. The PDPA also introduces striking changes in personal data processing and establishes new obligations for data controllers and processors.

Two years have passed since the law came into force, but little is known about its compliance. Two reasons may cause this. First, no compliance report has been issued by the PDPC, as it is done in other East African countries such as Kenya, where the PDPC shares those reports on its website, on the X platform, and on different social media platforms. Second, there is limited research on the country's compliance with data protection laws. This article aims to identify the changes and explore their practical relevance by examining the compliance of four Tanzanian Higher Learning Institutions (HLIs). These are University of Dar Es salaam (UDSM), Sokoine University of Agriculture (SUA), the Open University of Tanzania (OUT) and Tumaini University Makumira (TUMA).

This article's analysis is necessary for three reasons. First, it provides a thorough and comprehensive summary of the compliance trend from the selected higher learning institutions (HLIs). The primary objective is to assess the compliance rate of these institutions and determine whether it falls within the expected range, as per the provisions of the PDPA. The article highlights the importance of protecting personal information and the identity measures HLIs can take to improve compliance with regulations and enhance data protection and privacy. Second, the compliance trend in Tanzanian universities has implications for how other higher learning institutions in Africa can improve compliance with personal data protection regulations in their jurisdictions. The third reason

is to help HLIs raise awareness of the PDPA. The article begins with an introduction, followed by an analysis of personal data processing in HLIs. The text outlines the scope and applicability of the PDPA within higher learning institutions, followed by an analysis of the compliance status of selected HLIs. The article concludes with concluding remarks and recommendations for future directions.

2.0 Processing of Personal Data in Higher Learning Institutions

Currently, Tanzania has a total of 50 approved higher learning institutions (HLIs).[1] The institutions registered approximately 588,554 students and 8,625 academic staff in 2023, and the number is increasing.[2] Due to their digital transformation across various scholarly activities, HLIs have experienced accelerated development in the collection and processing of personal data. All aspects of institutional operations, from staff hiring and research administration to student admissions and alumni involvement, now depend on the processing of personal data. Data-driven administration has grown rapidly as a result of the increasing use of electronic technologies, including learning management systems (LMS), student information systems (SIS), and digital testing platforms. There are significant ethical and legal concerns since the quick growth of data-driven administration has not been accompanied by comparable data security safeguards.[3] This case study demonstrates that HLIs have become vast repositories of personal data in digital format.[4] The data-driven environment has created both opportunities and challenges in protecting individual data.[5]

The academic lifecycle of Tanzanian HLIs encompasses personal data processing at every stage. The admission procedure requires students to

[1] Tanzania Commission for Universities, 'University Institutions Approved to Operate in Tanzania as of March 1, 2025,' available at: https://tcu.go.tz/sites/default/files/file_uploads/documents2024-03/LIST%20OF%20UNIVERSITY%20INSTITUIONS%20IN%20TANZANIA%20AS%20OF%MARCH%2001-2025.pdf (last accessed 30th June 2025).

[2]Tanzania Commission for Universities: 'VITALSTATS on University Education in Tanzania of 2023,' available at https://www.tcu.go.tz. (Last accessed 3rd July 2025).

[3] D.Junkai and Q. Xiaoyan, 'Legal Challenges in Protecting Personal Information in Big Data Environments,' Available at: https://ssrn.com/abstract=5166908 or http://dx.doi.org/10.2139/ssrn.5166908 (Last accesed 30th June 2025).

[4] N. McKelvey, 'Data Protection Issues in Higher Education with Technological advancements,' *International Journal of Evaluation and Research in Education* (IJERE), Vol. 3, No.3, 2014 (133-141) p. 137.

[5] F. Schäfer, H. Gebauer, C. Gröger, O. Gassmann, & F. Wortmann, 'Data-driven Business and Data Privacy: Challenges and Measures for Product-based Companies,' *Business Horizons Journal*, Vol. 66, No. 4, 2023 (493-504) p 495.

provide personal information, including their names, national identification numbers, educational history, health information, and biometric data such as fingerprints and passport photographs. The institutions save student data sets for academic performance records, disciplinary files, financial records, and participation logs post-enrolment. Institutional personnel data encompasses employment contracts, payroll information, medical insurance documentation, and performance evaluation outcomes. Further, Universities conduct personal data processing for research purposes in the social sciences, public health, and education sectors. Identifiable data gathering from study participants often transpires without effective anonymisation techniques and insufficient consent protocols.[6] The establishment of digital libraries and online educational platforms has also initiated novel data collection techniques that analyse user behaviour and assess students' learning advancement.[7]

The comprehensive processing environment of Tanzanian HLIs functions within a regulatory framework that has recently begun to recognise data protection as a legal obligation. The PDPA instituted a significant legislative framework to govern the acquisition, storage, and utilisation of personal data in both public and commercial entities. The Act provides a comprehensive definition of personal data and outlines essential principles, including legality, fairness, transparency, purpose limitation, data minimisation, and accountability.[8] These principles are particularly significant in HLIs. As Tanzanian HLIs process large volumes of personal data in pursuit of legitimate educational and administrative objectives, there is a pressing need for these institutions to align their practices with national data protection laws.

Section 3 of the PDPA defines a data controller as an individual, legal entity, or public authority that independently or collaboratively establishes the objectives and methods for processing personal data. Moreover, according to the objectives and principles outlined in the

[6] V. Rupp, and M. Grafenstein, 'Clarifying "Personal Data" and the Role of Anonymisation in Data Protection Law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection,' *Computer Law & Security Review*, Vol. 52, No.1, 2024, 105932, availabe at, https://doi.org/10.1016/j.clsr.2023.105932.
[7] A. Haleem, M. Javaid, M. Qadri, R. Suman, 'Understanding the Role of Digital Technologies in Education: A review,' *Sustainable Operations and Computers Journal,* Volume 3, 2022, (275-285,) p 276.
[8] *The Personal Data Protection Act, 2022, S 4.*

PDPA, the term' data controller' refers to an individual, legal entity, or public authority, including their representative. Similarly, the same section defines the data processor as a legal, natural person, or public body that processes personal data on behalf of the controller. From the perspective of the above section, HLIs are considered both data controllers and data processors. This is because they determine the purpose and means of processing personal data of their clients and become subject to the PDPA. Therefore, it implies that compliance with PDPA is not only ethical but a legal requirement for HLIs.

3.0 Scope and Application of the PDPA and its applicability to Higher Learning Institutions

The PDPA regulates not only the processing of personal data by both public and private institutions but also governs automated and non-automated processing of personal data in Tanzania. However, the Act only permits the processing of personal data belonging to a living natural person, also known as a data subject. It does not extend to a juristic person. The Act applies to the processing of personal information carried out by a data processor or controller residing in the country or in a place where Tanzanian law is applicable in accordance with international law.[9] Similarly, it applies to controllers or processors residing outside Tanzania if the processing takes place in the country, but not for the purpose of merely transiting personal data through Tanzania to another country.[10] However, the requirement that data processing occurs within the country to trigger extraterritorial applicability limits the scope of PDPA compared to regulations like the GDPR.

The PDPC established by the Act is a body corporate.[11] Its functions include, among other things, monitoring compliance with the PDPA by data controllers and processors. To fulfil the above obligation, the PDPC is required to register data controllers and processors in the country.[12] It also has the power to receive, investigate, and deal with complaints about alleged personal data breaches.

[9] The Personal Data Protection Act, (n 9) s 22.
[10] Ibid.
[11] The Personal Data Protection Act, (n 10) s 6.
[12] The Personal Data Protection Act, (n 12) s 7.

The PDPA outlines specific situations where it is not applicable, as per section 58(2). These entail instances where personal data is processed for personal or domestic purposes, in compliance with legal requirements or court orders, and to ensure national security, public safety, and the public interest. The exemptions also cover purposes such as crime prevention or detection, preventing tax evasion, investigating the embezzlement of public funds, and conducting background checks for appointments to public service positions. Furthermore, Section 58(3) grants the Minister responsible for Information, Communications and Information Technology extensive powers to expand the scope of exemptions. Ministerial oversight is required for overall policy direction; however, the concentration of such broad powers within a single executive office, without sufficient institutional balances, raises legal and constitutional concerns about potential abuse. The powers in question pose a genuine risk of unlawful or arbitrary usage. The exercise of ministerial discretion may jeopardise both data subjects' rights and regulatory neutrality.

The PDPA is based on eight core principles for data processing, which are crucial and significant in HLIs. Section 5 of the PDPA provides the principles, and the responsible Minister formulates various regulations to complement them. These regulations include the Data Protection (Personal Data Collection and Processing) Regulation[13] and the Personal Data (Complaints Settlement Procedures) Regulation 2023.[14] Together, these regulations play a critical role in clarifying and operationalising the core data protection principles set out in the Act. Generally, the practical application of data processing principles depends significantly on the interpretive guidance provided in the regulations.

The first principle requires that personal data be processed legally, fairly, and transparently. The criteria for fairness are provided under Regulation 25 of the Personal Data Collection Regulation. Fair collection presupposes that the data subjects have been notified of the intention and purposes of collecting their personal data and have given their consent. Lawfulness entails adhering to the conditions provided under section

[13] The Data Protection (Personal Data Collection and Processing) Regulation, 2023. Available at http://www.mawasiliano.go.tz/uploads/documents/sw-1691159153-GN%20NO.%20449C%20OF%202023.pdf.

[14] The Personal Data (Complaints Settlement Procedures) Regulation, 2023. Available at https://www.mawasiliano.go.tz/uploads/documents/sw-1691159153-GN%20NO.%20449C%20OF%202023.pdf.

22(2), which requires a legitimate purpose of collection and showing that the collection was necessary in relation to the purpose. The principle is to the effect that HLIS must process personal data lawfully and transparently while ensuring fairness in every aspect of data processing.

The second principle is that personal data should be collected for explicit, specified, and legitimate purposes and not processed further in a manner incompatible with the original purposes. Section 25 of the Act, which provides for purpose limitation with certain exceptions, explains the principle as an obligation to the data controller. Furthermore, Regulation 26 of the Personal Data Collection Regulation clarifies that before collecting data, the controller must specify the purpose and identify the legitimate reasons for collecting the data. The principle requires HLIs to collect personal data for specific, explicit, legitimate purposes and limit data usage solely for the purpose for which it was collected.

The third principle states that personal data should be relevant, adequate, and limited to what is necessary in relation to the purposes for which it is processed. Regulation 28 elaborates on this principle, requiring data controllers to avoid processing personal data in bulk. In implementing this principle, they should only process personal data that is relevant to the purpose. This implies that HLIs are obligated to minimise and limit the amount of personal information collected to only what is necessary for intended purposes.

The fourth principle is that personal data should be accurate and, if necessary, kept up to date. Section 24 of the PDPA provides this principle as an obligation to the data controller. It requires HLIs to ensure that personal data in their custody is accurate, complete, relevant, and not misleading, in accordance with its purpose. Regulation 29 requires the data controller, during processing, to verify the accuracy of the data with the data subject before and at various stages of processing. The HLIs are obliged to update personal data as necessary for the purpose and to erase or rectify any inaccurate personal data without delay. Similarly, the controller is required to utilise technological and design features to minimise inaccuracy.

Storage limitation is the fifth principle, also known as data retention. It requires the controller, when processing personal data, not to retain

personal information longer than necessary for the purpose. Section 28 of the PDPA requires personal data to be retained for a period specified in the relevant laws or regulations. However, the same section allows the minister responsible by regulation to prescribe the retention and disposal period in accordance with the purpose of retention. Moreover, Regulation 30 stipulates that the data controller is responsible for ensuring that they have clear internal procedures for deleting and destroying personal data. According to the provisions above, HLIs should be able to determine the nature and duration of storage of personal data which are necessary for the intended purposes, promoting responsible data management.

The sixth principle is that personal data should be processed in accordance with the rights of the data subject, as provided in the PDPA. It entails securely processing personal data to protect the rights and privacy of individuals while preventing the accidental loss or destruction of the same. Read this principle in conjunction with part VI of the PDPA, which outlines the rights of the data subject. The data subject is entitled to access their personal data and information regarding the processing's purposes, categories of personal data, recipients to whom the data is disclosed, and the duration of storage, as indicated by these provisions. Additionally, they are entitled to request rectification or erasure of their personal data or to restrict its processing. Additionally, they must be informed about automated decision-making, its underlying logic, and the potential repercussions of such processing. The data user's right to receive and freely transmit the personal data they have provided to a controller should be guaranteed. The data must be presented in a format that is machine-readable, commonly used, and structured. To comply with this principle, HLIs must specify the forms in which data subjects may request the exercise of their rights to fulfil those rights. Furthermore, it is necessary to establish procedures that outline the process for resolving requests from data subjects.

The right to access, as provided under Section 33, is a critical principle. It is the basis for exercising other rights, such as rectification, blocking, erasure, and destruction of personal data. Moreover, according to Regulation 31, this principle requires HLIs to grant the data subject an autonomous right and freedom to control their personal data, enabling them to communicate and exercise their rights. Additionally, the

controller is required to incorporate human intervention to minimise biases that the automated decision-making process may introduce.

Security is the seventh principle. It advocates for the use of appropriate technical and organisational measures to ensure the security of personal data against unauthorised or unlawful processing, destruction, or damage. Section 27 of the PDPA outlines detailed provisions for this principle. Regulation 27 states that this principle requires the controller to have effective methods for managing information security policies and to handle data processing that can adapt to changes, legal requirements, incidents, and cyberattacks. It also ensures that only authorised personnel can access the personal data they need for their tasks and that the transfer of personal data is protected from unauthorised access. Additionally, it is necessary to ensure that only authorised personnel have access to the personal data required for their processing tasks and that the transfer of personal data is secured against unauthorised access. This duty is also an obligation to HLIs.

The eighth principle is the international transfer of personal data. It states that personal data should not be transmitted to another country unless the target country provides adequate protection. This section should be read in conjunction with PDPA Part V, which outlines the international data transfer criteria. Regulation 22 establishes international criteria for the transmission of personal data. HLIs transfer data internationally through academic collaboration, international student recruitment, research partnerships, cloud computing, and digital education platforms. Section 45 of the PDPA prohibits data controllers and processors, including HLIs, from transferring personal data outside Tanzania without observing certain prescribed circumstances.

HLIs have major operational issues due to this principle. Foreign service providers of cloud-based platforms are essential for managing student information systems, virtual learning environments (e.g., Moodle or Google Classroom), and research data. Personal data, including names, academic records, contact information, and biometric or health data, is transferred to servers outside Tanzania. These transfers without PDPA compliance will result in administrative or judicial penalties for institutions. HLIs also collaborate with international institutions and funding agencies to provide sensitive data, including survey results,

patient information, and socioeconomic profiles. Tanzanian law requires data-sharing agreements to protect transferred data. Failure to follow these procedures constitutes a violation of data protection and ethical research protocols. International student data handling is also a major issue. Higher education institutions, foreign embassies, credential evaluation bodies, and scholarship givers need approval to transfer data. According to PDPA criteria, data transfer consent must be informed, freely granted, and revocable. Many institutions fail to implement these principles.

4.0 HLI's Compliance obligations stipulated under the PDPA

The PDPA establishes various compliance standards that HLIs must adhere to, given their roles as data controllers and data processors. The PDPA compliance requirements enable HLIs to meet legal obligations while protecting individuals' privacy rights. The appointment of a Data Protection Officer (DPO) is a crucial requirement under the PDPA for institutions. Section 34 of the PDPA delineates this requirement. The PDPA mandates that HLIs appoint a qualified DPO responsible for ensuring compliance with data protection regulations, conducting regular audits, advising on processing activities, and maintaining communication with the PDPC.

The PDPA mandates that all HILs adhere to the compliance requirements outlined in Section 65. The provision requires each data controller to establish and enforce a code of ethics or a personal data protection policy. All HLIs are necessary to establish a comprehensive data protection policy that adheres to the principles of the Act and aligns with their operational data handling procedures. Policies must be comprehensive, readily accessible, and subject to regular updates to ensure alignment with changes in legal standards, technological advancements, and operational procedures. The policy should encompass all aspects of personal data processing activities, including collection, storage, sharing, and retention.

Individuals have the right to access their personal data, request corrections and deletions, and object to data processing, as specified in Section 27 of the PDPA. All institutions are required to adhere to this rule as a mandatory compliance obligation. HLIs must implement transparent procedures that enable individuals to exercise their rights effectively. The establishment of comprehensive data protection policies, mechanisms for

digital rights compliance, the publication of privacy notices, and the creation of a dedicated privacy contact point are essential for meeting this requirement.

Many HLIs utilise cloud services for data storage and employ third-party systems for managing student records and conducting research analytics. Section 35 of the PDPA requires institutions to secure written data processing agreements from their processors, thereby enforcing compliance with the PDPA. Contracts must delineate data processing boundaries, outline data protection responsibilities, and define liability terms to mitigate unauthorised data breaches.

According to Section 32, HLIs are required to establish appropriate technical and organisational measures to protect personal data from unauthorised access, destruction, and unlawful disclosure. Minimum protection requirements encompass encryption methods, authentication systems, firewalls, backup procedures, and record-keeping logs. Institutions must conduct regular vulnerability assessments to remain responsive to emerging cybersecurity threats.

According to Section 33, the Data Protection Commission and affected individuals must be notified of breaches that jeopardise data subject rights within a 72-hour period. The establishment of effective internal reporting systems, breach response plans, and documentation protocols by HLIs is essential to meet legal obligations and reduce institutional risk.

Section 26 of the PDPA prohibits data controllers from retaining personal data beyond the duration necessary to fulfil the purpose for which it was originally collected. HLIs must implement clear data retention schedules that involve organising data into categories based on sensitivity and relevance, while also establishing secure protocols for data disposal. Retention of personal data must be confined to information that is essential for academic or administrative functions. Section 45 of the Act prohibits the international transfer of personal data to jurisdictions that do not meet the standards of adequate protection. The international data transfer regulations outlined in Section 45 of the Act are essential for HLIs due to their utilisation of foreign learning platforms and participation in international research collaborations. Standard contractual

clauses and binding corporate rules represent the sole permissible mechanisms for facilitating data transfers.

The data controller is required to implement internal compliance monitoring systems, as stipulated in Section 38, which encompass scheduled audits and risk assessment procedures. The PDPA requires HLIs to document their data processing activities, verify the legal bases for all data operations, and generate audit reports to demonstrate accountability. The compliance obligations outlined above can be fulfilled if the HLIs establish and implement policies and operational procedures for the protection of personal data. The policy standards serve as a road map to guide all other compliance obligations.

5.0 Discussion

The PDPA's introduction above clearly portrays HLIs as data controllers. Assuming the role of a data controller entails significant compliance obligations. The term also applies to any processor, individual, or agency engaged in data processing on behalf of the controller. They must be responsible for and able to demonstrate their compliance with the basic principles of data protection. The PDPA and its Regulations indicate that all personal data processing in HILs must be conducted lawfully, transparently, and fairly, with data acquisition limited to the minimum necessary for the intended purpose of processing. Moreover, personal data must be precise and maintained in a manner that allows for the identification of individuals only as long as necessary, while providing adequate security measures. The accountability principle mandates HLIs to assume responsibility and exhibit compliance.

Furthermore, significant advancements concerning consent necessitate that it should be provided freely and demonstrate a specific, informed, and explicit expression of the data subject's wishes.[15] PDPA expands the data subject's rights, and HLIs are duty-bound to comply with these rights when processing personal data. Besides the data subject rights, PDPA imposes enhanced obligations on data processors and controllers. For example, designing appropriate technical and organisational measures to ensure data protection, such as encryption, is required. In section 27(1), the PDPA sets out the concept of 'data protection by design and default.

[15] The Personal Data Protection Act, (n 13) s 30.

This is further elaborated in Regulation 24, where the controller is required to design technical measures to safeguard and implement the principles of personal data protection. The PDPA, in Section 14, requires all entities that collect or process personal data in Tanzania, including HLIs, to register with the PDPC. However, Section 21 of the PDPA excludes public institutions from registration requirements. This is to the effect that immediately after the Act came into force, all public institutions are deemed to be registered and hence required to comply with the PDPA.

The University of Dar es Salaam (UDSM) is a public institution that processes a large volume of personal data related to students, faculty, and staff. The compliance rate of this HLI was examined by reviewing various policies available in the UDSM library and on its website. According to the website, it was established that there is no privacy notice embedded, which is a necessary requirement to demonstrate compliance. Additionally, there is no robust data protection policy document aligned with the PDPA that is readily available at UDSM, either in hard copy in the library or as a soft copy on the website.[16] The absence of a data protection policy is contrary to Section 65 of the PDPA, which requires institutions to draw up and implement a code of ethics or policy for personal data protection. However, the University has several policies that pertain to privacy and data protection, such as the Acceptable Use of ICT Resources Policy[17] and the Security Policy.[18] The UDSM Community site also upholds a 2020 privacy policy that outlines the management of personal data on their platform.[19]

Upon reviewing these policies, particularly the Acceptable Use of ICT Resources Policy and the Security Policy, it is evident that they ensure the proper use of ICT resources and protect individuals, assets, and the university's reputation from potential threats. These policies are not

[16] University of Dar Es Salaam Privacy Policy, 2020 available at https://alumni.udsm.ac.tz/privacy-policy&ved=2
[17] University of Dar es Salaam Acceptable use of ICT Resources Policy, 2024 available at http://www.udsm.ac.tz/sites/default/files/2024-9/03%2UDSM%20ICT%20Security%20and20%Acceptable%20Use%20of%20ICT%20Resources.pdf.
[18] University of Dar es Salaam Security Policy and Operational Procedures, available at https://www.udsm.ac.tz/sites/default/files/2025-03/UDSM%2520SECURITY%2520POLICY.pdf&.
[19] University of Dar Es Salaam Privacy Policy, 2020 available at https://alumni.udsm.ac.tz/privacy-policy&ved=2

intended to protect personal data; hence, the absence of a proper policy implies that the University has not complied with the PDPA. Additionally, reviewing the privacy policy, which was adopted in 2020, prior to the enactment of the PDPA. Similarly, a privacy policy was adopted to protect the personal data of the UDSM community in compliance with the GDPR; hence, it cannot be said that it was adopted in compliance with the PDPA, as it was adopted long before the PDPA's enactment. The above explanation shows the absence of a privacy notice on the website and the absence of personal data protection and privacy policies that align with the PDPA at UDSM. This indicates that UDSM has not taken reasonable steps towards compliance with the PDPA.

The second higher learning institution whose policies were analysed is Sokoine University of Agriculture (SUA). While reading and researching different policies in the library and on the institutional website, it was established that in line with UDSM, SUA's institutional repository (SUAIRE) website contains a privacy statement.[20] It highlights that they collect and process personal data and provides the purposes for which this data is collected. Additionally, it outlines the circumstances under which they can disclose personal data in their possession. On the other hand, SUA has several other policies and guidelines, including the SUA Information and Communication Technology Policy (ICT Policy)[21], the SUA Intellectual Property Policy,[22] The Institutional Repository Policy,[23] and many others. Some of these policies include provisions for data privacy and security.

For example, the ICT policy has some provisions that incline towards privacy protection.
Still, the main objective of the policy is to mainstream ICT access and proper use to support teaching, learning, research, consulting, and outreach. An analysis of all these policies and guidelines reveals that the protection provided for personal data is minimal and does not comply

[20] Sokoine University of Agriculture Institutional Repository Privacy Statement, available at https://www.suaire.sua.ac.tz/info/privacy.
[21] Sokonie University of Agriculture Information and Communication Technology Policy, 3rd Edition, 2023, available at https://www.sua.ac.tz/sites/default/files/ictpolicy2022%20-%20march%2017%20(2)pdf.
[22] Directorate of Planning and Investment, Sokoine University of Agriculture Intellectual PropertyPolicy, 2002, available at https://www.dpd.sua.ac.tz/intellectual-property-rights-ipr-policy-2002/
[23] Sokoine University of Agriculture, Institutional Repository Policy, 2014 Available at https://www.lib.sua.ac.tz/phocadownload/suair.pdf.

with the provisions of the PDPA. This conclusion is implied by the fact that the basis of all these documents is not the PDPA but in fulfilment of other obligations. Also, the presence of a privacy statement signifies transparency; however, it does not ensure adherence to the PDPA unless it explicitly references the PDPA. Such statements are non-compliant with the PDPA as they are formulated without adherence to the law's stipulations and employ generic privacy terminology rather than the legal responsibilities pertinent to specific scenarios. The privacy statement on SUA's website provides general information regarding data collection and user rights. These statements do not demonstrate compliance unless integrated into a comprehensive PDPA-compliant data protection system.

The third HLI, whose policies and regulations were analysed for non-compliance, is the Open University of Tanzania (OUT). It is a public institution that processes vast amounts of personal data relating to students, staff and other stakeholders; hence, it is subject to PDPA. The analysis was conducted through reading different policies found in the institution's library as well as on the website. It was found that no privacy notice is provided for users on the website. However, a draft data protection policy has not yet come into effect. Moreover, it was established that the OUT has appointed a DPO, who is responsible for compliance procedures. It was also discovered that several other policies are available on the website, including the ICT policy.[24] the ICT security policy and procedures,[25] the gender policy,[26] the health policy,[27] and many others. However, none of these available policies is intended to provide for personal data protection practices in the university. This implies that, although the compliance rate is still minimal at the time of writing this article, the OUT has taken reasonable steps towards compliance with the PDPA, as evidenced by the appointment of a DPO and the development of a draft personal data protection policy and procedures.

[24] The Open University of Tanzania, Information and Communication Technologies Policy2019, Available at https://sso.out.ac.tz/custom/media/docs/intranet_doc_202208031107.pdf
[25] The Open University of Tanzania, ICT Security Policy and Procedures, 2022. Available at https://sso.out.ac.tz/custom/media/docs/intranet_doc_202406121103.pdf.
[26] The Open University of Tanzania, Gender Policy Towards Balancing OUT Community, 2021. Available at https://sso.out.ac.tz/custom/media/docs/intranet_doc_202208310114.pdf.
[27] The Open University of Tanzania, Health Policy, 2022. Available at https://sso.out.ac.tz/custom/media/docs/intranet_doc_202209011223.pdf

Another institution whose policies and regulations underwent an examination is Tumaini University Makumira (TUMA). This is a private university that collects and processes a significant amount of data from its stakeholders. Analysis of the policies in the library, as well as on the institutional website, revealed that the university website does not contain a privacy notice to inform its users about privacy and data protection. However, the website contains a number of policies, such as the ICT policy,[28] the data security policy,[29] the research ethics policy,[30] and the consultancy policy and procedures,[31] to name just a few. Several of these policies include provisions relating to data protection and general information security. For example, among the objectives of the data security policy is to establish a data security programme and processes for ensuring the security and confidentiality of confidential information. In addition, it intends to establish physical, administrative and technical safeguards to protect against unauthorised access or use of confidential information, which resembles, to some extent, one of the compliance requirements provided by the PDPA. However, the primary purpose of the policy is to protect confidential information, whereas the PDPA provides for the protection of an individual's data. Further, the policy intends to establish a security program and not protect personal information in line with data protection principles; hence, it is not in compliance with the PDPA.

Another policy that was examined is the ICT policy. This policy ensures that its users have access to best practices for the identification, protection, and management of available ICT resources. It ensures the security and privacy of the data stored, redirected, or processed by TUMA ICT resources. Though the policy purports to protect the privacy of data, it is too broad. It focuses on preserving all data, not just personal data. In addition, the protection may not be in line with data protection principles because, in its wording, it does not explicitly state that it has been amended to comply with the PDPA, despite being reviewed after the

[28] Tumaini University Makumira, Information and Communication Technologies Policy, 2023. Available at https://makumira.ac.tz/docs/ICT-Policy.pdf.
[29] Tumaini University Makumira, Data security Policy, 2020. Available at https://makumira.ac.tz/docs/ICT-Policy.pdf
[30] Tumaini University Makumira, Research Policy,2023. Available at https://makumira.ac.tz/docs/Research%20Ethics%20Policy-1.pdf.
[31] Tumaini University Makumira, Consultancy Policy and Procedures, 2024. available at https://makumira.ac.tz/docs/TUMA%20consultancy%20policy%20and%20procedures.pdf.

PDPA came into force. The discussion above clearly demonstrates that TUMA is yet to take sensible steps towards compliance with the PDPA.

6.0 Conclusion

Analysis of the compliance practices of various top HLIs reveals the following common trends. First, in these universities, there is no privacy and data protection policy covering the fundamental principles and practices of data protection posted on HLI's websites or available in their libraries. This is the exception of OUT, which has a draft personal data protection policy in place. It is challenging to determine how the HLIs collect and process personal data in this digital era, where data protection is of paramount importance, without a policy to that effect. Secondly, some of the HLIs understand the importance of privacy and data protection and have posted privacy statements on their websites.

However, the statement is posted in either an institutional repository or a community site, but not on the main website. Furthermore, some of the statements were made prior to the enactment of the PDPA and were not in compliance with it. For example, the statement on the UDSM community site explicitly states that it is made in line with the GDPR. Thirdly, the HLIs have different policies, some of which have provisions for data protection. However, the protection offered is too general and may not necessarily be categorised as personal data protection. For example, Tumaini University's data security policy protects confidential information, which may not necessarily include personal data. Fourth, it is unclear whether the institutions are registered with the PDPC as data controllers and processors, as required by law. It is imperative to note that the HLIs or the PDPC have not shared the information about registration status with the public. This problem may be due to the fact that the registration deadline (30 April 2025) had just ended when the article was being written. Fifth, except for the OUT in all other examined HLIs, it was not possible to determine whether the institutions, as data controllers, have appointed a DPO as mandated by law. The information to that effect is not shared with the public by either the PDPC or the institutions. From the above discussion, it can be submitted that the compliance rate in HLIs is very low and still in its infancy stage, and in some institutions, it is non-existent. The main reasons may stem from inadequate training and awareness campaigns on the importance of not only personal data protection laws but also compliance with these laws.

7.0 Way Forward

Despite the non-compliance practices and the reasons presented above, the article provides a fertile ground for encouraging compliance in HLIs. First, by highlighting the noncompliance, one may propose that the PDPC has to offer training and awareness campaigns to bring the law to society. Seminars, workshops, presentations, and leaflets can all help achieve this. Additionally, the commissioner should exercise his statutory powers and make bold decisions to enhance compliance from various organisations, including HLIs. In addition, the HLIs should comply with the law by registering with the PDPC as data controllers and processors, thereby legitimising data handling activities within their institutions. Furthermore, they should appoint a DPO who will oversee compliance with the PDPA. Further, HLIs should adhere to data protection principles and facilitate or grant data subject rights as required by the PDPA. Lastly, the HLIs should adapt data protection policies and procedures to ensure ongoing compliance.