Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 5, Issue 1 (2025) p.135-177
DOI: https:doi.org/10.52907/jipit.v5i1.544

From Privacy Safeguards to Innovation Barrier: Assessing Tanzania's Personal Data Protection Act in the Age of AI

Mark-Silas Malekela[*] *& Tupokigwe Isagah*[**]

ABSTRACT

The rise of digitization has led to the widespread adoption of Artificial Intelligence (AI) technologies, driving efficiency and innovation across sectors. AI systems rely on vast datasets to enhance accuracy, but their deployment raises concerns over data privacy, misuse, and bias. In response to the growth of technology and the collection of personal data, different jurisdictions have enacted data protection laws. This study focuses on Tanzania's Personal Data Protection Act (PDPA), which aims to regulate the processing of personal data, and critically examines its implications for AI implementation in Tanzania. This study analyses key provisions of the PDPA, such as restrictions on data sharing, privacy safeguards, and the role of Data Protection Commissions (DPCs) in comparison with global and regional data protection frameworks to assess their implications for AI implementation. Findings suggest that, while the PDPA is not an AI-specific law, its stringent data access controls and compliance burdens may limit AI-driven advancements. The study also highlights how excessive personal data restrictions can reduce AI accuracy and fairness, as models require diverse datasets for effective learning. The study recommends potential strategies Tanzania could adopt, including regulatory sandboxes and risk-based compliance approaches, to balance privacy protection with AI innovation. This study advocates for the adoption of AI-specific guidelines that promote 'privacy by design' in AI models and introduces flexible policies that support responsible AI implementation. While the PDPA establishes a crucial

[*] Government Liaison, Alistair Group, Dar es Salaam, Tanzania. LL. M in International Commercial Arbitration Law, Stockholm University, Sweden. Email: malekelamark@gmail.com

[**] Ph.D. in Information Systems Management, Koblenz University, Germany. Lecturer, Mzumbe University, Morogoro, Tanzania. Email: timwalukasa@mzumbe.ac.tz

framework for data governance in Tanzania, its applicability requires continuous assessment to prevent unintended barriers to AI growth.

Keywords: Artificial Intelligence, Data Regulations and AI, Data Protection Act, Data Protection vs. Innovation, Data Access

TABLE OF CONTENTS

I. INTRODUCTION

Digital transformation initiatives have improved operations across both the public and private sectors. Digital transformation enables organizations to gather, store, and share data through digital platforms, thereby increasing the availability of digital data. As a result, numerous organizations are adopting data-driven technologies, such as the integration of Artificial Intelligence (AI) technologies, to enhance their operations and service delivery (Wamba-Taguimdje et al., 2020; Ben Dhaou et al., 2024). AI has gained considerable attention in this regard due to its potential to introduce new business processes that were previously unattainable with conventional technologies (Wamba-Taguimdje et al., 2020). AI contributes to better decision-making, for example, through prediction and recommendation capabilities (Ben Dhaou et al., 2024). As such, organizations can use the technology to monitor and forecast various conditions, enabling timely planning and interventions (Thekdi et al., 2022).

On the one hand, AI has demonstrated the potential to address local challenges and promote resilient, sustainable communities in Tanzania. For example, AI technologies can enhance food security by managing crop growth and recommending to farmers favorable agricultural practices based on the local context (Wamba-Taguimdje et al., 2020). Similarly, existing technologies such as Afya Intelligence provide communities with equitable access to quality health care by leveraging data and AI (Afya Intelligence, 2025).

On the other hand, the accuracy of AI systems depends on data quality, and it improves with increased data availability and representation (Harrison et al., 2019). AI systems rely on data to learn, adapt, and improve performance, thereby further enhancing AI's trustworthiness (Alzubaidi et al., 2023). Thus, data quality and fair representation are significant factors in responsible AI. As a result, practitioners strive to enforce data governance and regulations to support the responsible use of

data in data-driven technologies. Since personal information is a significant part of the data used by AI systems, governments and regulatory bodies have developed legal frameworks to standardize data collection, processing, and use. Some of these legal frameworks further prohibit data misuse to reduce biased data usage that may discriminate against specific groups. For example, Tanzania introduced the Personal Data Protection Act (PDPA) in 2022 to protect personal data and enhance data privacy rather than governing data towards AI implementation. The PDPA was enforced in 2023 and is overseen by the Data Protection Office, established in May 2023.

While some existing data regulations contribute to ethical and user-centric AI systems (Schuett, 2023), they do not explicitly govern the use of AI. Also, such laws can restrict innovation and technology within organizations due to limited data availability or friction in data accessibility. This is also the case in Africa, where strict consent requirements or data localization rules in many jurisdictions can prevent developers from accessing the large, diverse datasets needed to train effective AI models (Chen et al., 2024).[1] Thus, there is a need to explore the impact of existing data regulations on AI implementation, balancing innovation and data governance for sustainable development.

Although the PDPA in Tanzania was not designed with AI governance as its primary objective, its focus on the protection of personal data nonetheless functions as a *de facto* regulatory framework for data processing in AI applications. The absence of explicit AI-related data guidelines creates legal and compliance uncertainty for organizations seeking to implement AI-driven solutions, thereby constraining innovation under a privacy regime not tailored to emerging technologies.

[1] Data localisation refers to laws or regulations that require personal data to be stored, processed, or handled within the borders of a specific country or jurisdiction. These laws typically prohibit or limit the transfer of certain types of data (especially data with national significance or sensitive data) outside the jurisdiction. A major effect of localisation rules is restricting cross-border data flows, which can in turn limit access to diverse or large datasets (especially important for training AI models).

The central regulatory tension arises from the structure and requirements of the PDPA, which, although designed primarily to safeguard personal data, may now function as the principal legal instrument governing data processing in AI systems. This creates a concrete and immediate problem, as the PDPA imposes strict obligations regarding consent, purpose limitation, data minimization, cross-border transfers, and automated processing. Yet, it does not provide AI-specific safeguards, guidance, or supervisory mechanisms. As a result, the PDPA may unintentionally constrain access to large datasets needed for training AI models, create uncertainty for developers, and expose organizations to compliance risks. This tension is presently more concerning because the government of Tanzania is simultaneously introducing AI governance mechanisms, such as the national AI strategy, which is under development; the education sector has established guidelines for using AI in education; and the health sector guidelines aim to govern AI implementation in the health sector.

This paper focuses on the PDPA because, in the absence of a dedicated AI legislation or binding AI-specific regulatory instruments in Tanzania, the PDPA currently provides the only enforceable legal basis applicable to AI systems that process personal data. Continental and national AI initiatives remain non-binding, meaning that, while they guide strategic alignment, they do not impose operational obligations on AI developers in the Tanzanian context. In light of this regulatory gap, the PDPA represents the functional regulatory anchor for AI innovation today, setting the compliance parameters within which AI developers and regulators must operate until further national legislation or guidelines are adopted.

Recent domestic efforts also underscore this regulatory gap. Tanzania has signaled interest in developing a national AI strategy through participation in AU capacity-building forums, the establishment of digital innovation clusters at the Tanzania Commission for Science and Technology (COSTECH), and

the inclusion of AI within the 2023–2027 National ICT Policy Review consultations (Ministry of Information Communication and Technology, 2023). However, no consolidated national AI strategy, regulatory sandbox, or statutory framework has been formalized. This transitional policy environment reinforces the relevance of examining the PDPA. Whatever national AI strategy eventually emerges will need to align with the PDPA's principles—unless the legislator expressly provides otherwise. At the same time, the absence of dedicated AI guidance increases uncertainty around the interpretation of PDPA provisions when applied to algorithmic systems, potentially slowing innovation by limiting developers' confidence in regulatory expectations.

Continental AI strategies create directional pressure and shape future policy expectations, but the PDPA almost exclusively shapes Tanzania's immediate AI governance landscape. This dual reality highlights both the opportunity for alignment with African AI principles and the need to clarify how the PDPA can accommodate emerging AI use cases without stifling responsible innovation. This analytical lens enables the evaluation of regulatory requirements and their practical impact on the AI innovation environment in Tanzania.

Thus, this paper aims to contribute to the body of knowledge by assessing the impact of the PDPA on AI innovation in Tanzania. To achieve this objective, this paper adopts a doctrinal and comparative analytical method to examine how the PDPA's provisions— most relevant to AI such as consent requirements, data minimization, purpose limitation under Sections 25; limitations on disclosure of personal data under section 26; and automated decision-making safeguards under Section 36,— may inadvertently support or constrain AI innovation, or create compliance burdens that may limit AI systems' ability to process and learn from diverse datasets, hence affecting model accuracy and fairness. Therefore, this paper explores whether the PDPA incorporates mechanisms that could facilitate experimental AI development within a compliant framework. It further evaluates

the implications of each phase, such as data collection and processing, on AI design choices, including model training, transparency, and algorithmic fairness.

To achieve this aim, this paper draws comparative insights from the General Data Protection Regulation (GDPR), the European Union's Artificial Intelligence Act, and regional African data protection regimes to assess whether Tanzania's regulatory approach aligns with emerging international standards. The paper also incorporates policy analysis drawn from the AU AI Strategy (African Union, 2024) and evolving national efforts, including Tanzania's ongoing work toward a national AI strategy and the development of sectoral guidelines in education and health.

The remainder of this paper proceeds as follows: Part II explores the evolving relationship between privacy and AI, highlighting the inherent tension between promoting innovation and protecting fundamental rights. It also discusses Tanzania's policy efforts and ongoing struggle to strike this balance. Part III provides a detailed analysis of how the PDPA may inhibit AI development in Tanzania by imposing strict data access controls, lacking AI-specific safeguards, and creating regulatory uncertainty. Part IV offers practical recommendations, such as introducing regulatory sandboxes, adopting privacy-by-design (PbD) frameworks, and enhancing institutional guidance that could help recalibrate the law to support responsible innovation. Part V concludes the paper by synthesizing key insights and reaffirming the need to reform Tanzania's data governance regime to create a more enabling environment for AI.

II. INTRICATE INTERACTIONS BETWEEN PRIVACY LAWS AND AI

Globally, researchers and practitioners emphasize the importance of designing and deploying innovative, responsible AI. This ensures that developed solutions do not harm communities. Responsible AI involves the planning, design, and continu-

ous regulation of AI to promote human rights and fairness and to create better societies (Adeleke & Akinwale, 2024). It is also referred to as an approach where the lifecycle of an AI system must be designed to uphold, if not enhance, a set of foundational values and principles, including internationally agreed-upon human rights frameworks and Sustainable Development Goals (SDGs), as well as ethical principles such as fairness, privacy, and accountability (Adeleke & Akinwale, 2024).

A key milestone in pursuing responsible AI is the development of legal and policy instruments, such as the EU AI Act, which governs accountable design and deployment of AI systems across the EU (The EU AI Act, 2024). While this paper draws extensively on the EU AI Act as a maiden and comprehensive AI-focused framework, legal clarity, and direct relevance to data protection regimes modelled on the GDPR, it is also important to situate Tanzania within broader African AI governance developments. Africa has recently taken significant steps toward formalizing AI governance, most notably through the AU Continental AI Strategy, which articulates ethical principles, data governance standards, and innovation priorities for member states. However, unlike the EU AI Act, the AU AI Strategy remains a non-binding policy instrument. It does not offer the detailed regulatory architecture needed to analyze specific legal impacts on AI development. For this reason, the EU AI Act serves as the primary comparative benchmark in this paper, while the AU Strategy provides useful regional context, illustrating Africa's emerging normative direction.

While there are various approaches to responsible AI—such as ethical guidelines and responsible AI frameworks—governments, data protection authorities, and international organizations are exploring data governance. Several countries, including those in Africa, are increasingly treating data protection as a foundational tool for achieving responsible AI. This involves regulating the data lifecycle, which encompasses the entire process of data collection, storage, use, sharing, and ultimately

deletion or anonymization (Adeleke & Akinwale, 2024). Among the notable initiatives in Africa is the introduction of data protection laws that regulate the entire data lifecycle, including collection, storage, sharing, and deletion, even in AI contexts. This trend reflects a growing recognition that strong data governance is critical to ensuring AI systems operate in ways that are lawful, transparent, and accountable, especially when personal data is involved. As scholars have noted, this data governance approach is particularly important because AI is often intrusive and raises serious privacy concerns that must be addressed (Salami, 2024).

Therefore, regulatory developments in the EU set the tone for promoting responsible AI. This is because the EU AI Act prohibits the use of AI for potentially harmful purposes, and it sets out varying obligations depending on the risk level of the AI system or technology. It includes transparency requirements for the disclosure of training data for providers of AI technologies while facilitating innovation.

A. Data Regulation and AI

The dual effects of data privacy laws on AI include opportunities to build user confidence and promote ethical AI practices. Nonetheless, they also come with high compliance costs and operational difficulties. The massive amount of data generated by the internet and connected devices has increased the use of data-driven technologies in organizations, closely linking data and AI. AI systems rely on vast quantities of accurate, complete, representative, and quality datasets to train, test, validate, and improve the system. The increasing use and processing of such datasets raise many privacy challenges, including issues related to collection, standardization, anonymity, transparency, data ownership, and changing conceptions of informed consent (Adeleke & Akinwale, 2024). These privacy-related gaps can also have downstream effects. For instance, when inadequate transparency or flawed data-collection practices lead to biased data-

sets, AI systems may generate discriminatory outputs, raising both ethical and regulatory concerns under data protection law.

A frequently discussed principle of responsible AI is 'Privacy', which directly links to data privacy. Privacy concerns often arise in relation to how AI processes data (Alzubaidi et al., 2023). Among the privacy concerns inherent in the responsible use of AI are the use of big data analytics, issues surrounding transparency and accountability, and potential biases in decision-making processes (Hennemann, 2024). Mostly, end users are unaware of the amount and scope of personal data that AI systems access because they lack an understanding of how thoroughly these systems evaluate their data. Responsible AI principles such as transparency and explainability, fairness and non-discrimination, human oversight, robustness, and data processing security are often linked to personal rights and relevant privacy laws (Hennemann, 2024).

Also, integrating datasets may result in personal identification, which raises concerns about confidentiality and privacy (Malekela, 2025). Thus, the processing of personal data should adhere to general privacy standards, which form the basis of privacy and data protection. This entails guaranteeing restrictions on data collection, data quality, purpose specification, use limitation, accountability, and individual (human) involvement—human oversight.

African countries are increasingly enacting data protection laws to safeguard personal data and ensure responsible data use. Notable examples include South Africa's Protection of Personal Information Act (POPIA, Act No. 4 of 2013) and Kenya's Data Protection Act (DPA, 2019). These instruments represent the African continent's efforts to align with global trends in establishing comprehensive legal frameworks for data governance. Common components across these data protection laws include principles of lawful and fair processing, requirements for obtaining informed consent, the establishment of data protection authorities, provisions on data subject rights, and rules

on cross-border data transfers. Also, a key shared feature is the emphasis on transparency and accountability in data handling (Alzubaidi et al., 2023).

However, while these regulations are essential for protecting individual rights, they can also pose innovation challenges, particularly in emerging fields like artificial intelligence. Strict data localization rules, burdensome consent requirements, or ambiguous provisions can hinder the availability of data for training AI models or delay AI deployment and improvement (Alzubaidi et al., 2023). In response, some countries, such as Norway, Singapore, and Spain, are adopting flexible mechanisms, including regulatory sandboxes, phased compliance models, and innovation charters, to balance data protection with the need for technological advancement (Alzubaidi et al., 2023).

Tanzania has not yet issued sector-specific directives or interpretive guidance from the Personal Data Protection Commission (PDPC) to clarify how AI developers may lawfully process or share personal data for machine learning. Consequently, organizations exploring AI solutions across sectors such as health, agriculture, finance, and justice must navigate a framework primarily designed for traditional data processing. This framework is ill-suited to the high-volume, iterative, and cross-institutional data use that AI systems require.

The GDPR emphasizes the need for express consent, openness, and accountability while imposing strict restrictions on data collection, processing, and storage. Comparably, the California Consumer Privacy Act (CCPA, 2018) gives Californians more authority over their personal data and requires companies to protect data security and privacy. While the GDPR introduces mechanisms, such as regulatory sandboxes and accountability frameworks that can support responsible AI innovation, it simultaneously sets high compliance thresholds (Baldini & Francis, 2024).

A thorough assessment of how these privacy frameworks affect AI technology is therefore required. For example, the GDPR's strict criteria and significant effects on data-driven technologies, such as AI, were outlined in a thorough review of the law by Voigt and Von dem Bussche (2018), who highlighted the legal challenges posed by requirements such as data minimization, transparency, and informed consent. These features, while crucial for protecting fundamental rights, present formidable obstacles for AI developers who rely on large, often repurposed datasets for training machine learning models.

Similarly, Wachter, Mittelstadt, and Floridi's (2016) investigation into the ethical implications of the GDPR on AI focused on the 'right to explanation'. This criterion emphasizes the need for interpretability and openness in AI, sparking a body of research on explainable AI (XAI) techniques. To illustrate the trade-off between model complexity and transparency, Doshi-Velez and Kim (2017) examined several techniques to improve the interpretability of AI models. These techniques include model-agnostic approaches such as Local Interpretable Model-Agnostic Explanations (LIME) and Shapley Additive Explanations (SHAP), which generate human-understandable explanations for complex models by identifying which input features contributed most to a particular decision. They also discuss intrinsically interpretable models such as decision trees, sparse linear models, rule-based systems, and generalized additive models (GAMs), which prioritize transparency by design.

However, as Schuett (2023) also argues, a significant and persistent problem that calls for creative solutions and significant expenditures in technology and training is data anonymization. One important tactic for balancing regulatory compliance and AI innovation is the use of privacy-preserving methods such as federated learning, which enables AI models to be trained across decentralized devices without transferring raw data, and differential privacy, which introduces statistical noise into datasets to protect individual identities while enabling useful analysis. By

using these strategies, businesses can continue to exploit large datasets for model training and improvement while maintaining user privacy, as required under data protection law regimes.

Ethical AI would require adapting data protection standards and ethics to innovations and the implementation of AI systems. Since Tanzania currently lacks an AI-specific regulatory framework, ethical principles become even more crucial in guiding the responsible use of AI technologies. The literature suggests that ethics will become essential for regulating data protection in the absence of sufficient legislation (UNESCO, 2023). For example, in the EU, the 2019 Ethics Guidelines for Trustworthy AI preceded binding legislation and influenced compliance practices well before the AI Act. Similarly, African countries such as Mauritius have taken steps to modernize their digital ecosystems. They have issued a blueprint to develop a national AI Strategy, establish an AI Unit, implement ethical AI policies, and integrate AI into public services before legal reforms (UNESCO, 2023). An appeal to the moral compass of data controllers and processors to adhere to the minimal principles of data protection legislation, because it is the right thing to do, is equivalent to an appeal to adopt ethics in the regulation of data protection in AI systems (Luciano et al., 2016).

In Tanzania's case, the PDPA provides general data protection conditions, including lawfulness, fairness, transparency, and purpose limitation, but does not explicitly address ethical risks unique to AI systems, such as biased training data, opaque automated decision-making, or discriminatory outcomes. Therefore, the operationalization of 'responsible AI' in Tanzania would currently depend heavily on voluntary ethical commitments by AI developers and data controllers. Ethical frameworks help ensure that, even in the absence of AI-specific statutory duties, organizations integrate fairness assessments, risk-impact evaluations, and human oversight mechanisms when processing personal data through AI.

B. AI Implementation in Tanzania

Digitalization of public services in Tanzania has led to the massive availability of data that can be used to develop AI systems. Also, there is a significant increase in investment in internet and computing resources in Tanzania, which is promoting the availability of data (Freye et al., 2020). Tanzania is actively embracing AI technology, propelled by both government and private-sector innovation to tackle urgent socioeconomic issues and position itself for a future in the digital economy. For example, in the health sector, AI-powered chatbots are being used by startups like Elsa Health to increase healthcare, particularly in rural areas where there is a shortage of physicians and medical personnel. In agriculture and forestry, AI-powered chatbots are being used to hive youth and farmers with pertinent information about managing crops and forests in the climate change era (Sahara Ventures Report, 2024).

Additionally, the Tanzanian Judiciary has incorporated AI through a new transcription and translation system to improve court efficiency and processes, reducing the workload on judges and magistrates (The Citizen, 2024; The Chanzo, 2024). It has also been reported that eleven courtrooms have been equipped with an AI-powered transcription and translation system, with plans to scale it further (Robert, 2024). This AI integration is part of Tanzania's efforts to integrate Information and Communication Technology (ICT) systems into the judicial system, enabling lawyers and clients to track the progress of cases.

Despite the AI initiatives in Tanzania, such as the Judiciary's deployment of AI-powered transcription and translation tools, the use of AI chatbots like *Dr. Elsa* in the health sector, AI-driven agritech platforms providing climate and crop-advisory services, and the government's ongoing efforts through the Ministry of Information, Communication and Information Technology to draft a National AI Strategy, regulatory and

governance challenges remain (Global Partnership for Sustainable Development Data, (2023).[2]

III. THE INHIBITION OF AI INNOVATION UNDER THE PDPA

Beyond setting general obligations, the PDPA includes data protection principles like the right to explanation – Section 33 (1) (c), the fairness principle – Section 5(a), human oversight – Section 36 (1), and security of processing data – Section 27.

Section 33 (1) (c) of the PDPA requires a data controller to inform a data subject of the logic involved in automated decision-making for the purpose of evaluating the data subject. This provision implies that a data subject has a right to an explanation when automated decision-making means (including AI) is used. For example, where an AI recruitment tool screens resumes and scores candidates based on criteria such as education, experience, and keywords. A candidate whose application is rejected might request to know the logic behind the AI's decision (Wachter, et al., 2017).

The fairness principle in Section 5(a) obliges data controllers to ensure that processing, including AI-based profiling, does not result in discrimination or unjustified harm. The PDPA provides for the human oversight principle under section 36(1), which gives a data subject the right to request a data controller to ensure that any decision taken by or on behalf of the data controller, which significantly affects the data subject, is not based solely on the processing by automatic means. For example, an AI system used for hiring decisions analyzes candidates' resumes and ranks them for interview shortlisting. If the AI bases its decisions solely on algorithms without human review, it risks unfairly rejecting candidates due to bias in the training data

[2] In 2018, the Government of Kenya established the Distributed Ledgers Technology and Artificial Intelligence Taskforce which provided recommendation on how the Government can leverage new technologies in Kenya.

(e.g., favoring certain demographics). Under section 36 (1) of the PDPA, a data subject (candidate) could request the employer to ensure that decisions about hiring or rejection are reviewed by a human to account for unique qualifications or context that the AI might overlook.

The PDPA provides for data ownership, transparency, and the rights of data subjects, which can serve as a lawful basis for responsible AI usage. By recognizing individuals' control over their data, mandating clear information on data processing, and granting enforceable rights to access, correct, or delete personal information, the PDPA compels AI developers to ensure accountability, fairness, and transparency in algorithmic decision-making. Consequently, compliance with the PDPA is not only a regulatory requirement but also a practical mechanism to foster trust in AI systems operating within Tanzania. Similar privacy laws in other jurisdictions, such as the EU's GDPR, China's Personal Information Protection Law (PIPL), and the UK's Data Protection Act (DPA), include provisions related to these responsible AI principles (Marengo, 2023). From a comparative context, these data protection laws show that Tanzania's PDPA aligns with international standards that link data protection to transparency, fairness, and accountability in AI deployment.

Under PART IV, the PDPA outlines the conditions for processing personal data. These conditions are not responsible for AI principles themselves but closely resemble AI principles, as discussed above. In the context of the deployment of innovative and responsible AI, the PDPA establishes that for the processing of personal data to be lawful, such personal data must be collected for explicit, specified, and legitimate purposes and not further processed contrary to those purposes by the respective AI companies or developers. The PDPA also requires that personal data be accurate and kept up to date, and that it be corrected or deleted without delay when inaccurate, and that it be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Most importantly, pursuant to section 30(1) of the PDPA, the processing of sensitive personal data is prohibited without the data subject's written consent, and a data subject may withdraw their consent at any time. However, it should be noted that, as ruled in the *Tito Magoti v. the Attorney General* case (Misc. Civ. Case No. 18 of 2023), the High Court of Tanzania acknowledged the ambiguous and unclear nature of certain provisions under the PDPA, particularly those relating to lawful surveillance, consent, and the limits of personal data collection. The Court held that the law, as currently drafted, lacks sufficient clarity and precision to meet constitutional standards for legal certainty and the protection of fundamental rights. In the absence of legislation specifically regulating AI systems and technologies in Tanzania, this legal ambiguity raises further concerns about how existing PDPA provisions might be consistently applied to AI-related data processing, particularly where automated decision-making or large-scale data aggregation is involved. The PDPC has not yet issued any regulatory guidance or sector-specific directives on how to interpret or apply the PDPA in the context of AI systems. Tanzania has yet to establish authorities or oversight mechanisms mandated to regulate AI. This regulatory gap contributes to the prevailing uncertainty about how organizations deploying AI technologies should navigate issues such as consent, data sharing, and automated decision-making under the current legal framework.

A. Automated Decision in AI Systems and Protection of Personal Data

AI systems can make automated decisions that affect data subjects' rights and liberties, raising issues under data protection laws (Pasipamire et al., 2024). AI algorithms may be trained to evaluate the personal information of data subjects and determine their eligibility in a variety of contexts, including job and loan applications and e-government services (Pasipamire & Muroyiwa, 2024). In respect of automated decision-making, the

PDPA, read together with the Personal Data Protection (Personal Data Collection and Processing) Regulations (the Regulations), prohibits decisions made solely by automated means that affect the rights and freedoms of data subjects. Human oversight becomes essential for the lawfulness of automated decisions under the PDPA and the Regulations (Pasipamire et al., 2024).

Essentially, Section 36 of the PDPA provides a right in relation to automated decision-making, mandating data controllers and data processors to notify data subjects of decisions based solely on automated processing. Data subjects can request a review of the decision or a new decision that is not based solely on automated processing. The provision underscores the importance of human oversight and accountability in decisions significantly affecting data subjects when automated processing, such as in AI systems, is employed. It emphasizes protecting data subjects from the risks of unchecked automation by allowing them to challenge such decisions and ensuring transparency about the decision-making process involving an AI (Salami, 2024; Marengo, 2023).

Section 36(1) of the PDPA grants data subjects the right to demand that significant decisions affecting them are not based solely on automated processing (Personal Data Protection Act, 2022). In the same line, human involvement and evaluation of automated decisions prior to their adoption are very crucial, as human review can lessen or eliminate any prejudice or discrimination that can arise from using engineers or training data that are not representative (Bygrave, 2020). Section 36(2) of the PDPA further strengthens safeguards by requiring data controllers to notify data subjects when a decision is based solely on automated processing. This obligation ensures transparency, allowing individuals to understand how their personal data has been used in making such decisions. Additionally, the right to request a reconsideration introduces an essential layer of human intervention, ensuring that AI-generated outcomes are validated for fairness, accuracy, and contextual relevance.

Based on the foregoing, Section 36 of the PDPA provides that individuals have the right not to be subjected to decisions based solely on automated processing, including profiling that significantly affects them. However, Section 36 (3) introduces important exceptions to this rule. These exceptions allow automated decision-making where: (a) it is necessary for entering into or performing a contract; (b) a written law authorizes it; or (c) the data subject has explicitly consented to such processing. While these exceptions align with international standards, such as Article 22 of the GDPR, they warrant careful interpretation to prevent misuse. This is because their presence does not address or remedy the structural gaps identified earlier in this paper in relation to AI development and governance in Tanzania. In particular, the contractual necessity and consent-based exceptions do not provide substantive guidance on how AI systems should be designed, audited, or monitored to ensure fairness, transparency, and accountability.

In practice, AI services in sectors such as fintech, health, or digital public services frequently rely on standard-form contracts or bundled consent mechanisms, raising concerns that individuals may formally 'consent' to automated decision-making without meaningful understanding or real choice. Moreover, the exception for authorization by written law may be of limited practical value given the absence of any AI-specific legislation or detailed statutory standards governing automated decision-making in Tanzania. As a result, Section 36(3) functions primarily as a permissive clause rather than a regulatory framework for responsible AI use. It allows automated decision-making but does not impose affirmative obligations, such as explainability requirements, impact assessments, or risk-based safeguards, that are necessary to support trustworthy and innovative AI systems. Consequently, while the exceptions prevent an outright prohibition of automated decision-making, they may not fill the broader regulatory gaps identified in this study and therefore fall short of enabling a coherent and responsible AI development ecosystem under the PDPA.

It follows that the PDPA underscores the importance of transparency and accountability in the processing of personal data, which extends to AI systems. A key aspect of this requirement is the explainability of AI tools, ensuring that individuals understand how AI-driven systems make decisions that affect them. While the PDPA does not explicitly use the term 'explainability,' its principles of transparency, lawful processing, and data subject rights implicitly necessitate that AI tools provide comprehensible explanations, particularly when automated decision-making is involved.

However, in many cases, even AI developers struggle to explain how deep learning models arrive at specific outcomes fully. This creates a compliance dilemma; how can AI systems in Tanzania be made transparent enough to satisfy the PDPA's standards without compromising the efficiency and competitive advantage that complex AI models offer? To address this question in a more structured manner, a comparative perspective from a limited set of primary comparators, namely the European Union (as a global normative anchor on data protection), Kenya, and South Africa (as Tanzania's closest regional and regulatory peers), provides useful insights into the regulatory approach to AI explainability. Under the GDPR, Article 22, supported by regulatory guidance from the European Data Protection Board (EDPB), establishes the right for individuals not to be subject to solely automated decisions that significantly affect them unless they receive meaningful information about the logic involved, as well as the significance and consequences of such processing. This has prompted European AI developers to incorporate explainability features into their systems to meet transparency and accountability requirements.

Techniques such as decision trees, rule-based systems, and Shapley Additive Explanations (SHAP) values are used to provide interpretable outputs. Decision trees operate by breaking down decisions into a flowchart-like structure. Each internal node represents a test on an attribute, and each leaf node represents an

outcome. This allows users to trace how a particular conclusion was reached. (Durdymyradov et al., 2024). Rule-based systems rely on explicit 'if – then' rules derived from domain knowledge or data patterns, making the logic of the system transparent and auditable (Liu et al., 2015). SHAP values, on the other hand, quantify the contribution of each feature, for instance, income, age, or education, to a specific prediction made by the model, thus enabling developers and data subjects to understand which inputs were most influential in driving an automated outcome (Hassanien et al., 2025).

When these EU insights are viewed alongside Tanzania's regional peers, such as Kenya's Data Protection Act (DPA) and South Africa's Protection of Personal Information Act (POPIA), a similar limitation is witnessed. Despite Kenya's DPA recognizing that every data subject has a right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning or significantly affects the data subject (Data Protection Act, 2019), there is limited guidance on its operationalization. However, the Office of the Data Protection Commissioner has issued interpretive guidance for digital credit providers (Guidance Note For Digital Credit Providers, 2023), which provides some practical notes on profiling and automated decision-making, clarifying how consent, transparency, and human intervention should be applied in practice. As for South Africa, POPIA does not explicitly grant a right to an explanation, leaving uncertainty about how data subjects can meaningfully contest or understand automated decision-making. (Novazi, 2025).

Next, this paper analyses responsible AI principles applicable to the design, development, and deployment of AI solutions, with consideration of the PDPA.

B. Responsible AI Use and Its Relevance to Data Privacy Principles

The concept of responsible AI ensures that AI systems operate in an ethical, transparent, and rights-aligned manner, including privacy. Data privacy principles serve as the foundation for responsible AI deployment, governing how personal data is collected, processed, and used in AI-driven systems. Without adequate safeguards, AI systems may contribute to privacy violations, discrimination, and security risks, undermining public trust and regulatory compliance. The PDPA incorporates key privacy principles, such as data minimization, transparency, and certain data subjects' rights, all of which play a crucial role in shaping responsible AI practices. However, the extent to which these principles foster AI innovation or hinder its growth remains a subject of debate.

1. Data Minimization

Sections 22(2), 25, 26, and 30 of the PDPA illustrate how the principle of data minimization emphasizes collecting only the data necessary for the intended purpose. Data Controllers are encouraged to limit the scope of data collection to what is essential for the specified processing activities. AI systems are prone to collecting more personal data than necessary for any processing activity. This principle does not require reducing data collection to an absolute minimum, but seeks to reduce it to the lowest possible level in relation to the purpose of processing. Therefore, data minimization, as required under the PDPA, is essential to ensure AI-powered solutions are designed and applied with privacy protections to exclude unrelated data.

While the data minimization principle aligns with privacy protection, it may also create challenges for AI systems that rely on large, diverse datasets for training and improving accuracy. As a result, unlike the PDPA, some data regulations, such as the European Union's GDPR, balance data minimization with the legitimate interests of AI developers by allowing anonymized and

pseudonymized data processing (Article 6 GDPR). Article 6(1)(f) of the GDPR permits processing based on the data controller's legitimate interests, provided that it does not override the rights and freedoms of the data subject. Additionally, Recital 26 of the GDPR further clarifies that truly anonymized data falls outside the scope of the GDPR. At the same time, Article 4(5) defines pseudonymization as a safeguard measure that can support lawful processing and reduce privacy risks. This approach enables AI innovation while mitigating risks associated with personal data exposure.

2. Transparency and explainability

Transparency is another cornerstone of responsible AI. The transparency principle generally requires organizations to inform individuals about their individual rights and how they can assert them vis-à-vis the organization's services. The principle of transparency, embedded in both the PDPA and GDPR as a global standard regulation, requires data controllers and processors to provide clear information about how personal data is collected and processed in AI-driven systems (Section 5, Personal Data Protection Act, 2022; Art. 12, General Data Protection Regulations, 2018). The challenge, however, lies in implementing explainability mechanisms that make AI decision-making comprehensible to non-technical users. Transparency principles can be challenging in the AI context. Developers may limit disclosure of data sources to protect trade confidentiality and innovation. Additionally, the general-purpose nature of models makes it impossible for developers to enumerate all potential beneficial uses in advance.

In the European context, the EU AI Act (Regulation (EU) 2024/1689 – EU AI Act) complements the GDPR by emphasizing explainable AI, ensuring that automated decisions affecting individuals are understandable and can be challenged. African jurisdictions, including Tanzania, already contain legal safeguards against harmful automated decision-making. However,

what remains lacking in most African contexts is the operationalization of these provisions. There are few, if any, sector-specific guidelines, implementation frameworks, or institutional mechanisms that clarify what constitutes 'meaningful human involvement' or how data subjects can practically challenge algorithmic outcomes. Therefore, while the legal basis exists, the absence of complementary AI-specific regulations or enforcement tools raises concerns about the practical accountability and transparency of AI-driven decision-making in the region.

Also, as described in the Centre for Information Policy and Leadership (CIPL)'s 2024 publication, many AI developers have released explanatory documents (e.g., model or system cards and technical reports) to make AI models more transparent. These documents can include details about the AI model's construction, evaluation, mitigations, operation, types of data it was trained on, intended use cases and contexts, key limitations, and performance metrics. The report also buttressed that such documents should, if feasible and appropriate, also include metadata on the key attributes of the categories of personal data used in model training (for instance, what types of data are included in the dataset, where and how the data was collected, and which demographic groups are represented within it). Additionally, they ought to disclose the steps taken to reduce reasonably foreseeable risks.

Ultimately, laws and regulations should carefully balance transparency and data minimization principles.

3. Data Subject Rights

Part VI of the PDPA provides data subjects with rights, including the right to access their personal data, correct inaccuracies, and request deletion under certain circumstances. The PDPA details these rights and how individuals can exercise them under PART VI. The analysis of the rights in relation to AI is as follows:

i). The right to be informed:

As a guarantee of the protection of personal data, section 33(1) of the PDPA establishes the right to be informed of data collection and processing, as well as the purpose involved. Organizations deploying AI systems must uphold this right. This means individuals must be clearly and proactively informed before or during interaction with the system, whether their input prompts and generated outputs may be stored, reused for model training, or shared with third parties. Importantly, individuals must also be informed whether they can prevent their data from being used in future fine-tuning or model-improvement activities, especially when sensitive or identifiable personal data is involved. Furthermore, those deploying the AI must take responsibility for responding to data subject requests for access, objection, or deletion, as part of transparent and accountable data governance. Aligning these practices with the right to be informed ensures that consent, if relied upon, is meaningful and that users can exercise their autonomy over data-driven technologies (Centre for Information Policy and Leadership (CIPL), 2024).

ii). The right to object to the processing of personal data collected where such processing will lead to adverse impacts:

Under the PDPA, when organizations rely on the legitimate interest legal basis for processing, individuals have a right to object to processing pursuant to section 35 of the PDPA (Personal Data Protection Act, 2022). This provides individuals with an important level of control over their personal data. Therefore, organizations that rely on the 'legitimate interests' legal basis should allow individuals to object to the use of their personal data for model operation, development, and improvement at any time in and accessible manner, and cease processing, unless the organization can demonstrate compelling interests that override the reasons for the objection (Confederation for European Data Protection Organizations (CEDPO), 2023).

iii). The right to erasure:

Data protection law applies to various stages in the AI context, where data subject rights related to personal data may be relevant. These stages include the training data phase, where personal data is incorporated, and the deployment phase, where personal data is used to generate content and the resulting content itself. Additionally, the model itself may contain personal data (Centre for Information Policy and Leadership (CIPL), 2024). Regulators should consider the entire range of compliance requirements that organizations must meet to safeguard individual rights. In some instances, organizations may not be able to comply with erasure requests because the associated data is prohibited from further processing, including deletion or modification, because it is subject to data retention requirements from other legal acts, such as anti-money laundering requirements, or it is on hold because of litigation proceedings (Confederation for European Data Protection Organisations (CEDPO), 2023).

Certainly, there are broader societal benefits derived from training AI models on a wide variety of personal data, such as easing access to information and technology and enhancing AI's diversity and accessibility. However, as exceptions exist in every general rule, AI developers and organizations should be able to web scrape sensitive data that individuals choose to make public. The case of *Meta Platforms Inc. v. Bundeskartellamt* (Case C-252/21 *Meta Platforms Inc and Others v. Bundeskartellamt* [2023] ECLI:EU:C: 2023:537, para 77), in which the Court of Justice of the European Union (CJEU) examined whether sensitive data might be deemed publicly available and the legitimate interests of a controller to handle such data, provides a significant analogy. The CJEU clarified that personal data is manifestly made public in cases where an individual 'intended, explicitly and by a clear affirmative action, to make the personal data in question accessible to the general public'. When a person has settings at their disposal and is fully informed that their information may be accessible to the public or only a chosen few, and

they decide to make it public, they have clearly made their information public (Case C-252/21 *Meta Platforms Inc and Others v. Bundeskartellamt* [2023] ECLI:EU:C: 2023:537. at paras 77-85). As a general matter, AI model developers should be able to use such data so long as the developer's legitimate interest is not outweighed by the rights of individuals (Centre for Information Policy and Leadership (CIPL), 2024).

4. Data Transfers

If personal data is transferred to other countries, the PDPA includes provisions under PART V regarding the legal basis for such transfers and measures to ensure the protection of data during the transfer process, whether in places with or without adequate safeguards for personal data. However, as noted in the Centre for Information Policy and Leadership (CIPL)'s report on the application of data protection principles to AI, nations are increasingly imposing restrictions on certain cross-border data transfers through existing data protection laws. Tanzania's PDPA is not an exception. Sections 31 and 32 of the PDPA regulate the cross-border transfers of personal data, including the Minister's power to issue regulations specifying categories of processing for which cross-border transfers of personal data are completely prohibited. This may impede the development of accurate and fair AI models and have other unintended negative consequences for beneficial AI use (Centre for Information Policy and Leadership (CIPL), 2024).

For example, several advanced AI models require diverse, high-quality datasets, often necessitating the transfer of data across borders to improve performance and accuracy. Under the GDPR, the European Data Protection Board (EDPB) provides a structured framework for cross-border data transfers through adequacy decisions and standard contractual clauses (SCCs). Similarly, in Kenya, the Office of the Data Protection Commissioner (ODPC) has issued guidance on data transfer and sharing mechanisms, recognizing the need for international collaboration

in data-driven innovation (Office of the Data Protection Commissioner, Kenya, 2024). However, Tanzania's Personal Data Protection Commission has yet to issue any guidance or regulations set specifically on cross-border data transfers.

IV. RECOMMENDATIONS

It is important to acknowledge that the PDPA is not an AI-specific legislation and was not expressly enacted to facilitate or regulate AI. Its primary aim is to establish a comprehensive framework for the protection of personal data across all sectors in Tanzania. As such, any effect the PDPA may have on AI development arises incidentally through its application to data processing activities that support AI systems. While the PDPA does not explicitly promote innovation, its provisions, including those on data minimization, cross-border data transfers, and consent, inevitably interact with AI development practices, particularly those that depend on large, diverse datasets.

The PDPA, in its current form, tends to prioritize data minimization, consent-based processing, and strict controls on data sharing, all principles that, while crucial for data protection, may inadvertently inhibit the development, training, and deployment of AI systems that rely on access to large, diverse, and often sensitive datasets. The lack of specific provisions to accommodate AI's unique demands further compounds the problem.

This section, therefore, does not evaluate the PDPA for its success or failure in achieving an unexpressed goal of fostering AI innovation, but instead examines how the structure and requirements of the PDPA, such as those under Sections 25 and 26 of the PDPA, may inadvertently constrain AI innovation or create compliance challenges in the Tanzanian context. It does so by analyzing (i) the institutional role and scope of the PDPC, (ii) legal restrictions on sharing of personal and sensitive data under Section 26 of the PDPA, and (iii) the absence of mandates

for privacy-preserving design approaches such as 'Privacy by Design (PbD)' that could bridge the gap between data protection and AI innovation.

Against this backdrop, this section further examines practical strategies that reflect how the PDPA interacts with real-world AI applications in Tanzania—exploring them through concrete examples and operational dynamics to illuminate the practical implications of the PDPA's data protection requirements for AI development, innovation, and ethical deployment. This approach provides a grounded understanding of how existing regulatory constraints shape, and in some cases limit, the responsible and effective use of AI technologies in the Tanzanian context.

A. The Role of the Personal Data Protection Commission (PDPC)

The PDPC plays a crucial role in ensuring that AI systems comply with data protection principles, balancing innovation with the fundamental right to privacy. Since the PDPA is not a dedicated AI regulation, and the PDPC, as its implementing authority, is not designed to function as a comprehensive AI regulator. Instead, the PDPC's mandate is confined to overseeing compliance with data protection obligations, and its involvement in AI regulation is incidental, limited to ensuring that AI applications comply with the privacy and data protection requirements set out under the PDPA. This distinction is crucial in understanding both the scope and the limitations of the PDPC's oversight in the context of AI.

As such, it is pertinent to note that the extent to which the PDPC, as a data protection commission (DPC), has the necessary legal, technical, and institutional capacity to regulate AI-driven data processing remains an area of concern. The global experience suggests that DPCs must evolve rapidly to keep pace with the complexities of AI technologies and systems, as seen with the EDPB under the GDPR, which has recently adopted an opinion on AI and automated decision-making to address emerging risks

of AI technologies (European Data Protection Board, 2024).

In the African context, DPCs are noted for establishing themselves as important players in AI regulation. Their actions have mostly involved research, guidance, announcements of plans to regulate AI in the context of data protection, and, in the worst situations, moratoriums on facial recognition and other technology (Tsebee & Oloyede, 2024). For example, in 2020, Mauritius' Data Protection Commission published the 'Guide on Data Protection for Health Data and Artificial Intelligence Solutions,' providing crucial insights into handling sensitive health data within AI solutions and emphasizing the intersection of health care innovation and data protection (Data Protection Office, Mauritius, 2020). Subsequently, in 2023, the Moroccan DPA co-sponsored resolutions on generative AI systems and AI and employment (Tsebee & Oloyede, 2024).

These developments signal a growing tendency for DPCs to entrench their authority in AI governance, and they are essential in influencing the ethical and responsible advancement and use of AI across Africa. However, while such involvement is framed as promoting ethical and responsible AI use, it also risks reinforcing inflexible privacy regimes that may hinder innovation and the practical deployment of AI technologies across Africa since by prioritizing strict compliance with data protection principles such as purpose limitation, data minimization, and consent requirements, DPCs may create regulatory uncertainty or impose compliance burdens that deter experimentation and slow down the development of AI systems. This can particularly impact startups and research institutions that lack resources to navigate complex legal requirements.

As aforementioned, in the African context, DPCs are increasingly recognizing the importance of regulating AI to safeguard data subjects' rights. DPCs are pivotal in overseeing personal data processing and ensuring that AI applications do not infringe upon individual privacy (Tsebee & Oloyede, 2024). The PDPC's role becomes even more crucial when dealing with AI

models that utilize extensive datasets to generate insights or predictions. As the primary function of the PDPC is to enforce compliance with the PDPA, the role may extend to ensuring that AI developers, organizations, and data controllers adhere to the principles of lawfulness, fairness, and transparency in data processing. In practice, this requires proactive engagement with AI stakeholders to assess whether data collection, storage, and usage in AI systems align with legal requirements (Tsebee & Oloyede, 2024). The PDPC may also scrutinize the lawfulness of acquiring and processing datasets for AI models. Without such oversight, there is a risk of misuse that could lead to a backlash against AI systems in cases of individual privacy infringement. The PDPC thus acts as both a regulatory body and a trust-building institution, setting the stage for responsible AI practices within Tanzania's digital ecosystem.

In Europe and other jurisdictions, enforcement actions by national DPCs, such as fines imposed on AI-powered advertising firms for excessive data collection, illustrate how regulators can hold AI systems accountable. However, the PDPC in Tanzania has yet to develop sector-specific guidelines or conduct investigations into AI applications, leaving significant oversight gaps. Without clear regulatory interventions, AI developers in Tanzania may face uncertainty about compliance, potentially deterring innovation or leading to unchecked AI deployments that pose privacy risks.

B. Regulatory Sandboxes

Despite these challenges, the limitations imposed by the PDPA are not necessarily an outright impediment to AI innovation. Rather, they highlight the need for Tanzania to develop AI-specific data governance frameworks that enable responsible data-sharing practices while upholding privacy protections. One possible solution is the introduction of regulatory sandboxes—controlled environments where AI developers can experiment with data-sharing mechanisms under strict oversight (OECD

– Working Party on Artificial Intelligence Governance (AIGO), 2023). If Tanzania were to adopt a regulatory approach similar to that in the EU, AI companies could gain access to anonymized datasets for research and development while remaining within the legal parameters of the PDPA.[3]

Furthermore, the PDPA's restrictions on data sharing could incentivize AI developers to explore privacy-enhancing technologies (PETs), such as federated learning and homomorphic encryption (Feretzakis et al., 2024). These technologies allow AI models to be trained on decentralized datasets without exposing raw personal data, thereby enabling compliance with the PDPA while still advancing AI capabilities (Ward, 2025). For instance, Google's federated learning approach in mobile AI applications allows predictive text and voice recognition models to improve without transmitting user data to centralized servers (Sen et al., 2025). If similar approaches are encouraged in Tanzania, AI firms could navigate the PDPA's constraints without compromising innovation.

C. Incorporating and Implementing Privacy by Design in AI

Although the Tanzanian PDPA does not explicitly mandate incorporating privacy by design into AI systems, its core principles closely align with this best practice. Privacy by design (PbD) is a proactive approach to data protection that integrates privacy considerations at every stage of a system's development, rather than treating them as an afterthought (Bygrave, 2021; Goodbody, 2018). Originating as a concept developed by Dr. Ann Cavoukian, PbD has been widely recognized in global data protection frameworks, including the EU's GDPR, which explicitly enshrines it under Article 25.

[3] Research has shown that, although data anonymization techniques have improved, they often struggle to balance privacy and utility effectively. The risk of re-identification (de-anonymizing data) data still lingers as a valid concern.

While Tanzania's PDPA does not formally adopt PbD, its requirements on data minimization, purpose limitation, and security safeguards suggest that AI developers operating in Tanzania would benefit from embedding privacy-centric features into their systems from the outset. Failure to do so could lead to compliance risks, undermine user trust, and ultimately hinder AI innovation by creating legal uncertainty.

While it is unclear why the legislator did not include privacy by design as one of the technical and organizational measures,[4] the absence of a legal mandate for PbD in Tanzania places a greater responsibility on AI developers and organizations to voluntarily integrate privacy-friendly mechanisms into their systems.

However, if AI development does not embed privacy safeguards at an early stage, these systems risk violating key PDPA principles, such as lawful processing and data security. One significant concern is the issue of excessive data processing. Without PbD, AI systems may gather and process unnecessary personal data, increasing the likelihood of data breaches or unauthorized processing. A clear example of how PbD can mitigate this risk can be found in Europe's approach to AI-powered virtual assistants like Apple's Siri or Google Assistant. While these services generally require an internet connection to function fully, such as retrieving information from the web or syncing with cloud services, compliance with GDPR's PbD principles has led to the integration of on-device processing capabilities. For instance, tasks such as wake-word detection or basic voice-command interpretation are increasingly handled locally on the user's device, thereby reducing the transmission of sensitive voice data to external servers and enhancing privacy (Veale et al., 2018). If similar privacy-centric approaches were adopted in Tanzania, AI developers could reduce exposure to regulatory risks under the PDPA while fostering greater user confidence in AI applications.

[4] See, Recital 78 of the GDPR on Appropriate Technical and Organisational Measures. Available at: https://gdpr-info.eu/recitals/no-78/

This article argues that PbD offers long-term advantages for AI innovation in Tanzania. By embedding privacy-enhancing features early in AI development, companies can avoid costly retroactive compliance efforts, reduce liability risks, and enhance consumer trust. Moreover, the adoption of PbD can serve as a competitive advantage, positioning Tanzanian AI firms as leaders in ethical AI development within Africa. One practical way forward is for Tanzania's regulatory bodies, such as the PDPC, to issue PbD guidelines specific to AI systems. These guidelines could outline best practices, such as data minimization techniques, privacy-preserving AI architectures, and transparency requirements, helping AI developers navigate compliance while fostering responsible innovation.[5]

V. CONCLUSION

This article critically examines the PDPA and its implications for AI innovation, analyzing whether the Act fosters or hinders AI development in Tanzania. The analysis demonstrates that while the PDPA establishes an essential legal foundation for responsible data processing, its provisions introduce both opportunities and constraints for AI-driven systems. By exploring key areas such as the limitations on the sharing of personal data (Sections 25 and 26), the development of safeguards for privacy rights (Section 27), and the need for AI explainability, this study underscores the complex relationship between regulatory compliance and technological advancement.

One of the article's major findings is that the PDPA's emphasis on data protection principles, such as purpose limitation and security safeguards, aligns with global data protection standards, particularly the European Union's GDPR. However, unlike the GDPR, which explicitly mandates privacy by design

[5] This approach was also noted in the recent landmark case on the PDPA, *Tito Magoti v. Attorney Geneal*, Miscellaneous Civil Case No. 18 of 2023.

and provides detailed guidance on AI-driven decision-making, the PDPA lacks specific provisions or guidelines from the PDPC addressing AI regulation. This regulatory gap creates ambiguity for AI developers operating in Tanzania, as they must navigate compliance requirements that were not originally designed with AI in mind.

Despite its comprehensive analysis, this paper has certain limitations that must be acknowledged. First, the paper primarily focuses on the legal and regulatory aspects of AI innovation in Tanzania under the PDPA, without extensive empirical data on AI adoption trends in the country. AI development in Tanzania is still in its early stages compared to other jurisdictions such as Kenya, South Africa, and the EU. Consequently, some of the challenges and regulatory gaps identified in this study are based on theoretical and comparative analysis rather than direct empirical observations of AI implementation in Tanzania. Future research could benefit from case studies on AI deployment in Tanzanian industries, exploring how businesses and regulators navigate data protection compliance in practice.

Another limitation is the evolving nature of AI governance frameworks. AI regulation is a rapidly developing field, with global jurisdictions continuously refining their approaches to balance innovation and data protection. While this study compares Tanzania's PDPA with the GDPR and some other data protection frameworks,[6] it does not account for emerging AI regulatory frameworks, such as the EU AI Act, which introduces a risk-based classification system for AI applications. As international AI governance models evolve, Tanzania may consider adopting a more tailored AI regulatory framework that provides clear compliance pathways for developers while addressing sector-specific risks. Future studies should analyze how new global AI regulations influence Tanzania's approach to data protection and AI governance.

[6] For instance, Protection of Personal Information Act (POPIA) in South Africa

Finally, this paper assumes that Tanzania's PDPA will be enforced effectively, yet enforcement capacity remains an open question. The success of data protection regulations in fostering or hindering AI innovation depends not only on the legal framework but also on the strength of regulatory institutions. This paper does not extensively examine the PDPC's institutional capacity to oversee AI-related compliance. Given the technical complexity of AI systems, regulatory bodies need specialized expertise to evaluate AI compliance with data protection standards. Future research could assess whether Tanzania's regulatory institutions have the resources and technical capacity to effectively enforce AI-related provisions under the PDPA.

REFERENCES

A&L Goodbody. (2018). The GDPR: A Guide for Businesses – Data Privacy by Design, by Default and Privacy Impact Assessments, Page 24.

Adeleke, F & Akinwale, F. (2024). *Responsible AI Governance in Africa: Prospects for Outcomes Based Regulation.* African Observatory on Responsible AI. (March 2024). Available at: https://www.africanobservatory.ai/ai4d-resources/responsible-ai-governance-in-africa-prospects-for-outcomes-based-regulation

Ahmed Hilali et al. (2020). Linkage Attack and Protection Mechanism for Social Network From Mobility Profile. 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering 17 (May 2021), pp. 1-6. https://ieeexplore.ieee.org/document/9429665

Alowais, S.A., Alghamdi, S.S., Alsuhebany, N. et al. (2023). Revolutionizing healthcare: the role of artificial intelligence in clinical practice. BMC Med Educ 23, 689 (2023). https://doi.org/10.1186/s12909-023-04698-z

Alzubaidi, L, et al. (2023). Towards Risk-Free Trustworthy Artificial Intelligence: Significance and Requirements. International Journal of Intelligent Systems. https://doi.org/10.1155/2023/4459198

AU, (July,July 2024). Continental Artificial Intelligence Strategy: Harnessing AI for Africa's Development and Prosperity. Available at: https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy

Bakker, M. (2024). The Role of Data Privacy in AI Governance. KPMG. Available at: https://kpmg.com/nl/en/blogs/home/posts/2024/09/the-role-of-data-privacy-in-ai-governance.html

Baldini, D., & Francis, K. (2024). AI Regulatory Sandboxes between the AI Act and the GDPR: the role of Data Protection as a Corporate Social Responsibility. *CEUR Workshop Proceedings*, *3731*

Ben Dhaou, S., Isagah, T., Distor, C., & Ruas, I. C. (2024). *Global assessment of responsible AI in cities: Research and recommendations to leverage AI for people-centred smart cities*. UN-Habitat.

Birhane A. (2021). Algorithmic injustice: a relational ethics approach. Patterns (New York, N.Y.), 2(2), 100205. https://doi.org/10.1016/j.patter.2021.100205

Buocz, T., Pfotenhauer, S., & Eisenberger, I. (2023). Regulatory sandboxes in the AI Act: reconciling innovation and safety? Law, Innovation and Technology, 15(2), 357–389. https://doi.org/10.1080/17579961.2023.2245678

Bygrave, L. (2020). Article 22 Automated Individual Decision-Making, Including Profiling, The EU General Data Protection Regulation (GDPR) (Oxford University Press, New York 2020) https://doi.org/10.1093/oso/9780198826491.003.0055

Bygrave, L. (2021). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. Oslo Law Review 1(02):105-120. Available at: https://www.scup.com/doi/10.18261/issn.2387-3299-2017-02-03

Case C-252/21 *Meta Platforms Inc and Others v. Bundeskartellamt* [2023] ECLI:EU:C:2023:537C: 2023:537, para 77.

Cavoukian A. Privacy by design. Information Privacy Commission, Canada. Available at: https://www.ipc.on.ca/en/mdia/1826/download?attachment

CEDPO AI and Data Working Group (2024). *Is the DPO the right Person to be the AI Officer?* CEDPO. Available at: https://shorturl.at/YBsuL

Centre for Information Policy and Leadership (CIPL). (Dec, Dec 2024). *Applying Data Protection Principles to Generative AI: Practical Approaches for Organizations and Regulators.* Available at: https://shorturl.at/AMca3

Centre for Information Policy and Leadership (CIPL). (Febr 2024). *Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework*. Available at: https://shorturl.at/jwJlw (Accessed: 1st March 2025).

Chen, W, Wang, Y, Wu, D, Yin, X. (2024). *Can the establishment of a personal data protection system promote corporate innovation?* Research Policy, Vol 53, Issue 9, 2024. https://doi.org/10.1016/j.respol.2024.105080.

Clyde & Co, Global Guide on Artificial Intelligence – Kenya/South Africa. (2024). Available at: https://www.clydeco.com/en/expertise/services/technology-outsourcing-data/artificial-intelligence-ai

CNIL, France (11th Febr 2025). *Data governance and AI: Five Data Protection Authorities Commit to Innovative and Privacy-Protecting AI.* Available at: https://shorturl.at/GoF6c (Accessed: 21st February 2025).

CNIL, France (7th Febr 2025). *AI and GDPR: the CNIL publishes new recommendations to support responsible innovation.* Available at: https://shorturl.at/DRbAF (Accessed: 21st Febr 2025)

Confederation for European Data Protection Organisations (CEDPO). (2023). Generative AI: The Data Protection Implications. Available at: https://shorturl.at/YiQz1

Confederation for European Data Protection Organisations (CEDPO). (2023). AI and Personal Data: A Guide for DPOs" Frequently Asked Questions". Available at: https://cedpo.eu/ai-and-personal-data-a-guide-for-dpos-frequently-asked-questions/

Data Protection Office, Mauritius. (2020). Guide on Data Protection for Health Data and Artificial Intelligence Solutions https://shorturl.at/TF626

Davis, T., & W Trott, W. (2024). 'The regulation of artificial intelligence through data protection laws: Insights from South Africa' 1 African Journal on Privacy & Data Protection 207-219 https://doi.org/10.29053/ajpdp.v1i1.0010

Detwiller, B. (23rd May 2024). *Responsible AI: How can new technologies respect data privacy?* Celonis Blog. Available at: https://www.celonis.com/blog/responsible-ai-how-can-new-technologies-respect-data-privacy/

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608.

Durdymyradov, K., Moshkov, M., Ostonov, A. (2024). Decision Trees Versus Systems of Decision Rules: A Rough Set Approach. Germany: Springer Nature Switzerland.

European Data Protection Board (EDPB), (18th Dec 2024). EDPB opinion on AI models: GDPR principles support responsible AI. Available at: https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en (Accessed: 19th Jan 2025).

Feretzakis, G., Papaspyridis, K., Gkoulalas-Divanis, A., & Verykios, V. S. (2024). Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review. Information, 15(11), 697. https://doi.org/10.3390/info15110697

Freye, F, Kipker, D, Rindstone, E, Mwamlangala, D. (2020). *Strengthening protection of personal data in the health sector: a comparative analysis of the. Tanzanian and German eHealth system*. (2020). DuD – Datenschutz und Datensicherheit.

Global Partnership for Sustainable Development Data, (2023). Artificial Intelligence Practitioners' Guide: Kenya. GIZ Available at: https://shorturl.at/EzBmz; In 2018, the Government of Kenya established the Distributed Ledgers Technology and Artificial Intelligence Taskforce which provided recommendation on how the Government can leverage new technologies in Kenya.

Harrison, T, Luna-Reyes, L, et.al. (2019). The Data Firehose and AI in Government: Why Data Management is a Key to Value and Ethics. In Proceedings of the 20th Annual International Conference on Digital Government Research. Association for Computing Machinery, New York, NY, USA, 171–176. https://doi.org/10.1145/3325112.3325245; Liang, Weixin et al., Advances, challenges and opportunities in creating data for trustworthy AI. Nature Machine Intelligence 4 (2022): 669 - 677.

Hassanien, A., Garg, A., Singh, A., & Gupta, D. (2025). Explainable Edge AI: A Futuristic Computing Perspective. (2022). Germany: Springer International Publishing.

Hennemann, M. (2024). African Data protection Laws and Artificial Intelligence – Regulation, Policy and ways forward in Lukman Adebisi Abdulrauf and Hlengiwe Dube (eds) *Data Privacy Laws in Africa: Emerging Perspectives* (Pretoria University Law Press (PULP). Available at: https://www.pulp.up.ac.za/edited-collections/data-privacy-law-in-africa-emerging-perspectives

Hirsch, C. (March 2025). *The credit scoring company must disclose its algorithm but must explain it.* CDBF.CH. Available at: https://cdbf.ch/1400/>

https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide

Jonas Schuett, *Defining the scope of AI regulations*. Law, Innovation and Technology. Vol. 15 (1), 2023.

Liu, H., Gegov, A., Cocea, M. (2015). Rule Based Systems for Big Data: A Machine Learning Approach. Germany: Springer International Publishing.

Longo, L., et.al. (2024). Explainable Artificial Intelligence (XAI) 2.0: A manifesto of open challenges and interdisciplinary research directions. Information Fusion, 106, 102301. https://doi.org/10.1016/j.inffus.2024.102301

Luciano, F & Mariarosaria, T. (2016). *What is data ethics?* Phil. Trans. Royal Society Publishing. https://doi.org/10.1098/rsta.2016.0360

Marengo, F. (2023) Privacy in the Age of AI: Protecting Individuals' Rights in the Age of AI. Federico Marengo. Available at: https://shorturl.at/9RnZU

Marengo, F. (2023). Privacy in the Age of AI: Protecting Individuals' Rights in the Age of AI. Federico Marengo. Available at: https://shorturl.at/9RnZU

Martí-Bonmatí, L., Blanquer, I., Tsiknakis, M. et al (2025). *Empowering cancer research in Europe: the EUCAIM cancer imaging infrastructure*. Insights Imaging 16, 47 (2025). https://doi.org/10.1186/s13244-025-01913-x

Novazi, Z. (2025). Automated Decision-Making and the Right to an Explanation Under POPIA in South Africa: A Legal Perspective. Law, Technology and Humans. 7. 146-161. 10.5204/lthj.4081.

OECD – Working Party on Artificial Intelligence Governance (AIGO), (2023). Regulatory Sandboxes in Artificial Intelligence and other experimentation tools. Available at: https://shorturl.at/6Jo3i

Office of the Data Protection Commissioner, Kenya. (2023). Guidance Note For Digital Credit Providers. Available at: https://d4daccess.eu/en/kenya-guidance-notes-on-data-protection-and-privacy

Office of the Data Protection Commissioner, Kenya. (2024). *Data Sharing Code: A Guidance Note by the Data Protection Commissioner*. Available at: https://shorturl.at/tuflA

Office of the Privacy Commissioner of Canada, Canadian privacy regulators launch principles for responsible development and use of generative AI. International Symposium on Privacy and AI hosted by the Office of the Privacy Commissioner of Canada (2023). Available at: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/nr-c_231207/

Oxford Insights, Government AI Readiness Index (2023). Available at: https://oxfordinsights.com/ai-readiness/ai-readiness-index/

Pasipamire, N., & Muroyiwa, A. (2024). *Navigating algorithm bias in AI: ensuring fairness and trust in Africa*. Frontiers in research metrics and analytics, 9, 1486600. https://doi.org/10.3389/frma.2024.1486600

Pasipamire, N., & Muroyiwa, A. (2024). *Navigating algorithm bias in AI: ensuring fairness and trust in Africa*. Frontiers in research metrics and analytics, 9, 1486600. https://doi.org/10.3389/frma.2024.1486600

Paul Voigt and AxelAxel, von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide. (Springer Cham 2024) https://doi.org/10.1007/978-3-031-62328-8

Personal Information Protection and Electronic Document Act (S.C. 2000, c.5). Available at: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html

Protection of Personal Information Act (POPIA)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 (Regulation (EU) 2016/679). https://gdpr-info.eu

Robert, K. (4th March 2024). Tanzania's Court system goes for AI solutions. Africa Legal. Available at: https://www.africa-legal.com/news/tanzanias-court-system-goes-for-ai-solutions/102631; Adams & Adams, The Judiciary integrates Artificial Intelligence (AI) into its processes. (12th April 2024). Available at: https://www.adams.africa/general-adams-news/the-judiciary-integrates-artificial-intelligence-ai-into-its-processes/

Saeed, W., & Omlin, C. (2023). Explainable AI (XAI): A systematic meta-survey of current challenges and future opportunities. Knowledge-Based Systems, 263, 110273. https://doi.org/10.1016/j.knosys.2023.110273

Sahara Ventures Report, (2024). Artificial Intelligence in Tanzania, what's happening: Latest information on AI startups and projects in Tanzania. Sahara Ventures. Available at: https://publication.saharaventures.com/publication/Artificial-Intelligence-in-Tanzania-What-is-Happening

Salami, E & Nwankwo, I. (2024). 'Regulating the privacy aspects of artificial intelligence systems in Nigeria: A primer' (2024) 1 African Journal on Privacy & Data Protection 220-247 https://doi.org/10.29053/ajpdp.v1i1.0011

Salami, E. (2024). The Ascent of Artificial Intelligence in Africa: Bridging Innovation and Data Protection in Lukman Adebisi Abdulrauf and Hlengiwe Dube (eds) *Data Privacy Laws in Africa: Emerging Perspectives* (Pretoria University Law Press (PULP) 2024).Available at: https://www.pulp.up-.ac.za/edited-collections/data-privacy-law-in-africa-emerging-perspectives

Salami, E. (2024). The Ascent of Artificial Intelligence in Africa: Bridging Innovation and Data Protection in Lukman Adebisi Abdulrauf and Hlengiwe Dube (eds) *Data Privacy Laws in Africa: Emerging Perspectives* (Pretoria University Law Press (PULP) 2024).Available at: https://www.pulp.up-.ac.za/edited-collections/data-privacy-law-in-africa-emerging-perspectives

Salami, E. (2024). The Ascent of Artificial Intelligence in Africa: Bridging Innovation and Data Protection in Lukman Adebisi Abdulrauf and Hlengiwe Dube (eds) *Data Privacy Laws in Africa: Emerging Perspectives* (Pretoria University Law Press (PULP) 2024). Available at: https://www.pulp.up-

.ac.za/edited-collections/data-privacy-law-in-africa-emerging-perspectives

Sandra Wachter, Brent Mittelstadt, Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*. International Data Privacy Law, Volume 7, Issue 2, May 2017, Pages 76–99, https://doi.org/10.1093/idpl/ipx005

Schuett, J. (2023). *Defining the scope of AI regulations.* Law, Innovation and Technology. Vol. 15 (1), 2023.

Selbst, A.D., et al. (2019). '"Fairness and Abstraction in Sociotechnical Systems.' Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency: 59-68.

Sen, J., Waghela, H., & Rakshit, S. (2025). Privacy in Federated Learning. IntechOpen. doi: 10.5772/intechopen.1006677

Tandon, M. (2024). *Federated Learning: Powering AI With Innovation and Privacy*. Available at: https://www.usaii.org/ai-insights/federated-learning-powering-ai-with-innovation-and-privacy;

The California Consumer Privacy Act of 2018 (CCPA)

The Chanzo, *Experts Reflect on Tanzania's Readiness for the AI Revolution.* (25th April 2024). The Chanzo Initiative. Available at: https://thechanzo.com/2024/04/25/experts-reflect-on-tanzanias-readiness-for-the-ai-revolution/

The Citizen, (7th February 2024). Tanzania plans to adopt AI in e-govt platforms. The Citizen Newspaper. Available at: https://www.thecitizen.co.tz/tanzania/news/national/tanzania-plans-to-adopt-ai-in-e-govt-platforms-4516832

The Citizen, (7th February 2024). Tanzania highlights its ambitious plans for AI. The Citizen Newspaper. Available at: https://www.thecitizen.co.tz/tanzania/news/national/tanzania-highlights-its-ambitious-plans-for-ai-4519516

The Citizen. (6th April 2024). *Tanzania Highlights strategy for harnessing AI in the digital economy era.* The Citizen Newspaper. Available at: https://www.thecitizen.co.tz/tanzania/news/national/tanzania-highlights-strategy-for-harnessing-ai-in-the-digital-economy-era-4580746

The Data Protection Act, No. 24 of 2019

The EU AI Act, 2024.

The Personal Data Protection (Complaints Settlement Procedures) regulations, GN No. 449B of 2023.

The Personal Data Protection (Personal Data Collection and Processing) regulations, GN No. 449C of 2023

The Personal Data Protection Act, CAP 44 of 2022 (PDPA)

Thekdi, S., Tatar, U., Santos, S., Samrat Chatterjee, S. (2022). *Disaster risk and artificial intelligence: A framework to characterize conceptual syner-*

gies and future opportunities. Risk Analysis: An International Journal (2022). Available at: https://doi.org/10.1111/risa.14038

Tito Magoti v. the Attorney General, Miscellaneous Civil Case No. 18 of 2023.

Tsebee, D. & Oloyede, R. (2024*). DPAs and AI Regulation in Africa. IAPP Newsletter*. Available at: https://iapp.org/news/a/dpas-and-ai-regulation-in-africa

Tsebee, D. & Oloyede, R. (2024). DPAs and AI Regulation in Africa. IAPP Newsletter. Available at: https://iapp.org/news/a/dpas-and-ai-regulation-in-africa

UK Information Commissioner's Office (ICO), (15th March 2023). *Guidance on AI and Data Protection*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ (Accessed: 20th February 2025).

UK Information Commissioner's Office (ICO), *Guidance on the AI auditing framework*. Available at: https://shorturl.at/qJx2N (Accessed: 20th February 2025).

Veale, M., Binns, R., Ausloos, J. (2018). When data protection by design and data subject rights clash, International Data Privacy Law, Volume 8, Issue 2, May 2018, Pages 105–123, https://doi.org/10.1093/idpl/ipy002

Verhenneman, G. (2025). AI and Healthcare Data. In N. A. Smuha (Ed.), The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence (pp. 306–321). chapter, Cambridge: Cambridge University Press.

Wachter, S & Mittelstadt, B and Floridi, L. (2016). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation (December 28, 2016). International Data Privacy Law, 2017, Available at http://dx.doi.org/10.2139/ssrn.2903469

Wamba-Taguimdje, S.-L., Fosso Wamba, S., Kala Kamdjoug, J.R. and Tchatchouang Wanko, C.E. (2020), *Influence of artificial intelligence (AI) on firm performance: the business value of AI-based transformation projects*, Business Process Management Journal, Vol. 26 No. 7, pp. 1893-1924. https://doi.org/10.1108/BPMJ-10-2019-0411 .

Ward, S. (2025). Leveraging AI and Emerging Technology to Enhance Data Privacy and Security. Policy Study No. 317, R Street Institute. Available at: https://www.rstreet.org/research/leveraging-ai-and-emerging-technology-to-enhance-data-privacy-and-security/

White & Case, 2024. AI Watch: Global Regulatory Tracker - Kenya. Available at: https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-kenya

White & Case, 2024. AI Watch: Global Regulatory Tracker - South Africa. Available at: https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-south-africa

Whittaker, M. et al. (2018). AI Now 2018 Report. New York: AI Now Institute, 2018. Available at: https://ainowinstitute.org/publications/ai-now-2018-report-2