Telematics and Informatics Reports 21 (2026) 100299

Contents lists available at ScienceDirect

Telematics and Informatics Reports

journal homepage: www.elsevier.com/locate/teler

Assessing the organisational readiness and compliance with the personal data protection legislation in Tanzania

Noe Nnko [a,b], Petro Nzowa [a], Franklin Mungulluh [a], Emmanuel Mkilia [a], Hamza Malombe [c], Godbless Minja [d], Cesilia Mambile [e], Augustino Mwogosi [e,*]

[a] Personal Data Protection Commission, Dodoma, Tanzania
[b] Department of Computer Science, University of Dodoma, Dodoma, Tanzania
[c] Department of Accounting and Finance, Moshi Cooperative University, Kilimanjaro, Tanzania
[d] Department of Computer Science and Engineering, University of Dodoma, Tanzania
[e] Department of Information Systems and Technology, University of Dodoma, Tanzania

ARTICLE INFO

Keywords:
Readiness
Compliance
Organizations
Personal data
Legislation
Privacy
Data protection officer

ABSTRACT

The rapid digitization and digitalization of services, along with extensive use of personal data across public and private sectors, have raised concerns about personal data protection and privacy. In response, like other countries, Tanzania enacted the Personal Data Protection Act (PDPA), Cap. 44 of 2022, and its associated regulations. While these instruments establish a legal framework for data protection, their effectiveness depends on organizations' readiness to implement and comply with them. This study assesses organizational readiness and compliance with the PDPA, identifies key implementation challenges, and proposes measures to strengthen personal data protection practices in Tanzania. A pragmatic mixed-methods design guided by institutional theory was employed, with data collected from 232 organizations using a structured electronic questionnaire. Quantitative items assessed five readiness dimensions - awareness, internal policies, staff training, technical infrastructure, and management support. Meanwhile, open-ended questions examined implementation challenges and solutions. Quantitative data were analyzed using Partial Least Squares Structural Equation Modelling (PLS-SEM), and revealed that all five readiness dimensions were positively and significantly associated with compliance, with technical resources ($\beta = 0.412$) being the strongest predictor. Qualitative responses were thematically analyzed using NVivo v14, with results corroborating the quantitative findings and revealing deeper barriers, including limited awareness and capacity, and regulatory challenges. Integrated findings indicate that while larger organizations demonstrate basic preparedness, SMEs and NGOs face systemic capacity limitations. Overall, the study highlights the need for strengthened institutional capacity and a compliance-oriented culture, and provides evidence-based recommendations to support effective implementation of the legislation.

1. Introduction

The rapid expansion of data-driven technologies and digital services has led to an unprecedented increase in the collection, storage, and sharing of personal data [1]. While these developments support innovation, economic growth, and improved service delivery, they also heighten concerns about privacy risks, data misuse, and information security [2]. The growing reliance on technologies such as artificial intelligence (AI), cloud computing, smart cities, big data analytics, and the Internet of Things (IoT) has further amplified these concerns by increasing the scale, complexity, and interconnectedness of personal data processing activities. Consequently, personal data protection and privacy have emerged as critical governance and regulatory issues, requiring both robust legal frameworks and effective organizational implementation mechanisms.

In response to these challenges, many jurisdictions have enacted personal data protection laws to regulate the processing of personal data and ensure accountability among data controllers and processors [3,4]. Notable regulatory frameworks, including the European Union's General Data Protection Regulation (GDPR), California's Consumer Privacy Act (CCPA), and Brazil's Lei Geral de Proteção de Dados (LGPD), have set standards for lawful processing, transparency, consent, and

* Corresponding author.
E-mail address: mwogosia@gmail.com (A. Mwogosi).

https://doi.org/10.1016/j.teler.2026.100299
Received 7 July 2025; Received in revised form 30 January 2026; Accepted 5 February 2026
Available online 11 February 2026

cross-border data transfers [5,6]. Similarly, within Africa, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and national laws in countries such as South Africa, Nigeria, and Kenya reflect a broader continental commitment to privacy and data protection. In 2022, Tanzania joined this regulatory trajectory by enacting the Personal Data Protection Act (PDPA), Cap. 44, which imposes legal obligations on both public and private organizations to process personal data lawfully, fairly, transparently, and securely.

Despite the proliferation of data protection legislation, organizational compliance remains a persistent challenge globally [7,8]. Organizations often face difficulties in operationalizing legal requirements due to limited awareness of regulatory obligations, inadequate internal policies and governance structures, insufficient staff training, constrained technical and financial resources, weak enforcement mechanisms, and regulatory ambiguities [9–11]. These challenges suggest that the effectiveness of data protection laws depends not only on their legal design but also on the level of organizational readiness to implement and sustain compliance measures.

In Tanzania, where the legislative framework for personal data protection is relatively new [12,13], the extent to which organizations are prepared to meet the PDPA's legal and operational requirements remains largely unclear. While the Act establishes comprehensive obligations, there is limited empirical evidence on whether organizations possess the necessary awareness, internal policies, technical infrastructure, trained personnel, and management support to implement these requirements. This knowledge gap presents a significant policy and operational challenge. Without empirical insight into organizational readiness, regulators may struggle to design effective enforcement and support mechanisms, while organizations may lack guidance on where to prioritize compliance investments. Existing studies on data protection in Tanzania have largely focused on policy analysis and legal frameworks, offering limited evidence on how organizational readiness translates into actual compliance practices.

This study addresses this gap by assessing organizational readiness for PDPA compliance in Tanzania, examining key readiness dimensions, identifying barriers to effective implementation, and proposing actionable insights to strengthen personal data protection practices. Guided by institutional theory, the study examines how awareness, internal policies, staff training, technical resources, and management support influence compliance behaviour. In addition, it explores organizational challenges and practical solutions through qualitative analysis. By integrating quantitative and qualitative evidence, the study provides context-specific insights to support regulators, policymakers, and organizations in strengthening PDPA implementation and advancing responsible data governance in Tanzania. In doing so, this study contributes to the broader discourse on regulatory compliance, institutional capacity building, and accountable data governance in emerging data protection regimes.

The contributions of this study are threefold. First, it provides one of the earliest large-scale empirical assessments of organizational readiness for compliance with Tanzania's personal data protection legislation, offering timely evidence during the PDPA's early implementation. Second, it operationalizes organizational readiness across key dimensions: awareness, internal policies, staff training, technical resources, and management support, and empirically examines their effects on compliance using a mixed methods approach, thereby extending the literature beyond predominantly normative and legal analyses. Third, the study offers context-specific evidence on structural and institutional barriers to compliance across different organizational types, particularly SMEs and NGOs, informing targeted regulatory enforcement, capacity-building, and policy interventions in emerging data protection regimes.

The remainder of this study is structured as follows: Section 2 presents a review of relevant literature. Section 3 describes the research methods. Section 4 provides the findings and analysis. Section 5 discusses the results and their applicability to the Tanzanian context. Finally, Section 6 presents a conclusion and recommendations.

2. Literature review

2.1. Theoretical framework

This study is grounded in institutional theory, which provides a robust lens for examining how organizations respond to regulatory demands within their legal, social, and normative environments [14]. Unlike technology or efficiency-oriented theories, institutional theory explains compliance behaviour as a function of external pressures and internalized organizational practices shaped by formal rules, social expectations, and shared beliefs.

Institutional theory conceptualizes organizational behaviour through three interrelated pillars: regulative, normative, and cultural-cognitive [15]. The regulative pillar captures formal laws, enforcement mechanisms, and sanctions that compel compliance. This study encompasses the PDPA and the oversight role of regulatory authorities. The normative pillar reflects organizational norms, professional standards, internal policies, and governance structures that define appropriate conduct. The cultural-cognitive pillar relates to shared understandings, values, and taken-for-granted practices that shape how individuals perceive and enact compliance in daily operations.

While the regulative pillar is central due to the legal focus of this study, the normative and cultural-cognitive pillars remain essential for understanding how compliance is enacted in practice through organizational norms, leadership support, staff training, and shared interpretations of data protection responsibilities. Together, these pillars explain how organizations translate external legal requirements into internal readiness and sustained compliance behaviour.

2.2. Empirical literature review

2.2.1. Influence of organizational readiness on compliance with personal data protection legislation

A substantial body of empirical literature identifies organizational readiness as a critical determinant of compliance with personal data protection legislation. Across jurisdictions and sectors, studies consistently show that organizations with higher levels of preparedness demonstrate stronger compliance outcomes, while inadequate readiness contributes to reactive, fragmented, and superficial compliance efforts [16].

Organizational readiness is widely conceptualized as a multidimensional construct encompassing awareness of legal requirements, internal policies, staff training, technical infrastructure, governance capacity, and resource allocation [16–19]. Technological readiness includes secure IT systems, encryption, access controls, and monitoring tools that enable organizations to operationalize legal requirements [17]. Human readiness reflects staff awareness, skills, and training, which shape the organization's ability to interpret and apply regulatory obligations [18]. Strategic and financial readiness support the alignment of compliance activities with organizational objectives and resource planning [19].

Empirical evidence from both conceptual and applied studies reinforces the importance of these dimensions. Studies in Nigeria and other developing contexts highlight the absence of automated compliance systems and proactive risk management mechanisms, resulting in largely reactive compliance approaches [20]. Cross-national research further shows that embedding privacy engineering practices and cultivating a structured privacy-oriented culture significantly strengthens organizational readiness [21]. However, several studies caution that readiness is often uneven across sectors and organizations, with formal compliance structures existing without deep institutionalization [22].

Qualitative and conceptual research across African and global contexts emphasizes the role of internal policies, staff training, governance structures, and privacy-by-design practices in sustaining compliance [23,24]. Organizations that integrate data protection into operational

workflows, supported by internal policies and technological upgrades, tend to achieve more consistent compliance outcomes [25,26]. Large-scale benchmarking studies further demonstrate that investment in data privacy programmes is associated with improved regulatory compliance, operational efficiency, and organizational resilience [27].

Leadership and governance structures emerge as key enablers of readiness. Multi-case and industry-focused studies show that organizations with dedicated privacy teams, clearly defined data stewardship roles, and enterprise-wide governance frameworks exhibit stronger compliance postures [28]. However, research also cautions that financial and technical investments alone are insufficient without institutional capacity building, role clarity, and organizational accountability [28]. Sectoral variations further influence readiness practices, with industries such as digital commerce and insurance prioritizing consent management, audits, and role-specific protocols to ensure compliance [26,28].

Broader readiness frameworks reinforce these findings by demonstrating that effective data governance, cross-functional collaboration, and legal literacy are essential for regulatory adherence [18,29]. High organizational readiness enables proactive compliance practices, while low readiness leads to misinterpretation of legal requirements, technical vulnerabilities, and delayed incident responses [30,31]. SMEs are particularly vulnerable due to limited resources and expertise, whereas larger organizations tend to maintain more structured compliance programmes [31].

Despite extensive international evidence, there remains a need for context-specific analysis in Tanzania, where the PDPA is newly enacted, and unique regulatory, infrastructural, and institutional conditions shape organizational readiness.

2.2.2. Challenges faced by business organizations in complying with data protection laws

The literature identifies a consistent set of challenges that hinder effective compliance with personal data protection legislation. These challenges span financial, technical, organizational, legal, and governance-related dimensions.

Resource constraints are among the most frequently cited barriers. Studies consistently report that high compliance costs, limited access to technology, and inadequate financial capacity restrict organizations' ability to implement required safeguards, particularly among SMEs [9,32]. Limited awareness and legal literacy further exacerbate these challenges, leading to partial or incorrect implementation of regulatory requirements [9,32].

Regulatory complexity and ambiguity also impede compliance. Empirical studies highlight difficulties in translating abstract legal provisions into operational routines, particularly in environments where legislation is evolving or lacks detailed implementation guidance [33]. Fragmented data governance structures, siloed systems, and unclear accountability mechanisms further increase compliance risks and operational inefficiencies [3].

Technical vulnerabilities, including insecure cloud environments, outdated infrastructure, and weak cybersecurity controls, are widely documented across sectors and regions [4,34–37]. Organizations operating across jurisdictions face additional challenges arising from regulatory fragmentation and conflicting legal requirements [38,39]. Governance and leadership misalignment further constrain compliance, particularly when innovation objectives conflict with regulatory obligations or when institutional support is weak [40,41].

In African and developing country contexts, limited institutional capacity, weak enforcement mechanisms, and low regulatory awareness intensify these challenges [40,41]. These constraints underscore the importance of empirical research that captures how such barriers manifest within specific national and organizational contexts, including Tanzania.

2.2.3. Strategies and solutions for enhancing compliance

The literature proposes a range of integrated strategies to strengthen compliance with data protection legislation. These strategies combine technological, organizational, and policy-oriented interventions [22,42,43].

Technological solutions include automated compliance monitoring systems, privacy-preserving technologies, encryption, access controls, and AI-driven risk detection tools that enhance regulatory visibility and operational efficiency [20,21,44–46]. Organizational strategies emphasize staff training, internal audits, privacy-by-design frameworks, and the institutionalization of compliance roles such as Data Protection Officers (DPO) [22,25].

Policy and governance-focused solutions stress the importance of sector-specific guidelines, harmonized regulatory frameworks, public–private partnerships, and institutional capacity building, particularly in low-resource contexts [23,24,38]. Financial and incentive-based interventions, including subsidized training and targeted support for SMEs, are also identified as critical enablers of compliance [47].

Collectively, these studies suggest that effective compliance requires a multi-layered approach that aligns legal mandates with organizational capacity, technological infrastructure, and cultural change. However, empirical evidence on how these strategies can be contextualized and implemented within Tanzania remains limited.

2.3. Literature gap

Recent research on personal data protection increasingly frames compliance as an organisational capability rather than a purely legal or technical issue. Empirical studies emphasise that compliance outcomes are shaped by the interaction of organisational awareness, governance structures, staff capacity, and technical resources, often examined through analytical or model-based approaches. This body of work highlights that regulatory adoption alone is insufficient unless organisations possess the internal readiness required to operationalise data protection requirements in practice. However, empirical evidence from low- and middle-income countries remains limited, particularly studies that formally assess readiness–compliance relationships within newly established regulatory environments. Most studies rely on conceptual models or single-method designs and offer limited insight into the predictive relationships between readiness and compliance outcomes.

In Tanzania, where personal data protection legislation is relatively new, empirical evidence on organizational readiness and compliance remains scarce. This gap is significant, as understanding how readiness factors operate within the local institutional context is essential for designing effective regulatory strategies and organizational interventions.

2.4. Conceptual framework

Guided by institutional theory, this study proposes a conceptual framework (Fig. 1) that links organizational readiness dimensions to compliance with the personal data protection legislation. Compliance is treated as the dependent variable, reflecting the extent to which organizations have taken concrete steps to meet legal obligations under the PDPA. Five independent variables represent key readiness dimensions: awareness of legal requirements, internal data protection policies, staff training, technical resources, and management support.

Each readiness dimension reflects institutional pressures that shape compliance behaviour. Awareness reflects regulative pressures, internal policies and management support reflect normative pressures, and staff training reflects cultural-cognitive processes, while technical resources enable the operationalization of compliance across pillars. The framework provides a structured basis for empirical testing using PLS-SEM and supports analysis of how institutional readiness translates into compliance within Tanzanian organizations.

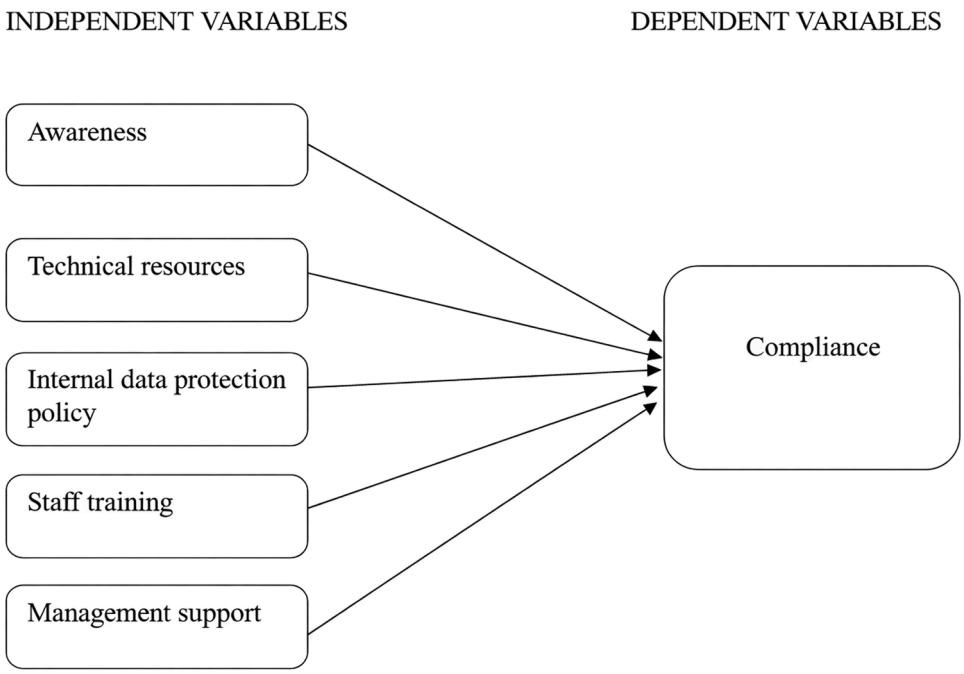

Fig. 1. Conceptual framework guiding the study (authors' work).
Source: Authors' work.

3. Methods

3.1. Study philosophy

This study was guided by a pragmatic research philosophy, which prioritizes methods best suited to addressing the research problem. Pragmatism recognizes that no single method is sufficient to capture the complexity of real-world issues such as data protection compliance, especially in diverse organizational settings [48].

3.2. Study approach

A mixed-methods approach was adopted to collect both numerical and descriptive data. This approach was chosen to provide a more comprehensive understanding of organizations' readiness to comply with personal data protection legislation. Quantitative data were used to measure key factors, including awareness levels, the presence of internal data protection policies, technical resources, staff training, and management support. Similarly, qualitative data were used to explore the contextual realities behind those factors, including challenges and solutions to compliance. The use of mixed methods allowed for both breadth and depth in the analysis and interpretation [49].

3.3. Study design

A cross-sectional study design was used, with data collected at a single point in time [50]. Both quantitative and qualitative data were collected through a structured questionnaire that included closed-ended items for quantitative responses and open-ended questions to capture narrative insights. The integration of both data types within the same tool enabled a unified, efficient data collection process. This design supported a comprehensive assessment of organizational readiness by examining not only statistical trends but also respondents' underlying experiences and concerns regarding data protection compliance.

3.4. Study population and setting

The study focused on organizations operating in Tanzania, selected from both the public and private sectors. This inclusive approach recognized that data protection obligations under the personal data protection legislation apply to all entities, regardless of ownership structure, that collect, process, or store personal data. The study included small, medium, and large organizations across key sectors such as finance, education, agriculture, healthcare, manufacturing, media, hospitality, and tourism, all of which are data-intensive.

3.5. Sampling strategy

The sample frame was primarily drawn from the database of registered data controllers and data processors maintained by the Personal Data Protection Commission (PDPC). This ensured that the organizations selected for the study had formal recognition of their role in handling personal data and were therefore directly relevant to the study's objectives.

The sample size for this study was determined using the Yamane formula for sample size calculation from a known population, assuming a 95 % confidence level and a 5 % margin of error [51]. Based on an estimated total of 9000 registered organizations in Tanzania that collect and process personal data, the resulting sample size was approximately 370. Within each selected organization, one DPO was purposively selected as a study respondent. However, the final analytical sample comprised 232 completed responses, yielding a response rate of 62.7 %. The lower response rate was primarily attributable to non-response and partial survey attrition, which are common in organizational surveys, particularly in newly regulated environments where compliance roles are still emerging. Competing organizational priorities and varying levels of familiarity with the Personal Data Protection Act also contributed to differential participation across organizations.

While lower than the initial target, this sample size was considered adequate for the planned analysis. Partial Least Squares Structural Equation Modelling (PLS-SEM) is suitable for moderate sample sizes and emphasises predictive accuracy rather than strict distributional assumptions. Following established guidance, the achieved sample exceeded the minimum requirements for estimating the specified model and provided sufficient statistical power for hypothesis testing. The reduced sample size is acknowledged as a limitation, but it does not

compromise the robustness of the analytical approach employed.

To assess the potential influence of non-response bias, early and late responses were compared across key organizational characteristics, including size, sector, and ownership type. No substantial differences were observed between early and late respondents, suggesting that non-response bias was unlikely to systematically distort the findings. Nevertheless, the possibility of residual non-response effects cannot be entirely excluded and is acknowledged in the limitations section.

3.6. Data collection tools

A structured questionnaire was designed to collect quantitative data on key areas, including the organizational profile (such as size, ownership, and sector), compliance, awareness of personal data protection legislation and its requirements, the existence of internal policies, staff training, availability of technical resources, and management support. In addition, two open-ended questions were included to capture respondents' qualitative insights on compliance challenges and solutions.

The questionnaire was administered electronically via Google Forms, enabling broad distribution and convenient access for respondents across different regions and sectors. Before full deployment, the instrument was pretested with a purposive sample of eight participants representing various organizational types and roles. The pretest aimed to assess the clarity, relevance, and contextual appropriateness of the items in Tanzania's business environment. Feedback from this process informed minor adjustments to wording and structure, thereby enhancing the instrument's reliability and validity.

3.7. Operationalization of variables

This study includes one dependent variable, compliance with legislation, and five independent variables representing organizational readiness. These were measured using structured items from the questionnaire, including binary, categorical, and Likert-scale formats. The dependent variable (compliance) was assessed by asking respondents to rate their organization's preparedness to comply with the legislation, using a five-point Likert scale from "Strongly Agree" to "Strongly Disagree."

The independent variables include awareness of legal requirements (familiarity and understanding of the law); presence of internal data protection policies (whether such policies exist within the organization); staff training (whether any employees have received relevant training); and availability of technical resources (staffing and ICT infrastructure) and management support. Table 1 summarizes the operationalization of the variables.

Table 1
Operationalization of variables.

Variable	Description	Type	Measurement approach
Compliance	Organizational preparedness to comply with the legislation	Dependent	1= Strongly Agree, 2= Agree, 3= Neutral, 4= Disagree, 5= Strongly Disagree
Awareness	Knowledge and understanding of the data protection legislation	Independent	1= Strongly Agree, 2= Agree, 3= Neutral, 4= Disagree, 5= Strongly Disagree
Technical resources	Availability of ICT infrastructure	Independent	1= Strongly Agree, 2= Agree, 3= Neutral, 4= Disagree, 5= Strongly Disagree
Internal data protection policy	Existence of formal written data protection policies	Independent	Binary (Yes/No) 1= Strongly Agree, 2= Agree, 3= Neutral, 4= Disagree, 5= Strongly Disagree
Staff training	Whether staff have received training on data protection	Independent	Binary (Yes/No) 1= Strongly Agree, 2= Agree, 3= Neutral, 4= Disagree, 5= Strongly Disagree
Management support	Whether an organizational management supports data protection compliance	Independent	1= Strongly Agree, 2= Agree, 3= Neutral, 4= Disagree, 5= Strongly Disagree

Source: Authors' work.

3.8. Data analysis

Data analysis followed a convergent mixed-methods approach, where quantitative and qualitative data were analyzed separately and then integrated during interpretation.

3.8.1. Quantitative data analysis

Quantitative data analysis followed a structured approach, beginning with data cleaning and descriptive statistics and proceeding to inferential analysis. Data from the Google Form were exported into Microsoft Excel, where cleaning and coding were done before exporting the dataset to SMARTPLS4 for PLS-SEM analysis. Partial Least Squares Structural Equation Modelling (PLS-SEM) was employed because it is more suitable than Covariance-Based SEM (CB-SEM) for studies that emphasize prediction and theory development rather than model fit testing. In this study, the aim was to assess how organizational readiness dimensions predict compliance, not to confirm an established theoretical model. PLS-SEM is advantageous in such contexts, as it performs well with moderate sample sizes, reflective indicators, and data that may deviate from normality. It also provides greater statistical power for estimating direct relationships among constructs, making it appropriate for examining readiness–compliance relationships in emerging research settings, such as data protection compliance in Tanzania.

Descriptive statistics, including frequencies, percentages, means, and standard deviations, were computed to summarize the characteristics of the organizations and responses to key variables such as awareness, policy presence, training, and perceived compliance.

Inferential statistics was done to examine the relationships among the variables. The analysis involved estimating path coefficients between the five independent variables and the dependent variable. To test the strength and significance of these relationships, bootstrapping with 5000 resamples was employed, with statistical significance set at $p < 0.05$. In addition, the coefficient of determination (R^2) was used to assess the model's explanatory power in accounting for variance in organizational compliance. In addition to assessing the coefficient of determination (R^2), model robustness and predictive validity were evaluated using the Q^2 test through the blindfolding procedure and the PLSpredict technique in SmartPLS. Positive Q^2 values indicate predictive relevance, while PLSpredict compares the PLS-SEM model's predictive performance against a linear regression benchmark to confirm out-of-sample accuracy.

3.8.2. Qualitative data analysis

Qualitative data derived from the open-ended responses in the questionnaire were analyzed thematically using the six-phase approach outlined by Braun and Clarke [52], supported by NVivo version 14 for data management and coding. The analysis began with a process of familiarization, in which the researchers read all responses multiple times to immerse themselves in the content and gain a comprehensive understanding of respondents' perspectives on data protection compliance. Initial impressions and potential patterns were noted to guide subsequent analysis.

Following this, the data were coded inductively, allowing themes to emerge naturally from the responses without applying pre-existing theoretical categories. Two independent researchers conducted the initial coding separately to enhance analytical rigour and reduce bias.

The coding process involved systematically identifying and labelling meaningful data segments that related to key issues such as organizational capacity, regulatory uncertainty, and compliance behaviour. Any discrepancies between the researchers' codes were resolved through discussion and consensus.

After generating initial codes, related codes were grouped into broader candidate themes based on shared meaning and conceptual coherence. The themes were iteratively reviewed and refined to ensure internal consistency and distinctiveness across the dataset. Some preliminary themes were merged, redefined, or excluded based on their relevance and strength to responses.

The final themes were then clearly defined and named to capture their central meaning. In some cases, sub-themes were identified to capture more specific dimensions within a broader thematic category. This process allowed for a detailed interpretation that accounted for variations in respondents' experiences across different organizational types and contexts. Verbatim excerpts from participants were selected to illustrate and support each theme, ensuring that the analysis remained grounded in the data and reflected participants' authentic responses.

Throughout the process, care was taken to ensure the analysis's trustworthiness. This was achieved through investigator triangulation, audit trails within NVivo, and collaborative discussions to resolve differences in interpretation. Thematic saturation was considered reached when no new themes or concepts emerged during the later stages of coding and review. The resulting thematic analysis not only enriched the interpretation of the quantitative findings but also provided more profound insights into the organizational, technical, and regulatory dynamics shaping data protection compliance in Tanzania.

3.9. Integration of quantitative and qualitative data

After separate analyses, findings from the quantitative and qualitative components were compared and integrated during the interpretation phase using triangulation. Points of convergence, divergence, and complementarity were identified to provide a holistic understanding of organizational readiness.

3.10. Reliability and validity

To ensure the rigour and credibility of the findings, both reliability and validity of the measurement model were thoroughly assessed as part of the PLS-SEM procedure. Internal consistency reliability was evaluated using Cronbach's alpha and Composite Reliability (CR). A threshold value of 0.70 or higher was used to indicate acceptable reliability for both measures, confirming that the items within each construct consistently measure the same underlying concept [53].

Convergent validity was assessed using the Average Variance Extracted (AVE). An AVE of 0.50 or higher was considered sufficient to demonstrate that each latent construct accounted for the majority of the variance in its indicators. Constructs that met both the CR and AVE criteria were considered to exhibit strong internal validity. Discriminant validity was evaluated using the Heterotrait-Monotrait (HTMT) ratio. The HTMT ratio was used as a more stringent test, with values below 0.85 indicating adequate discriminant validity.

Additionally, multicollinearity diagnostics were performed to assess the degree of redundancy among predictor variables. Variance Inflation Factor (VIF) values were calculated for each independent variable in the model. VIF values below 5.0 were considered acceptable, indicating that multicollinearity was not a concern and that each construct contributed uniquely to the explanation of the dependent variable. This diagnostic ensured that the estimated path coefficients were stable and interpretable.

3.11. Ethical considerations

Informed consent was obtained from all participants before their involvement in the study. Each participant was provided with detailed information about the study's purpose. Participation in the study was entirely voluntary. This ensured that participants made fully informed, autonomous decisions about their involvement.

4. Results

4.1. Profile of respondent organizations

A total of 232 organizations participated in the study, yielding a response rate of approximately 62.7 % based on the initially targeted sample size of 370. The respondents represented a diverse mix of ownership types, organizational sizes, sectors, and experiences with handling personal data. Of the participating organizations, 148 (63.8 %) were from the private sector, 46 (19.8 %) from the public sector, and 33 (14.2 %) were NGOs. Faith-based organizations (FBOs) and other entities such as diplomatic missions and mixed-ownership institutions accounted for the remaining small fraction, with 2 FBOs (0.9 %) and 3 (1.3 %) in other categories.

In terms of organizational size, participation was relatively balanced across all four major categories. Large organizations (250+ employees) accounted for 22.4 % ($n = 52$) of the sample, while medium-sized enterprises (50–249 employees) accounted for 25.9 % ($n = 60$). Small enterprises (10–49 employees) represented the largest group at 26.7 % ($n = 62$), followed closely by micro-enterprises (1–9 employees), which comprised 25.0 % ($n = 58$) of the sample.

The organizations represented a wide array of sectors, with notable concentrations in finance (12.1 %), education (10.3 %), technology (8.6 %), and hospitality and tourism (8.2 %). Other participating sectors included healthcare (6.5 %), agriculture (6.5 %), manufacturing (5.2 %), media (2.2 %), retail and e-commerce (1.7 %), transportation (1.7 %), legal services, construction, energy, real estate, consultancy, insurance, and public utilities, among many others (37 %). This diversity ensured a comprehensive view of readiness and compliance across Tanzania's data-relevant sectors.

In assessing organizational experience with handling personal data, the majority of respondents demonstrated substantial engagement. Out of the 232 organizations surveyed, 45.3 % ($n = 105$) reported having more than five years of experience managing personal data. This indicates a relatively high level of operational maturity in data governance among many participating entities. A further 9.9 % ($n = 23$) had experience ranging from four to five years, while 10.3 % ($n = 24$) reported two to three years of experience. Collectively, these figures suggest that 65.5 % ($n = 152$) of the organizations had been handling personal data for at least two years. Conversely, 25.0 % ($n = 58$) of the organizations had been involved in personal data handling for less than one year, and an additional 9.5 % ($n = 22$) reported exactly one year of experience. These findings highlight a spectrum of data protection experience, ranging from long-established practices in some institutions to more recent engagements, particularly among organizations responding to the enactment of Tanzania's personal data protection legislation.

4.2. Measurement model assessment

The reliability and validity of the measurement model were evaluated to ensure the robustness of the constructs used in the structural equation model. The analysis revealed that all latent variables met the recommended thresholds for internal consistency, convergent validity, and discriminant validity. Specifically, the factor loadings for all indicators ranged from 0.780 to 0.963, exceeding the acceptable minimum of 0.70, indicating strong indicator reliability. The AVE values ranged from 0.692 for management support to 0.916 for compliance, demonstrating sufficient convergent validity across all constructs.

Composite reliability values were also satisfactory, ranging from 0.916 to 0.970, while Cronbach's alpha values varied between 0.855 and 0.970. These results indicate that the constructs exhibit high

internal consistency and reliability. Discriminant validity was confirmed using the HTMT ratio, with all values falling below the recommended threshold of 0.85. Furthermore, multicollinearity diagnostics using VIF values showed that all indicators had VIF values below 5.0, indicating no multicollinearity issues. The maximum VIF observed was 4.016, well within acceptable limits. A summary of the measurement model assessment is presented in Table 3.

4.3. Structural model results

The structural model was assessed to evaluate the hypothesized relationships between the organizational readiness constructs and compliance with the legislation. The results of the path model analysis, including standardized path coefficients, T-statistics, and p-values, are illustrated in Fig. 2 and summarized in Table 2. The model exhibited strong explanatory power, accounting for 74 % of the variance in the dependent variable, compliance ($R^2 = 0.740$).

The path coefficients indicated significant, positive relationships between all five independent variables and compliance. Specifically, technical resources (TR → CO) had the most substantial effect with a path coefficient of 0.412 ($T = 11.958$, $p < 0.001$), followed closely by awareness (AW → CO) at 0.405 ($T = 13.449$, $p < 0.001$) and staff training (ST → CO) at 0.400 ($T = 12.902$, $p < 0.000$). Internal data protection policy (IP → CO) also demonstrated a significant positive effect, with a coefficient of 0.370 ($T = 11.125$, $p < 0.000$), while management support (MS → CO) had the smallest but still significant effect at 0.292 ($T = 9.806$, $p < 0.001$). These results indicate that all proposed readiness factors contribute meaningfully to organizational compliance with the personal data protection legislation. Fig. 2 presents the structural equation model.

To further assess the predictive validity of the structural model, the Q^2 test was performed using the blindfolding procedure in SmartPLS. The obtained Q^2 value for the compliance construct was 0.487, indicating substantial predictive relevance of the model. In addition, the PLSpredict procedure was applied to evaluate out-of-sample predictive performance. The results showed that the PLS-SEM model yielded lower root mean square errors (RMSEs) across all indicators than the linear regression benchmark, confirming its superior predictive accuracy. These findings collectively demonstrate that the model has strong predictive capability and robust explanatory power for organizational compliance.

Table 2
Summary of path model results.

Path	Path Coefficients	T statistics (|O/STDEV|)	P-values
AW -> CO	0.405	13.449	0.001
IP -> CO	0.37	11.125	0.000
MS -> CO	0.292	9.806	0.001
ST -> CO	0.4	12.902	0.000
TR -> CO	0.412	11.958	0.001

Source: Authors' work.

4.4. Thematic analysis of qualitative responses

4.4.1. Overview of emergent themes from open-ended responses

Thematic analysis was conducted on the responses related to challenges in complying with personal data protection legislation, producing over 180 individual codes. These were inductively refined into sixteen sub-themes, which were grouped into four overarching thematic categories: (1) awareness and capacity building, (2) governance and institutional support, (3) resource and operational constraints, and (4) policy and regulatory barriers. These categories represent the most frequently cited areas of concern and are detailed in the next section. A summary table of the sub-themes and corresponding codes is presented in Appendix A.

Thematic analysis of responses to challenges yielded over 200 individual codes. These were inductively refined into sixteen sub-themes, which were grouped into three overarching thematic categories: (1) awareness and capacity building, (2) governance and policy support, and (3) technical and security compliance measures. These categories represent the most frequently cited areas of concern and are detailed in

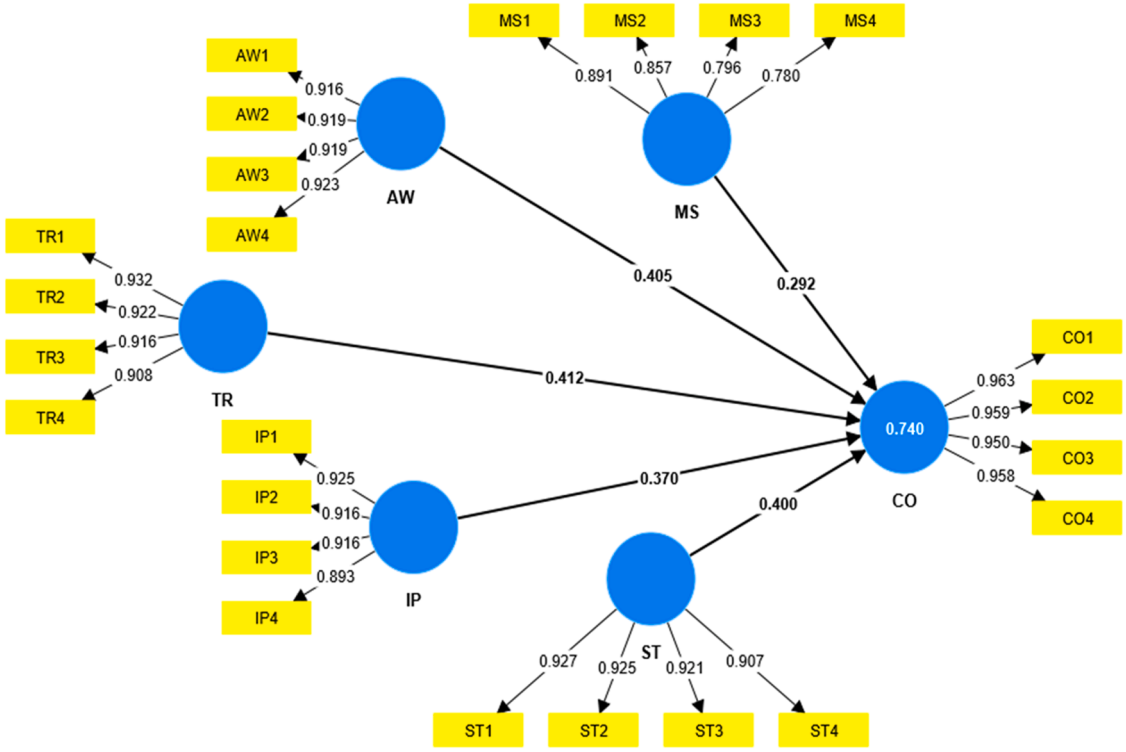

Fig. 2. Structural equation model path diagram.

Table 3
Summary of measurement model assessment results.

Latent variable	Indicator	Loading	AVE	Composite reliability	Cronbach's Alpha	Discriminant Validity (<0.85)	Maximum VIF
AW (Awareness)	AW1	0.916	0.845	0.945	0.939	Yes	3.324
	AW2	0.919					3.845
	AW3	0.919					3.901
	AW4	0.923					3.995
TR (Technical Resources)	TR1	0.932	0.845	0.96	0.939	Yes	3.735
	TR2	0.922					4.016
	TR3	0.916					3.8
	TR4	0.908					3.477
IP (Internal Data Protection Policy)	IP1	0.925	0.833	0.947	0.933	Yes	3.533
	IP2	0.916					3.772
	IP3	0.916					3.512
	IP4	0.893					3.136
ST (Staff Training)	ST1	0.927	0.846	0.96	0.94	Yes	3.693
	ST2	0.925					3.833
	ST3	0.921					4.006
	ST4	0.907					3.557
MS (Management Support)	MS1	0.891	0.692	0.916	0.855	Yes	2.105
	MS2	0.857					2.08
	MS3	0.796					1.89
	MS4	0.78					1.827
CO (Compliance)	CO1	0.963	0.916	0.97	0.97	Yes	3.584
	CO2	0.959					3.106
	CO3	0.95					3.97
	CO4	0.958					3.896

Source: Authors' work.

the next section. A summary table of the sub-themes and frequency counts is presented in Appendix A, while a visual representation of commonly used terms is shown in the word cloud (Fig. 3).

4.4.2. Thematic categories

The qualitative data analysis was organized into two main components: challenges and solutions, as detailed in the following subsections.

4.4.2.1. Challenges. The thematic analysis revealed four principal categories of challenges: (1) Awareness and Capacity Building, (2) Governance and Institutional Support, (3) Resource and Operational Constraints, and (4) Policy and Regulatory Barriers.

Awareness and capacity building. The most prominent challenges reported centered around a general lack of awareness and limited capacity among staff and leadership. Many respondents indicated that their employees lacked even basic knowledge of data protection laws and were unaware of their specific responsibilities under the legislation. As one participant noted, "*Our staff are not aware of what personal data protection actually requires.*" Others highlighted the absence of structured training programs, especially for newly appointed DPOs, with one respondent stating, "*As a DPO, I have never received any official training on what my duties entail.*"

Furthermore, several respondents noted the lack of clear, accessible guidance on applying data protection practices in daily operations. For instance, one participant commented, *"There is no manual or toolkit to help us interpret the law and implement it."* Related to this, respondents expressed uncertainty about the scope of compliance, noting that the law's provisions were not sufficiently explained. One respondent observed, *"We do not even know which data needs to be protected and how."*

Taken together, these responses indicate that limited awareness, lack of training, and uncertainty about compliance responsibilities are common across organizations, particularly among staff involved in operational data handling.

Fig. 3. Word Cloud of commonly cited themes in compliance solutions.
Source: Generated by authors using NVivo 14 software from open-ended qualitative responses (2025).

Governance and institutional support. A second cluster of responses pointed to governance-level weaknesses within organizations. Numerous respondents reported lacking the structural and leadership support needed to implement compliance measures effectively. Even where a DPO had been appointed, many noted that the role was unsupported, isolated, or sidelined. A respondent explained, "*There is no coordinated effort, everyone is doing their own thing, and no one is backing the DPO*". Another added, "*The DPO is left to figure everything out alone. There is no team, no collaboration*".

Leadership commitment was also called into question. Respondents noted that management often viewed data protection as an external obligation rather than a core organizational concern. One respondent shared, *"My role is barely recognized. I am treated as an obstacle, not as someone fulfilling a legal mandate*".

Additionally, weak internal accountability and the absence of governance frameworks were cited as significant barriers. Organizations reported having no internal compliance structures, no monitoring, and no escalation mechanisms. As noted by one respondent, "*There is no clear internal structure to oversee data privacy issues, so nothing moves forward*".

Participants' accounts indicate limited internal coordination and leadership engagement in data protection activities, with compliance roles poorly integrated into existing governance structures. The isolation of DPOs and the absence of formal oversight mechanisms suggest that

data protection responsibilities are not yet consistently embedded across organizational units.

Resource and operational constraints. A significant number of responses pointed to practical limitations tied to financial, human, and technical resources. High compliance costs, particularly training fees and registration expenses, were widely reported. One participant wrote, "*We cannot afford the training; the fees are too high for a small company like ours*". Other respondents mentioned a lack of allocated budget for data protection, even within government-affiliated entities.

On the technical side, many respondents described struggling with outdated IT infrastructure and a lack of cybersecurity tools. Several respondents stated that their systems lacked even basic protections such as encryption, secure storage, or access controls. "*We do not have any digital safeguards; it is just basic Excel sheets and folders*," one respondent admitted.

Challenges also emerged around data governance processes. Respondents cited difficulties in maintaining consent records, documenting data transfers, and tracking access logs. For instance, respondents explained, "*Capturing, tracking, and updating user consent in compliance with data protection laws is challenging, especially when data is collected through various channels such as physical forms, digital platforms, and verbal agreements"*. These issues were compounded by understaffing and a lack of in-house expertise.

The responses indicate that financial, technical, and human resource constraints limit organizations' ability to consistently implement data protection measures. These constraints are reflected in reliance on manual processes, outdated systems, and limited internal expertise.

Policy and regulatory barriers. A common concern was the absence of clear internal policies and procedures to guide compliance with the legislation. Many respondents reported that they had not yet developed privacy policies, consent protocols, or breach response procedures. One respondent noted, "*We do not have any internal documents or guidelines; everything is reactive*". Another added, "*There is no formal data protection policy in place, so staff are unsure of what actions are appropriate or required*".

Participants' responses suggest that unclear internal procedures and limited implementation guidance affect how organizations interpret and apply legislative requirements in practice. This contributes to compliance approaches that are primarily reactive rather than structured.

4.4.2.2. Solutions. Thematic analysis revealed a wide range of solutions organized into three categories: (1) Awareness and Capacity Building, (2) Governance and Policy Support, and (3) Technical and Security Compliance Measures.

Awareness and capacity building. The most frequently cited recommendation emphasized the need for widespread, continuous training. Some respondents stressed the importance of both initial and refresher sessions tailored to different organizational roles, as one respondent commented, "Training should be conducted every quarter." *At the same time,* another noted, *"We need more and regular awareness training"*. Others demanded affordable training fees, as pointed out by one respondent: "Training fee for the DPOs is too high to encourage participation in PDP."

There was also strong demand for stakeholder-specific awareness, particularly for top-level management. Respondents stated that sensitizing executive leaders would lead to better institutional support for compliance activities. One respondent advised, *"Train the managers of organizations so they can be aware of the risks associated with data protection"*. Another respondent suggested, *"PDPC to conduct awareness sessions with CEOs and share the role of DPOs and reporting structure"*.

Some respondents also called for public-facing campaigns to improve general understanding of privacy rights and legal obligations. One comment read, *"Public awareness is very important"*, while another respondent emphasized, *"Governments and organizations should invest in public education campaigns to raise awareness about data protection rights*".

Governance and policy support. Respondents emphasized the need for more explicit regulatory guidance and for PDPC to be more proactive. Many recommended issuing sector-specific compliance guidelines and simplified templates for key documents, such as privacy policies, consent forms, and breach reporting protocols. One suggestion read, *"Develop simple guidelines for Civil Society Organization (CSOs) and small organizations,"* and another elaborated, *"PDPC should provide ready-to-use templates to help grassroots organizations save time and reduce legal complexity"*.

There were also repeated calls for greater regulatory flexibility and responsiveness. For example, a respondent urged, *"Have effective mechanisms for approval for transfer of data outside… it is not practical to ask for approval every time,"* while another respondent recommended, *"Create a compliance incentive and engagement strategy*".

Technical and security compliance measures. Respondents proposed concrete technical solutions and infrastructure improvements to support compliance. Recommendations included stronger cybersecurity practices, automated data management tools, and privacy-by-design frameworks. One detailed response proposed the *"implementation of encryption, access controls, and regular penetration testing"*, while another emphasized *"data mapping and inventory tools to maintain a live inventory of personal data"*.

Several called for the provision of affordable or subsidized compliance tools for small organizations. One submission read, "The government should consider offering subsidized data protection software or facilitate partnerships with local tech firms".

Respondents also requested practical mechanisms for incident management, including the development of formal data breach response plans, consent management platforms, and tools for handling data subject requests. One respondent proposed, *"Deploy tools to automate responses to Data Subject Access Requests (DSARs)"*, while another called for *"clear procedures for handling data breaches, including notification timelines and mitigation steps"*.

Several responses called for formalizing and recognizing the DPO role. Some advocated for certification programs and standardized training pathways. For instance, one respondent commented, *"Special certification courses for DPOs like that of CPA(T),"* while another respondent suggested, *"Each DPO upon appointment must be trained by the agency itself first*".

4.5. Integration of quantitative and qualitative findings

Quantitative results identified key predictors of compliance, particularly technical resources ($\beta = 0.412$), awareness ($\beta = 0.405$), and staff training ($\beta = 0.400$), while qualitative responses illuminated the underlying factors behind these relationships. For instance, lack of staff capacity and technical infrastructure reported qualitatively aligned with the statistical significance of those variables. Similarly, the importance of management support was reflected not only in quantitative modelling ($\beta = 0.292$) but also in respondents' calls for top-level leadership engagement and policy guidance. Together, the findings revealed that while many organizations have foundational structures in place, deeper institutional and contextual gaps persist.

5. Discussion

This study examined organizational readiness for compliance with Tanzania's PDPA, identified key barriers to implementation, and explored practical measures for strengthening compliance. The findings indicate that organizational readiness is significantly associated with

compliance, with all five examined readiness dimensions showing positive effects. Technical resources, awareness, and staff training emerged as the strongest predictors, while internal data protection policies and management support exhibited comparatively weaker but still significant effects. At the same time, readiness levels varied across organizational types, with SMEs and NGOs facing more pronounced constraints. These findings suggest that the effectiveness of the PDPA depends not only on the presence of a legal framework but also on the extent to which organizations possess the technical, human, and institutional capacity required to operationalize legal obligations.

5.1. Interpretation of findings

The results show that technical resources have the strongest association with compliance ($\beta = 0.412$). Within the institutional theory framework, this reflects the influence of the regulative pillar, which emphasizes formal rules and enforcement mechanisms, and the organizational capacity to implement them through concrete systems and controls [15]. In the context of data protection, technical resources such as secure IT infrastructure, access controls, encryption, and data management tools enable organizations to translate legal requirements into operational practices. This interpretation is consistent with empirical studies cited in the literature review, which identify technical readiness and privacy-by-design mechanisms as critical enablers of compliance [17,28]. While some studies caution that financial or technical investment alone may not guarantee compliance without broader institutional capacity [16,29], the present findings suggest that in Tanzania's early-stage regulatory environment, basic technical capability remains a central condition for compliance.

Awareness and staff training were also found to be strong and statistically significant predictors of compliance ($\beta = 0.405$ and $\beta = 0.400$, respectively). These findings align with the cultural-cognitive pillar of institutional theory, which emphasizes shared understanding, knowledge, and meaning systems that shape organizational behaviour [15]. Organizations in which staff understand the PDPA requirements and their data protection responsibilities are more likely to consistently adopt compliant practices. This interpretation is directly supported by prior studies referenced in the literature review, which report that limited awareness and insufficient training undermine compliance, particularly in SMEs and organizations operating in emerging regulatory contexts [9,18,23]. The qualitative findings reinforce this interpretation, as respondents frequently reported uncertainty about legal obligations, limited training opportunities, and a lack of clarity regarding compliance roles.

The positive relationship between internal data protection policies and compliance ($\beta = 0.370$) reflects the normative pillar of institutional theory, which emphasizes organizational norms, rules, and governance structures [15]. Formal policies provide a framework for expected behaviour and support the standardization of data protection practices across organizations. This finding is consistent with the literature, which indicates that internal governance arrangements and documented policies contribute to more systematic compliance efforts [16,19]. However, qualitative evidence from this study suggests that the presence of policies does not always translate into effective implementation, indicating that normative structures may be only partially institutionalized in some organizations.

Although management support was statistically significant, it exhibited the weakest effect among the readiness dimensions ($\beta = 0.292$). Institutional theory suggests that leadership commitment plays a vital role in legitimizing organizational responses to regulatory pressure [15]. The relatively weaker effect observed here contrasts with findings from studies conducted in more mature regulatory environments, where executive leadership has been identified as a dominant driver of compliance [28,29]. In the Tanzanian context, this may reflect the relatively recent enactment of the PDPA, in which management support is often formally expressed but has not yet been fully integrated into strategic and operational decision-making. This interpretation is supported by qualitative responses highlighting limited senior management engagement and weak institutional recognition of data protection roles.

The qualitative findings provide important contextual insight into how institutional constraints shape readiness and compliance in practice. Respondents highlighted limited technical infrastructure, lack of trained personnel, unclear regulatory guidance, and cost-related challenges as key barriers. These constraints were more frequently reported by SMEs and NGOs, supporting existing evidence that smaller organizations face disproportionate compliance burdens due to limited resources and institutional capacity [9,32]. In contrast, larger organizations were more likely to report formal policies, training programmes, and structured compliance initiatives, indicating uneven institutionalization of compliance across sectors.

The findings support the central argument of institutional theory that compliance is shaped by the interaction of regulative requirements, normative structures, and cultural-cognitive understandings, rather than by legal mandates alone [14,15]. In Tanzania's emerging data protection regime, compliance appears strongest where technical capability, awareness, and training are present, and weakest where institutional capacity and support mechanisms remain underdeveloped. This highlights the importance of regulatory and policy approaches that combine enforcement with capacity building and institutional support tailored to the organizational context.

Additionally, the findings support the view that compliance with personal data protection legislation is fundamentally an organisational process. The strong association between technical resources and compliance indicates that, in emerging regulatory contexts, basic infrastructural and system capacities may play a more decisive role than formal policy provisions alone. This reinforces analytical perspectives that conceptualise data protection compliance as a socio-technical outcome, dependent on the alignment of organisational structures, human capacity, and enabling technologies rather than awareness or legislation in isolation.

5.2. Study implications

The findings of this study have several important implications for theory, policy, and organizational practice. From a theoretical perspective, the study extends the application of institutional theory to the emerging field of personal data protection in low- and middle-income countries. By empirically linking organizational readiness dimensions to the regulative, normative, and cultural-cognitive pillars, the study demonstrates how institutional pressures are translated into compliance behaviour in a newly established regulatory environment. This contributes to the literature by moving beyond descriptive accounts of data protection legislation to provide evidence on how institutional capacity conditions shape organizational responses to regulation.

From a policy and regulatory perspective, the results highlight that legal enforcement alone is unlikely to ensure effective compliance with the Personal Data Protection Act. The strong influence of technical resources, awareness, and staff training suggests that regulators should complement enforcement mechanisms with targeted capacity-building initiatives. These may include sector-specific guidance, structured awareness programmes, and practical compliance tools, particularly for SMEs and NGOs that face disproportionate resource constraints. Such differentiated regulatory support can help reduce compliance gaps while maintaining the integrity of the legal framework.

At the organizational level, the findings underscore the importance of viewing data protection compliance as an institutional process rather than a purely technical or legal obligation. Organizations seeking to improve compliance should prioritize foundational technical safeguards alongside sustained investment in staff training and awareness. The results also suggest that formal policies and management endorsement, while necessary, are insufficient in isolation unless accompanied by operational integration and active leadership engagement. Embedding

data protection responsibilities within everyday organizational routines is, therefore, critical for sustaining compliance over time.

Collectively, these implications emphasize that strengthening personal data protection in Tanzania requires coordinated efforts across regulatory institutions, organizational leadership, and professional practice. By addressing technical, human, and institutional dimensions simultaneously, stakeholders can support more consistent and meaningful compliance with the PDPA as the regulatory framework continues to mature.

5.3. Limitations of the study

This study has several limitations that should be considered when interpreting the findings. First, although the achieved sample size ($n = 232$) was adequate for the prediction-oriented PLS-SEM analysis, it was lower than the initially estimated target sample size. This reduction was mainly attributable to non-response and partial survey attrition, which are common in organizational surveys, particularly in newly regulated environments. While appropriate analytical techniques were applied and non-response bias was assessed, the findings should be interpreted with this constraint in mind Table 4.

Second, the study relied primarily on self-reported data from designated organizational respondents, which may be subject to social desirability or perceptual bias. However, using senior staff and data protection officers as key informants, combined with the integration of qualitative responses, helped mitigate this risk by providing contextual validation of the quantitative results.

Third, the cross-sectional design captures organizational readiness and compliance at a single point in time, shortly after the PDPA's enactment. As institutional arrangements and compliance practices continue to evolve, longitudinal research would be valuable for examining how organizational readiness and compliance dynamics change as the regulatory framework matures.

Finally, while this study focused on key organizational readiness dimensions grounded in institutional theory, other factors such as regulatory enforcement practices, sector-specific requirements, and external support mechanisms were beyond the scope of the analysis. Future studies could extend this work by incorporating these elements to further enrich the understanding of data protection compliance in emerging regulatory contexts.

Despite these limitations, the study provides robust, timely empirical evidence on organizational readiness and compliance with Tanzania's personal data protection legislation, offering a strong foundation for future research and policy development.

6. Conclusion

This study examined the readiness and compliance of organizations in Tanzania with the country's PDPA and revealed differentiated capacity gaps across organizational types. While larger organizations demonstrate relatively stronger preparedness, particularly in awareness, internal policies, and technical controls, SMEs and NGOs face systemic constraints, including limited technical infrastructure, insufficient staff training, and weak governance support. These findings suggest that a uniform compliance approach is unlikely to be effective. Consequently, regulators should prioritize sector-specific guidance, simplified compliance frameworks for SMEs and NGOs, and targeted capacity-building initiatives focused on awareness, policy development, training, technical capacity, and leadership support. Large organizations, on the other hand, should strengthen internal accountability mechanisms and leadership-driven oversight of compliance to sustain and deepen compliance practices. Generally, effective implementation of the PDPA will depend on coordinated regulatory support, differentiated compliance strategies, and sustained investment in institutional capacity to build a culture of responsible data governance across Tanzania.

Table 4
Thematic categorization of challenges faced by organization.

Codes	Subthemes	Final Themes
Lack of staff awareness, Employees unaware of compliance roles, unaware of personal data protection legislation requirements, Poor understanding of legal obligations	Knowledge Gaps	Awareness and Capacity Building
No regular training, Insufficient training, DPO not trained, Lack of practical workshops, No training for new staff	Training Limitations	
Insufficient guidance materials, Lack of clear manuals or templates, No awareness brochures or policies, Missing consent forms	Learning Resources Deficit	
Confusion about what the law requires, Partial understanding among staff and leadership, Misinterpretation of the law	Interpretation Challenges	
Lack of Coordination, No recognition, No staff assigned to data governance	Structural Gaps	Governance and Institutional Support
Management not supportive, Leadership uninformed, DPO disrespected or undermined, No internal champions	Leadership and Accountability Issues	
DPO works in isolation, Lack of collaboration, No defined roles or team for data protection	Coordination and Role Clarity	
No internal compliance monitoring, No governance structure for privacy, Governance not aligned with PDPC	Internal Governance Deficiency	
High registration fees, Expensive training costs, No financial support, Lack of budget for compliance	Financial Constraints	Resource and Operational Constraints
Outdated IT infrastructure, Insecure systems, No encryption, Legacy data storage	Technical Limitations	
Difficulty tracking consent, No audit logs, Inadequate reporting processes, Manual data handling	Data Governance Challenges	
Limited staff capacity, Overworked compliance staff, No legal or IT experts in-house	Human Resource Limitations	
No response from PDPC, Helpdesk delays, Contradictory guidance, long processing times	Regulatory Responsiveness Gaps	Policy and Regulatory Barriers
Complex registration process, Cross-border compliance delays, Difficult to amend permits	Procedural Burdens	
Lack of clear implementation guidelines, Unclear scope of obligations, Legislation too general	Regulatory Ambiguity	
No stakeholder communication strategy, Weak engagement with CSOs and SMEs, No local support hubs	Institutional Communication Gaps	

Funding

This research did not receive any specific grant from funding agencies.

Declaration of generative AI use

During the preparation of this manuscript, generative AI tools were used to support language editing and structural refinement. All content generated using these tools was critically reviewed, revised, and validated by the authors, who take full responsibility for the integrity, accuracy, and originality of the final manuscript.

Data availability

The data generated and analyzed during this study are not publicly available due to confidentiality and organizational identification concerns, but are available from the corresponding author upon reasonable request.

CRediT authorship contribution statement

Noe Nnko: Writing – review & editing, Conceptualization. **Petro Nzowa:** Writing – review & editing, Conceptualization. **Franklin Mungulluh:** Formal analysis. **Emmanuel Mkilia:** Supervision. **Hamza Malombe:** Formal analysis. **Godbless Minja:** Investigation, Formal analysis. **Cesilia Mambile:** Writing – original draft, Methodology. **Augustino Mwogosi:** Writing – review & editing, Writing – original draft, Methodology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors thank all participating organisations and individuals who contributed valuable insights. We also acknowledge the administrative and technical support from the Personal Data Protection Commission, Tanzania.

The authors acknowledge all organizations and respondents who participated in this study for their time and valuable insights. The authors also acknowledge the institutional support that facilitated access to participating organizations during data collection.

Appendix A

Sub-theme	Theme
Awareness Initiatives	Awareness and Capacity Building
Capacity Support	
Stakeholder Education	
Training Programs	
Capacity Support	
Institutional Support	Governance and Policy Support
Monitoring and Review	
Policy and Framework Development	
Regulatory Compliance	
Stakeholder Engagement	
Strategic Alignment	
Data Handling Controls	Technical and Security Compliance Measures
DPIA Implementation	
Infrastructure Readiness	
Security Controls	
Technical Tools and Systems	

References

[1] V. Estrada-Galiñanes, K. Wac, Collecting, exploring and sharing personal data: why, how and where, Data Science 3 (2020) 79–106, https://doi.org/10.3233/DS-190025.
[2] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L.F. Cranor, S. Komanduri, et al., Nudges for privacy and security, ACM. Comput. Surv. 50 (2018) 1–41, https://doi.org/10.1145/3054926.
[3] A.E. Babatope, I.P. Adewumi, D.O. Ajisafe, K.O. Adepoju, A.R. Babatope, Assessing the factors militating against the effective implementation of electronic health records (EHR) in Nigeria, Sci. Rep. 14 (2024) 31398, https://doi.org/10.1038/s41598-024-83009-y.
[4] S. Bhatia, J. Malhotra, CSPCR: cloud security, privacy and compliance readiness - A trustworthy framework, Int. J. Electr. Comput. Eng. 8 (2018) 3756–3766, https://doi.org/10.11591/ijece.v8i5.pp3756-3766.
[5] C. Tolani, Pareek ProfJ, Introduction to Data Protection frameworks: a review, Int. J. Adv. Res. Sci., Commun. Technol. (2024) 251–255, https://doi.org/10.48175/IJARSCT-18732.
[6] R. Creemers, China's emerging Data Protection framework, SSRN Electr. J. (2021), https://doi.org/10.2139/ssrn.3964684.
[7] S.A. Oyetunji, Investigating data protection compliance challenges, Int. J. Innovative Sci. Res. Technol. (IJISRT) (2024) 2131–2147, https://doi.org/10.38124/ijisrt/IJISRT24AUG1583.
[8] Y. Smirnova, V. Travieso-Morales, Tech startups and general data protection regulation: an empirical exploration of compliance challenges, J. Small Bus. Enterprise Develop. 32 (2025) 54–82, https://doi.org/10.1108/JSBED-09-2024-0495.
[9] P. Chatsuwan, T. Phromma, N. Surasvadi, S. Thajchayapong, Personal data protection compliance assessment: a privacy policy scoring approach and empirical evidence from Thailand's SMEs, Heliyon. 9 (2023), https://doi.org/10.1016/j.heliyon.2023.e20648.
[10] R. Huising, S.S. Silbey, Accountability infrastructures: pragmatic compliance inside organizations, Regul. Gov. 15 (2021), https://doi.org/10.1111/rego.12419.
[11] H.N. Chua, A. Herbland, S.F. Wong, Y. Chang, Compliance to personal data protection principles: a study of how organizations frame privacy policy notices, Telemat. Inform. 34 (2017) 157–170, https://doi.org/10.1016/j.tele.2017.01.008.
[12] A. Mwogosi, R. Simba, Digital policy and governance frameworks for EHR systems in Tanzania: a scoping review, Digital Policy, Regul. Governance (2025), https://doi.org/10.1108/DPRG-11-2024-0289.
[13] D. Shao, F. Ishengoma, A. Nikiforova, M. Swetu, Comparative analysis of data protection regulations in East African countries, Digital Policy, Regul. Governance (2024), https://doi.org/10.1108/DPRG-06-2024-0120.
[14] D.G. Magnano, S.M.F. Grimstad, R. Glavee-Geo, F. Anwar, Disentangling circular economy practices and firm's sustainability performance: a systematic literature review of past achievements and future promises, J. Environ. Manage 353 (2024) 120138, https://doi.org/10.1016/j.jenvman.2024.120138.
[15] S.M. Gonçalves, R.V. Silva, Discussing the potential of the institutional theory to leverage service-dominant logic advancements, Eur. J. Manage. Stud. 26 (2021) 3–16, https://doi.org/10.1108/EJMS-01-2021-0004.
[16] S. Prabowo, M. Abdurohman, H.H. Nuha, S. Sutikno, Identifying and validating critical factors in designing a comprehensive data protection impact assessment (DPIA) framework for Indonesia, In. J. Safety Secur. Eng. 15 (2025) 113–126, https://doi.org/10.18280/ijsse.150113.
[17] B.M. Kalema, M. Mokgadi, Developing countries organizations' readiness for Big Data analytics, Problems Perspect. Manage. 15 (2017) 260–270, https://doi.org/10.21511/ppm.15(1-1).2017.13.
[18] F. De Prieelle, M. De Reuver, J. Rezaei, The role of ecosystem data governance in adoption of data platforms by Internet-of-things data providers: case of Dutch horticulture industry, IEEe Trans. Eng. Manage 69 (2022) 940–950, https://doi.org/10.1109/TEM.2020.2966024.
[19] B.M.V. Bernardo, H.S. Mamede, J.M.P. Barroso, V.M.P.D dos Santos, Data governance & quality management—Innovation and breakthroughs across different fields, J. Innov. Knowledge 9 (2024) 100598, https://doi.org/10.1016/j.jik.2024.100598.
[20] J.J. Tom, A. Wilfred, N.P. Anebo, B.A Onyekwelu, An analysis of data protection regulation compliance monitoring and enforcement, Int. J. Comput., Intell. Secur. Res. (IJCISR) 2 (2023).

[21] L.H. Iwaya, M.A. Babar, A. Rashid, Privacy Engineering in the wild: understanding the practitioners' Mindset, organizational aspects, and current practices, IEEE Trans. Softw. Eng. 49 (2023) 4324–4348, https://doi.org/10.1109/TSE.2023.3290237.
[22] R. Cherekar, Cloud Data governance: policies, compliance, and ethical considerations, Int. J. AI, BigData, Comput. Manage. Stud. 3 (2022) 24–31, https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I2P103.
[23] A.T. Oyewole, B.B. Oguejiofor, N.E. Eneh, C.U. Akpuokwe, S.S. Bakare, Data privacy laws and their financial impact on financial technology companies: a review, Comput. Sci. IT Res. J. 5 (2024) 628–650, https://doi.org/10.51594/csitrj.v5i3.911.
[24] I.M. Leghemo, O.D. Segun-Falade, C.S. Odionu, C. Azubuike, A collaborative model for data governance: enhancing integration across multi-line businesses, Gulf J. Advance Bus. Res. 3 (2025) 47–63, https://doi.org/10.51594/gjabr.v3i1.66.
[25] R. Aserkar, A. Seetharaman, J.A.M. Chu, V. Jadhav, S. Inamdar, Impact of personal data protection (PDP) regulations on operations workflow, Human Syst. Manage. 36 (2017) 41–56, https://doi.org/10.3233/HSM-161631.
[26] T.R. Chhetri, A. Kurteva, R.J. DeLong, R. Hilscher, K. Korte, A. Fensel, Data protection by design tool for automated GDPR compliance verification based on semantically modeled informed consent, Sensors 22 (2022) 2763, https://doi.org/10.3390/s22072763.
[27] R.M. de Carvalho, C. Del Prete, Y.S. Martin, R.M. Araujo Rivero, M. Önen, F. P. Schiavo, et al., Protecting citizens' Personal Data and privacy: joint effort from GDPR EU cluster research projects, SN. Comput. Sci. 1 (2020) 217, https://doi.org/10.1007/s42979-020-00218-8.
[28] Julakanti S.R., KiranmayeeSattiraju N.S., Julakanti R. Data Protect. Through Governance Frameworks. ArXiv Preprint ArXiv:250210404 2025.
[29] B.M.V. Bernardo, H.S. Mamede, J.M.P. Barroso, V.M.P.D dos Santos, Data governance & quality management—Innovation and breakthroughs across different fields, J. Innov. Knowl. 9 (2024) 100598, https://doi.org/10.1016/j.jik.2024.100598.
[30] A. Mabina, N. Rafifing, B. Seropola, T. Monageng, P. Majoo, Challenges in IoMT adoption in healthcare: focus on ethics, Security, and privacy, J. Inf. Syst. Inf. 6 (2024) 3162–3184, https://doi.org/10.51519/journalisi.v6i4.960.
[31] A.D. Ochigbo, A. Tuboalabo, T.T. Labake, O. Layode, Regulatory compliance in the age of data privacy: a comparative study of the Nigerian and U.S. legal landscapes, Int. J. Appl. Res. Soc. Sci. 6 (2024) 1355–1370, https://doi.org/10.51594/ijarss.v6i7.1297.
[32] A. Johannsen, D. Kant, R. Creutzburg, Measuring IT security, compliance and data governance within small and medium-sized IT enterprises, in: IS and T International Symposium on Electronic Imaging Science and Technology, Society for Imaging Science and Technology, 2020, https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-252 vol. 2020.
[33] O. Klymenko, O. Kosenkov, S. Meisenbacher, P. Elahidoost, D. Mendez, F. Matthes, Understanding the implementation of technical measures in the process of data privacy compliance: a qualitative study, in: International Symposium on Empirical Software Engineering and Measurement, IEEE Computer Society, 2022, pp. 261–271, https://doi.org/10.1145/3544902.3546234.
[34] A.O. Salako, J.A. Fabuyi, N.T. Aideyan, O. Selesi-Aina, D.L. Dapo-Oyewole, O. O. Olaniyi, Advancing information governance in AI-driven cloud ecosystem: strategies for enhancing data security and meeting regulatory compliance, Asian J. Res. Comput. Sci. 17 (2024) 66–88, https://doi.org/10.9734/ajrcos/2024/v17i12530.
[35] T. Brée, M. Jagals, E. Karger, Preparation is everything – Organizational readiness factors for acting in data ecosystems, Die Unternehmung 77 (2023) 24–41, https://doi.org/10.5771/0042-059x-2023-1-24.
[36] V.R. Kommidi, S. Padakanti, V. Pendyala, Securing the cloud: a comprehensive analysis of data protection and regulatory compliance in rule-based eligibility systems, Int. J. Res. Comput. Appl. Inf. Technol. (IJRCAIT) 7 (2024) 432–447, https://doi.org/10.5281/zenodo.13991239.
[37] S. Naik, Cloud-based Data governance: ensuring security, compliance, and privacy, Eastasouth J. Inf. Syst. Comput. Sci. 1 (2023) 69–87.
[38] E. Coche, A. Kolk, V. Ocelík, Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business, J. Int. Business Policy 7 (2024) 112–127, https://doi.org/10.1057/s42214-023-00172-1.
[39] D. Kaul, AI-powered autonomous compliance management for multi-region data governance in cloud deployments, J. Current Sci. Res. Rev. 2 (2024) 82–98.
[40] T. van den Broek, A.F. van Veenstra, Governance of big data collaborations: how to balance regulatory compliance and disruptive innovation, Technol. Forecast. Soc. Change 129 (2018) 330–338, https://doi.org/10.1016/j.techfore.2017.09.040.
[41] J. Hardman, Fixing the misalignment of the concession of corporate legal personality, Legal Stud. 43 (2023) 443–460, https://doi.org/10.1017/lst.2022.44.
[42] N. Lieftink, C. dos S Ribeiro, M. Kroon, G.B. Haringhuizen, A. Wong, L.H.M. van de Burgwal, The potential of federated learning for public health purposes: a qualitative analysis of GDPR compliance, Europe, 2021, Eurosurveillance 29 (2024), https://doi.org/10.2807/1560-7917.ES.2024.29.38.2300695.
[43] N.A. Zaguir, G.H. de Magalhães, Mesquita de, M. Spinola, Challenges and enablers for GDPR compliance: systematic Literature review and future research directions, IEEE Access. 12 (2024) 81608–81630, https://doi.org/10.1109/ACCESS.2024.3406724.
[44] Z. Tang, C. Zeng, Y. Zeng, Research on data security in industry 4.0 manufacturing industry against the background of privacy protection challenges, Int. J. Comput. Integr. Manuf. (2024), https://doi.org/10.1080/0951192X.2024.2319656.
[45] P. Ryan, M. Crane, R. Brennan, GDPR compliance tools: best practice from RegTech. Lecture Notes in Business Information Processing, vol. 417, Springer Science and Business Media Deutschland GmbH, 2021, pp. 905–929, https://doi.org/10.1007/978-3-030-75418-1_41.
[46] Š. Grigaliūnas, M. Schmidt, R. Brūzgienė, P. Smyrli, S. Andreou, A. Lopata, Holistic information security management and compliance framework, Electronics. (Basel) 13 (2024) 3955, https://doi.org/10.3390/electronics13193955.
[47] F. Inasius, Factors influencing SME tax compliance: evidence from Indonesia, Int. J. Public Administration 42 (2019) 367–379, https://doi.org/10.1080/01900692.2018.1464578.
[48] D.L. Morgan, Paradigms lost and pragmatism regained, J. Mix. Methods Res. 1 (2007) 48–76, https://doi.org/10.1177/2345678906292462.
[49] J.W. Creswell, V.L.P. Clark, Designing and Conducting Mixed Methods Research, 3rd ed, SAGE Publications, Inc, 2017.
[50] K.A. Levin, Study design III: cross-sectional studies, Evid. Based. Dent. 7 (2006) 24–25, https://doi.org/10.1038/sj.ebd.6400375.
[51] Yamane, Statistics: an introductory analysis, 2nd edition, J. Bangladesh Agricult. Univers. 22 (1967) 146–157, https://doi.org/10.3329/jbau.v22i2.74547.
[52] V. Braun, V. Clarke, Using thematic analysis in psychology, Qual. Res. Psychol. 3 (2006) 77–101, https://doi.org/10.1191/1478088706qp063oa.
[53] L.J. Cronbach, P.E. Meehl, Construct validity in psychological tests, Psychol. Bull. 52 (1955) 281–302, https://doi.org/10.1037/h0040957.