

# NOTICE: REGISTRATION OF DATA COLLECTION AND PROCESSING.



In recent years, Tanzania has grappled with significant challenges related to the handling and protection of personal data by private and public entities. These challenges have underscored the urgent need for a robust framework to regulate and oversee personal data collection, storage, and processing. This article provides an in-depth overview of the recently introduced *Notice to Register for Data Collection and Processing*, addressing critical aspects such as: **Who is required to register, The registration process, Penalties for non-compliance, and The importance of compliance.**

Prepared by



**Adv. Simon Patrick**  
**Partner at SVTL Advisory**



**Warren Mnzava**

**Disclaimer.**

*This article is for informational purposes only and does not constitute legal or professional advice.*

## WHO IS REQUIRED TO REGISTER?

Under the law, no individual or organization is authorized to collect or process personal data without being registered as a data controller or data processor. Understanding who needs to register requires a clear grasp of the nature of personal data the law seeks to protect. Any person or entity handling such data must comply with the registration requirement to ensure accountability and transparency in data management.

1. Personal data relating to the race, national or ethnic origin, religion, age, or marital status of the individual.
2. Personal data concerning the education, medical, criminal, or employment history of the individual.
3. Any identifying number, symbol, or other particular assigned to the individual.
4. The address, fingerprints, or blood type of the individual.
5. The name of the individual appearing on personal data of another person relating to that individual, or where disclosing the name itself would reveal personal data about the individual.
6. Correspondence sent to a data controller by the data subject that is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence.
7. The views or opinions of any other person about the data subject.
8. Genetic data, data related to children, data related to offenses, financial transactions of the individual, security measures, or biometric data.
9. Personal data that, if processed, reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, or data concerning health or sex life.
10. Any personal data otherwise considered under the laws of the country as presenting a major risk to the rights and interests of the data subject.

## SECTORS REQUIRING CONSIDERATION FOR REGISTRATION

Certain sectors handle sensitive personal, financial, or confidential data, making them subject to stringent regulatory requirements. These sectors include:

### 1. Education Sector

- Institutions (Schools, Colleges, Universities): Manage student records, personal identification, academic history, and, in some cases, medical information.

### 2. Legal Sector

- Law Firms and Legal Advisory Services: Process confidential client information, including legal documents, financial data, and case-sensitive materials, requiring strict confidentiality.

### 3. Healthcare Sector

- Hospitals, Clinics, and Medical Research Institutions: Handle highly sensitive health data, including medical records, genetic information, and patient history.

### 4. Financial Sector

- Banks, Insurance Companies, and Accounting Firms: Manage financial transactions, customer identification data, credit histories, and investment details, demanding strong data security measures.

### 5. Hospitality and Tourism Sector

- Hotels, Resorts, and Travel Agencies: Collect customer details such as passport information, payment details, and travel itineraries, often involving cross-border data processing.

### 6. Construction and Real Estate Sector

- Construction Companies and Property Developers: Store employee records, financial transactions, and confidential client or project-related data.

### 7. Human Resource and Recruitment Sector

- HR Firms and Employment Agencies: Handle sensitive employee data, including personal identification, salaries, employment history, and performance evaluations.

### 8. Telecommunications and IT Sector

- Internet Service Providers (ISPs), Mobile Network Operators, and IT Service Providers: Manage large volumes of customer data, including call records, browsing history, and personal communications.

Each of these sectors processes sensitive information that necessitates careful regulatory oversight, data protection policies, and compliance with national and international data security standards

## THE REGISTRATION PROCESS.

The registration process begins with the completion of Form No. 1 and payment of the prescribed registration fees. For individuals, the application must be accompanied by a valid identity document, while for legal entities, a certificate of incorporation is required. Additional documents may also be requested at the discretion of the commissioner.

The application will be processed within seven days. During this period, the commissioner will verify the submitted information. If deficiencies are identified, the commissioner will provide guidance on necessary corrections and request the applicant to resubmit the updated application for re-verification.

In cases where the application is rejected, the decision will be communicated in writing, with reasons clearly stated, within fourteen days from the date of the decision.

It is important to note that the registration certificate is valid for five years from the date of issuance, subject to renewal upon expiry.

## IMPORTANT UPDATE ON DATA PROTECTION COMPLIANCE DEADLINES

The Personal Data Protection Commission (PDPC) issued a public notice on **10th January 2025**, extending the deadline for compliance with the registration requirement from **31st December 2024 to 30th April 2025**. This extension provides organizations and data controllers additional time to meet the registration obligations under the applicable data protection regulations. Starting **1st May 2025**, the PDPC will begin enforcement measures against non-compliance. Failure to register as required will attract penalties ranging from a minimum fine of **100,000 TZS** to a maximum of **5,000,000 TZS**. Stakeholders are urged to take this opportunity to ensure full compliance and avoid potential penalties.



## CONCLUSION: WHY PRIORITIZE DATA PROTECTION IN TANZANIA.

A robust data protection system is essential for safeguarding personal and organizational information, ensuring trust, and fostering accountability in Tanzania's rapidly digitizing economy. As businesses, government agencies, and individuals increasingly rely on digital platforms, the risks of data breaches, identity theft, and unauthorized access to sensitive information grow significantly. Legally, such a framework enforces compliance with international standards, enhancing Tanzania's appeal as an investment destination. Politically, it ensures the integrity of sensitive electoral and governance data, protecting democratic processes. Socially, it safeguards citizens' rights to privacy, promoting confidence in digital services. Economically, secure data environments facilitate innovation, e-commerce, and cross-border trade, catalyzing growth in critical sectors like fintech, healthcare, and tourism. By prioritizing data protection, Tanzania can build a resilient foundation that aligns with global digital transformations while protecting its national interests.

**Your Trusted Partner in Data protection laws,** SVTL Advisory, is dedicated to securing highest standards of data protection for businesses and individuals. With years of expertise in this field, our seasoned team is dedicated to helping businesses and individuals navigate the complexities of data privacy. We offer in-depth guidance on all aspects of personal data collection, storage, and processing, ensuring full compliance with Tanzania's data protection laws. Our experienced experts assist clients through the entire process, from the Notice to Register for Data Collection and Processing to addressing the compliance procedures and understanding potential penalties for non-compliance. With a deep understanding of the evolving regulatory landscape, we provide tailored solutions that protect your data, mitigate risks, and strengthen trust and transparency.



— ADVISORY —

### Contact Us

✉ [info@svtl.co.tz](mailto:info@svtl.co.tz)

☎ +255 763 406 162

📍 Mezzanine Floor, EY Building Plot No 162/1  
Mzingaway, Oysterbay Dar es Salaam,  
Tanzania

📍 House No. 10, Atlantis Estate Mawalla  
Road, Burka Area Arusha, Tanzania