NAVIGATING DATA PROTECTION: A GUIDE FOR HR PROFESSIONALS IN TANZANIA

OUR CONTACT

NIC Life House Building, 3rd Floor,
Wing "C", 2207/29, Block "13,
Sokoine Drive/Ohio Street,
P.O. Box 31576,
Dar es Salaam.
info@secureattorneys.co.tz
+255 717 425 183

Table Contents

1. Introduction

As an employer, the organization navigates through extensive amounts of personal data belonging to its employees. In its role as a data controller, the organization is duty-bound to respect the rights of employees, commonly referred to as data subjects by data protection laws. These rights notably include the right to access personal data linked to them. Embracing a practical view, it becomes imperative for the organization not only to acknowledge but also to fulfill its responsibilities, ensuring strict compliance with data protection obligations.

This involves navigating through people management in alignment with the data protection principles. These principles dictate that personal data should be processed lawfully, fairly, and transparently. Additionally, data collection should be confined to specified, explicit, and legitimate purposes, and the processing should be adequate, relevant, and limited to what is necessary. Ensuring accuracy, limiting data retention to necessary periods, and implementing robust security measures are integral components of upholding these principles in all aspects of employee data management.

As part of compliance with data protection laws, it is mandatory for each organization to have a Data Protection Policy. Employers must ensure that all employees, consultants, and workers receive the Employee Data Protection Policy upon joining the organization. The policy should offer guidance on the principles and procedures governing the responsible management of personal data. It should foster transparency and awareness among individuals within the organization regarding how their data is collected, processed, and secured.

To fortify the data protection framework, employers should also implement additional policies, such as the Data Protection and Security Policy and the Data Retention Policy. These policies collectively establish a robust structure to govern the entire data lifecycle within the organization. Regular evaluation and updates to these policies are essential to ensure ongoing alignment with evolving data protection standards and best practices.

The Tanzania Personal Data Protection Act, 2022 ("the PDPA") and its Regulations impose obligations on employers regarding data processing throughout their business operations. The legislation holds employers accountable at all levels of business administration, carrying significant consequences for data breaches. This guide aims to elucidate key areas related to employee data management, offering insights to help you navigate these aspects effectively. This guide specifically addresses HR practitioners, providing insights into handling employee data to ensure the fulfillment of their duties while aligning with the newly enacted data protection laws in Tanzania. It's important to clarify that this guidance doesn't replace professional legal advice on data protection matters; it is intended solely for informational purposes.

2. Definitions

"Data processor" means a natural person, legal person or public body which processes personal data for and on behalf of the controller and under the data controller's instruction, except for the persons who, under the direct authority of the controller, are authorised to process the data and it includes his representative.
"Data Subject" means the subject of personal data which are processed under this Act;

"Data Controller" means a natural person, legal person or public body which alone or jointly with others determines the purpose and means of processing of personal data; and where the purpose and means of processing are determined by law, "data controller" is the natural person, legal person or public body designated as such by that law and it includes his representative.
"Personal Data" means data about an identifiable person that is recorded in any form, including:-

(a) personal data relating to the race, national or ethnic origin, religion, age or marital status of the individual;
(b) personal data relating to the education, the medical, criminal or employment history;
(c) any identifying number, symbol or other particular assigned to the individual;
(d) the address, fingerprints or blood type of the individual;
(e) the name of the individual appearing on personal data of another person relating to the individual or where the disclosure of the name itself would reveal personal data about the individual;
(f) 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, and the views or opinions of any other person about the data subject;

"Sensitive Personal Data" includes:-
(a) genetic data, data related to children, data related to offences, financial transactions of the individual, security measure or biometric data;
(b) if they are processed for what they reveal, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliation, trade-union membership, gender and data concerning health or sex life; and
(c) 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;

"Commission" means the Personal Data Protection Commission established under section 6.
"Processing" means analysis of personal data, whether or not by automated means, such as obtaining, recording or holding the data or carrying out any analysis on personal data, including:
(a) organization, adaptation or alteration of the personal data;
(b) retrieval or use of the data; or
(c) alignment, combination, blocking, erasure or destruction of the data.

3. Operational Procedures

As HR Managers and HR Officers, there are key responsibilities to ensure compliance with data protection requirements. Here's a checklist of day-to-day activities to be followed:

- Ensure everyone working for or on behalf of the organization understands their responsibility for appropriate data collection, storage, and handling, aligning with policies and procedures.
- Grant access to personal data only to employees who need it for their work and are authorized. Personal data should be used only for the lawful purpose for which it was obtained.
- Employees should secure personal data, avoiding unauthorized sharing, and informal disclosure.
- Regularly review and update personal data in your access, and ensure your teams are informed of any changes, especially in contact details.
- Discourage making unnecessary copies of personal data, and ensure secure storage and disposal of any copies.
- Encourage the use of strong passwords and advise team members to lock their computer screens when away from their desks.
- Personal data transferred electronically to authorized external contacts should be encrypted.
- Consider anonymizing data or using separate keys/codes to prevent the identification of the data subject during transfers.
- Employees should not save personal data on personal computers or other devices.
- Personal data should not be transferred outside Tanzania unless in compliance with the PDPA and its regulations.
- Ensure that drawers and filing cabinets containing personal data are locked, and no paper with personal data is left unattended.
- Employees should not take personal data off the organization's premises without proper authorization.

- Personal data must be shredded and disposed of securely.
- Personal data in email inboxes should be stored in the relevant file folder and deleted from the inbox promptly.
- Employees should keep personal data secure and not share it with unauthorised people or informally.

4. Subject Access Requests (SARs)

In alignment with the PDPA and its regulations as applicable in Tanzania, the following guidelines detail the process for handling subject access requests:
Every person affiliated with the organization, including workers, consultants, and job applicants, shares responsibility for appropriate data collection, storage, and handling, adhering to data protection policies and procedures.

In the absence of specific guidelines on the timeframe for responding to SARs in the PDPA and its regulations, a recommended approach can be adopted from the General Data Protection Regulation (GDPR). According to GDPR, organizations should promptly address Subject Access Requests from employees, maintaining a standard response time of one month. In cases of complex requests, this period can be extended to three months. The organization commits to communicating any delays within the initial month of receiving the SAR.

In the case of manifestly unfounded or excessive requests, the organization may charge a fee based on the administrative cost of responding. However, such circumstances are expected to be rare.

1. Responding to a Subject Access Request

(a) Identification of Request
Subject access requests should follow the internal procedure of each organization. Any submission through alternative routes, such as email or direct contact, should still be acknowledged and responded to.

(b) Verification of Identity
While employees' ongoing relationships may not require proof of identification, job applicants may need to provide proof, such as a national identity card or passport or other IDs, to verify their identity.

(c) Assessment of Complexity
Assess whether the request is complex, especially when dealing with a large amount of data. If using the extended 3-month limit, notify the employee within the first month, stating the reasons for the extension.

(d) Communication and Collaboration
Keep the employee informed about potential delays, reducing the risk of complaints. For broad requests, engage with the employee to discuss and clarify the scope, seeking additional information if necessary.

(e) Processing the Request
- Organize and file employee data according to data protection policies. Include various records, from application forms to disciplinary records, ensuring compliance with the law.
- Acknowledge third parties that may process data on behalf of the organization. Consider their data in the response to subject access requests.
- Before responding, review personal data to ensure compliance with data protection principles. The right to obtain a copy should not adversely affect the rights and freedoms of others.

(f) Providing the Data
- Respond electronically, unless another format is requested. Utilize a secure system to provide data. Password protect electronic data for security.
- Explain the conducted searches, reasons for withholding documents (if applicable), and provide an account of redactions made. Transparency minimizes the risk of complaints.

(g) Record Maintenance
Maintain records of steps taken to comply with subject access requests. Include response timeframes, notifications of delays, data restrictions, and reasons. These records align with the accountability principle.

5. What to do if there is a Security Breach

1. Data Breach Management under Tanzanian PDPA

The PDPA emphasizes the obligation to notify the Commission without 'undue delay', a term not explicitly defined in the law. Drawing inspiration from GDPR, it suggests a similar timeframe for notification, within 72 hours of becoming aware of the breach, where feasible.

(a) Internal Reporting
If a data breach is discovered or suspected, the responsible person should be contacted promptly, providing:

- The time and date of the breach.
- The time and date the breach was discovered.
- The type(s) of data involved.
- The category(s) of data subjects affected.
- Information on whether sensitive personal data is involved.
- Estimated number of affected data subjects.
- If relevant, names of customers likely to be affected.

(b) Initial Management and Recording
Upon notification, an initial assessment of the data breach should be done, including:

- Estimating the severity of the data breach.
- Containing and recovering the affected data as practicable.
- Identifying who needs to be notified initially.
- Recording the breach and initial steps in the Data Breach Register.

(c) Investigation and Assessment
An investigation, starting within 24 hours of discovering the breach, considers:

- Types and sensitivity of data involved.
- Organizational and technical measures in place.
- Potential effects on data subjects and the organization.
- Number of affected data subjects and potential consequences.

(d) Notification

Notification shall be required to:
- The Commission.

Notification may be required to:
- Affected data subjects.
- The police.
- The Company's insurers.
- Affected commercial partners and clients.

(e) Notifying the Commission
- Notify within 72 hours of becoming aware.
- Include categories and approximate numbers of affected data subjects.
    - Specify the contact person within the organization.
    - Describe the likely consequences of the breach.
    - Detail measures taken to address the breach.

(f) Notifying Individual Data Subjects
- Notify without undue delay.
- Provide a user-friendly description of the breach.
- Offer clear advice on protective steps.
- Describe measures taken to address the breach.
- Provide contact details for further information.

(g) Evaluation and Response

- Conduct a comprehensive review of the causes of the breach.
- Assess the effectiveness of response measures.
- Consider changes to systems, policies, or procedures to prevent future breaches.
- Evaluate data storage, security measures, transmission methods, data sharing practices, and staff awareness.

(h) Record Keeping

- Maintain records of all data breaches, irrespective of notification.
- Document the decision-making process surrounding notification in the Company's Data Breach Register.

THANK YOU