ESWATINI COMMUNICATIONS COMMISSION

ESCCOM

EDPA NOTICE NO. 3/2024

Enforcement Notice in Terms of Section 41 of the Eswatini Data Protection Act 2022 – MTN Eswatini

June 2024

Sibekelo Building,
Fourt Floor, North Wing
P.O Box 7811, Mbabane

dataprotection@esccom.org.sz
www.edpa.org.sz

+268 2406 7000

ESWATINI DATA PROTECTION AUTHORITY

ENFORCEMENT NOTICE ON MTN ESWATINI IN TERMS OF SECTION 41 OF THE DATA PROTECTION ACT 2022.

1. INTRODUCTION

1.1. The Data Protection Act, 2022 (hereinafter referred to as the ACT) was passed to provide for the processing and protection of personal information. Section 5 of the Act designates the Eswatini Communications Commission as the Eswatini Data Protection Authority (hereinafter referred to as the EDPA), charged with the responsibility to administer the Act and enforce compliance thereto.

2. DISCLOSURE OF PERSONAL INFORMATION TO A THIRD PARTY BY MTN ESWATINI

2.1. PARTICULARS OF INCIDENT

2.1.1. On 27th February 2024, MTN Eswatini **(the Organisation),** reported a personal data breach to the Eswatini Data Protection Authority as required by Section 17(1)(a) of the Act.

2.1.2. The Organisation submitted that on 5th February 2024, a customer named **(X)** filed a complaint through the Call Centre, which is outsourced by the Organisation and managed by NDZ Corporate, stating that her Mobile Money Statement had been shared with a third party without her consent.

2.1.3. The customer, who is a dressmaker in Manzini, informed the Call Centre Manager that she was summoned to appear at the Manzini Police Station in January 2024 regarding a case about her failure to repay a debt reported by one **(Y).** At the Police Station, the customer learned that the third party **(Y)** had in his possession her 6-month Mobile Money statement from MTN to support his case, claiming that she had available funds to settle her debt.

2.1.4. In response to the complaint, the Organisation conducted an internal investigation and noted the following:

2.1.4.1. On 5th December 2023, the third party **(Y)** requested the Call Centre Agent to share the customer's 6-month statement via the Organisation's WhatsApp line.

2.1.4.2. The customer's 6-month statement was shared with the third party **(Y)** after they were advised on the correct process to follow when requesting his/her information, which includes, among other things, an identity card.

2.1.4.3. The Call Centre Agent was engaged about the incident; however, upon engagement by her employer, namely NDZ, the Call Centre Agent resigned before the commencement of disciplinary proceedings.

2.1.5. After the investigation, the Call Centre Manager provided feedback to the customer about how the information ended up in the hands of the third party. During the feedback session, the customer was also informed about MTN's procedures for sharing information, especially with third parties. MTN then expressed regret and apologised for how the information was shared with the third party.

2.1.6. On the 8th of March 2024, the EDPA requested further details from the Organisation to analyse the impact and extent of the personal data compromise.

2.1.7. On 21st March 2024, the Organisation provided the requested details to the EDPA. The Organisation's submission revealed the following:

2.1.7.1. The relationship between The Organisation and NDZ Corporate is guided by a contract, policies, processes, and procedures of the Organisation. The contract clearly outlines each party's roles and responsibilities and includes confidentiality provisions.

2.1.7.2. The Organisation submitted that there are present mechanisms in place to report all observed and suspected information security incidents as soon as employees become aware of an incident, including an anonymous tip-off and whistle-blowing policy.

2.1.7.3. The Organisation submitted that NDZ staff received training on whistleblowing, ethics, and compliance and that policies and processes for engaging with customers and sharing information are regularly communicated to the relevant staff members and NDZ employees.

2.1.7.4. The Organisation submitted that it conducts Data Protection and Privacy Training for all employees, including NDZ employees, at least once a year. Additionally, mandatory huddles are held for Call Centre Agents every Monday and Thursday for 20 minutes, followed by a test to confirm their understanding. The Organisation submitted that these sessions cover the information that agents should collect before sharing any information.

2.1.7.5. The Organisation submitted that they perform root cause analysis to address issues or non-conformances and pinpoint the underlying cause of the problem. Additionally, the Organisation submitted that they have a Quality Assurance (QA) function that oversees agents and customer interactions to guarantee high standards which involves reviewing calls, emails, chats, and other interactions between agents and customers.

2.1.7.6. Furthermore, the Organisation submitted that NDZ staff members sign a Non-Disclosure Agreement upon onboarding.

2.1.7.7. The Organisation submitted that MTN Policies regulate the sharing of customer information, including the Provision of Communication Related Information Policy. They submitted that this policy applies not only to internal staff, but also to third party service providers, such as NDZ staff members.

2.1.7.8. In addition, the Organisation submitted that the Call Centre/NDZ staff have specific procedures for sharing MoMo statements with customers, which require the submission of certain requirements.

3. THE EDPA'S CONSIDERATIONS

3.1. The Organisation has shown that it has implemented measures and mechanisms to ensure the safety and security of customers' personal data. MoMo statements are considered customer information and must be shared according to the same process outlined in the policy for disclosure. However, in this case, the Organisation failed to uphold the confidentiality and integrity data protection principle despite having these measures and mechanisms in place. This failure occurred due to the following reasons:

3.1.1. Provision of Communication-Related Information Policy

3.1.1.1. The Organisation has not reviewed the Communication Related Information Policy since 2021. As a result, the policy does not include procedures and processes on how the Call Centre Agents should resolve requests from a third-party requesting information about another subscriber.

3.1.2. Data protection compliance: foundations – data privacy 101

3.1.2.1. The Organisation has not provided adequate evidence of the training received by Call Centre Agents, including attendance records. Moreover, the Organisation submitted that they offer training only once a year, despite dealing with a substantial amount of personal data.

3.1.3. Contract of employment

3.1.3.1. The Organisation is aware of the high turnover in the call centre, which is attributed to the yearly contracts given to Call Centre Agents. However, the Organisation has not implemented role-based access to sensitive information. The submission indicates that the Call Centre Agent has unrestricted access to all customer information, which is not reviewed

before being shared with clients.

3.1.4. Call centre transcript

3.1.4.1. The call centre Agent failed to take precautions against a foreseeable risk of harm and was aware that they were sharing the statement with a third party.

3.1.4.2. Based on the review of the call centre transcript, the Call Centre Agent did not follow any script to communicate with the third party who was requesting information.

3.1.4.3. The Call Centre Agent did not have any verification mechanisms and procedures to ensure the information was shared with authorised personnel.

3.1.4.4. The Organisation failed to ensure that personal data shared via WhatsApp was password protected to ensure that it was only accessed by authorised individuals.

3.1.4.5. The absence of sufficient managerial oversight in the compilation and distribution of the message indicates a lack of appropriate safeguards and the ineffective implementation of measures to secure the personal information of data subjects.

3.1.5. Training awareness programme

3.1.5.1. The Organisation's awareness program is ineffective, and there is a lack of evidence to support its effectiveness. For instance, an attendance register should have been provided to confirm training participation. As a result, the Authority cannot verify if Call Centre Agents are adequately trained in data protection.

3.1.6. Quality assurance function

3.1.6.1. The Organisation's quality assurance function failed to review the interactions between the Call Centre Agent and the requester, resulting in the issue not being identified until a complaint was received from the client.

4. THE ORGANISATION'S OBLIGATIONS UNDER THE ACT

4.1. The Organisation is a "Data Controller" as envisaged by the Act with an obligation under Section 14(1) to *"…secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and administrative measures to prevent –*

4.1.1. *loss of, modification and damage to or unauthorized destruction of personal information; and*

4.1.2. *unlawful access to or processing of personal information."*

4.2 The Organisation processes both personal and sensitive personal information at a significant scale and therefore incurs a greater obligation to ensure that it has in place all corresponding technical and organisational measures to protect the personal data in its control.

4.3 Section 14(2) enjoins the Data Controller to take "reasonable measures to –

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards."

4.4 The Organisation is obligated under Section 17 to notify the EDPA and the data subjects of the data compromise.

5. THE EDPA'S FINDINGS

5.1. The EDPA has considered the matter in its totality and has determined that the incident constitutes a data breach notifiable under Section 17 of the Act.

5.2. The EDPA has determined that MTN has breached the provisions of the Act in that:

5.2.1. It has failed and/or neglected to "…*secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and administrative measures to prevent unlawful access to or processing of personal information*" in terms of Section 14(1)(b) of the Act.

5.2.2. It has failed in terms of Section 14(2) of the Act, to "*take reasonable measures to –*

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards."

6. EDPA'S DECISION

6.1. The EDPA, in the exercise of its powers under Section 41(1) of the Act, hereby **imposes a warning** to MTN.

6.2. The Enforcement Notice shall be valid for a period of one (1) year from the date of issue subject to MTN not committing the same or similar breach within the Enforcement Notice period.

6.3. In light of the foregoing and in terms of Section 41(a), the EDPA directs MTN to do the following:

6.3.1. Conduct a data protection impact assessment (DPIA) for the call centre to ensure that appropriate measures and standards exist to comply with the conditions for the lawful processing of information.

6.3.2. To implement procedures and controls for the transfer of information, including procedures for protecting sensitive information shared in attachments:

6.3.2.1. Ensure that personal data shared via WhatsApp is password protected.

6.3.3. Document processes, policies and customer service processes which are well-defined and easily accessible. This includes documenting call centre scripts to ensure that they provide the customers with accurate information, therefore leaving no room for ambiguity.

6.3.4. Train the Call Centre Agents regularly on data protection principles and attendance registers kept as evidence.

6.3.5. Introduce Call Centre Agent onboarding and training program on their roles and responsibilities.

6.3.6. Update the communication policy to include procedures on how Call Centre Agents can resolve issues concerning requests from a third party.

6.3.7. Ensure that Call Centre Agents on short-term contracts have limited access to client information.

6.3.8. Implement role-based access for sensitive information, as the call centre currently has unrestricted access to all customer information without prior review before sharing it with clients.

6.3.9. Segregation of duties should be implemented when sharing information externally, including having a supervisor review the information before it is shared with the requester.

6.3.10. The quality assurance team should maintain access logs and conduct regular audits to monitor and track user activities. This will enable the Organisation to identify unauthorized access attempts and unauthorized sharing of information.

6.3.11. The quality assurance function should also audit all communication between agents and requestors, including communication on WhatsApp.

6.4 MTN shall within three (3) months of receipt of notice, submit a comprehensive report to the EDPA of the progress in the implementation of the measures listed in paragraph 6.3 above.

7. RIGHT TO APPEAL

7.1. MTN has the right to appeal this decision.

Date of decision……2024

_____

Mvilawemphi Dlamini

Chief Executive