ESWATINI COMMUNICATIONS COMMISSION

EDPA-NOTICE 4/2024

EDPA Enforcement Notice in Terms of Section 41 of the Eswatini Data Protection Act 2022 – Liberty Life Swaziland Limited

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 LIBERTY LIFE SWAZILAND LIMITED 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 BY LIBERTY LIFE SWAZILAND LIMITED DUE TO MISDIRECTED EMAIL

2.1. PARTICULARS OF INCIDENT

2.1.1. On the 7th of November 2023, Liberty Life Swaziland Limited (the "**Organisation**"), a specialist life insurance company that provides group, individual, and personal risk insurance solutions for life changing events, notified the Eswatini Data Protection Authority (the "**EDPA**") of a personal data compromise (the "**Incident**"), discharging an obligation placed by Section 17(1)(a) of the Act.

2.1.2. The Organisation notified the Authority that on the 3rd November 2023, an employee of the Organisation erroneously included as a recipient, an external person in an email intended for internal staff members. The said email contained names, surnames, and identity numbers of 4174 (four thousand one hundred and seventy-four) of data subjects.

2.1.3. On becoming aware of this error, the Organisation informed their client **"X"** whose members' personal data was compromised and assured them that the

incident will not be repeated as the Organisation's IT processes are equipped to detect and prevent such incidents.

2.1.4. Furthermore, the Organisation engaged the unintended recipient to delete the email she was erroneously copied in.

2.1.5. On the 16th of November 2023, the EDPA requested further particulars from the Organisation to analyse the impact and extent of the data compromise.

2.1.6. On the 27th of November 2023, the Organisation furnished the EDPA with the requested particulars. The Organisation's submission disclosed that Liberty Life Swaziland Limited does not have an in-house IT department and piggybacks on the Standard Bank Eswatini platform, entailing that all their IT processes are run and managed by Standard Bank's IT department as part of their Group IT arrangements.

2.1.7. The Organisation submitted that there are present mechanisms in place to report all observed and suspected information security incidents to the Organisation's Data Protection Officer and/or Line Manager as soon as employees become aware of an incident.

2.1.8. The Organisation's submission further revealed that all external emails have a disclaimer and confidentiality link at the foot of the email, guiding that unintended recipients should delete an email received from the Organisation immediately, and the sender thereof notified.

2.1.9. Furthermore, the Organisation's submission demonstrated that all employees sign an attestation annually that has clear provisions on emailing confidential data.

2.1.10. The Organisation submitted that there are API controls implemented by the Organisation which scan all emails directed to external domains for Personal Identifiable Information (PII) (National ID numbers, passport, and travel document numbers, payment card details, bank account numbers) and other

sensitive information. The emails are blocked from exit unless they are sent by a person in a whitelist (a group of individuals whose day-to-day function involves sending correspondences with clients). The alerts are blocked and sent to the line manager, IT security management personnel and Standard Bank Risk Management.

2.1.11. The Organisation submitted that the email detection system worked as expected and blocked the email and the alerts were sent to the personnel mentioned herein above in paragraph 2.1.10.

2.1.12. Furthermore, the Organisation submitted that the employee who sent the email, on realisation of the mistake, tried to report to the IT Security Managers via Teams Calls who did not answer the call. The IT Security Manager later returned the call, and the employee who sent the email missed the call. Seeing the employee had not picked up, the IT Security Manager assumed that the sender required for the email to be released urgently and released the email which resulted in the email being sent to the unintended recipient.

3. THE EDPA'S CONSIDERATION

3.1. The Organisation has demonstrated that it has measures and mechanisms in place to ensure that the personal data of customers is safe and secure including:

3.1.1. The Organisation's submission further revealed that all external emails have a disclaimer and confidentiality link at the foot of the email, guiding that unintended recipients should delete an email received from the Organisation immediately, and the sender thereof notified.

3.1.2. There are API controls implemented by the Organisation which scan all emails directed to external domains for Personal Identifiable Information (PII) (National ID numbers, passport, and travel document numbers, payment card details, bank account numbers) and other sensitive information. The emails are blocked from exit unless they are sent by a person in a whitelist (a group of individuals whose day-to-day function involves sending correspondences with clients). The alerts

are blocked and sent to the line manager, IT security management personnel and Standard Bank Risk Management.

3.1.3. The Organisation's submission demonstrated that all employees sign an attestation annually that has clear provisions on emailing confidential data.

3.2 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:

3.2.1 The Sender failed to take precautions against a foreseeable of harm and did not take all measures to ensure that all the recipients were intended.

3.2.2 The Sender failed to take all necessary precautions to ensure that the message is not released to the unintended recipient as they called only called one of the IT security Managers when the incident happened when the control can be approved by 2 other Managers as described in paragraph 2.1.10 herein above.

3.2.3 The IT Security Manager was negligent by releasing the blocked email without ensuring that it is addressed to the authorised personnel.

3.2.4 Deficiency in the process of releasing external emails where IT Security Manager assumed the call was to release the email without ascertaining the veracity thereof.

3.2.5 The Organisation failed to ensure that personal data shared via email was encrypted to ensure that it is only accessed by authorised individuals.

3.2.6 The unlawful disclosure affected a large number of data subjects and thus the likelihood of harm to the claimants occasioned by the compromise is considered significant by the EDPA.

3.2.7 However, the EDPA has considered that the data was exposed to one (1) external unintended recipient only and not broadcast widely.

3.2.8 The Organisation is obligated under Section 17 to notify the EDPA and the data subjects of the data compromise. From the Organisation's submission, it is clear that the notification was only sent to the data processor "**X**" and not to the data subjects whose data was compromised.

3.2.9 In addition, the Organisation did not disclose the complete details of the security compromise in its first notification to the Authority. The Organisation indicated that the only information that was unlawfully disclosed included names, surnames, and identity numbers of data subjects whilst the email contained more categories of personal and sensitive information. The disclosed email contained the following personal information:

Document	**Number of Data Subjects affected**	**Categories of personal data disclosed**
a) **Y** Umbrella Funeral Scheme – member date joined.	4147	Personal data • DataID • Identity Number • First Name • Surname • Date of birth Sensitive data • Gender
b) **Y** Umbrella Funeral Scheme –List 2023	191	Personal data • Church Name • Inception date • Membership at last date

c) **Y** Umbrella Funeral Scheme – claim list	406	Personal data • Policy Number • ID number • Broker • Member Name • Member Date of Birth • Deceased Name • Deceased Date Of birth • Deceased Date of Death • Deceased relationship • Marital Status • Benefit amount Sensitive personal data • Religion • Children Data

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 sharing of information amounts to processing in terms Act.

5.2. The EDPA has considered the matter in its totality and has determined that Liberty Life Swaziland Limited has breached the provisions of the Data Protection Act, 2022.

5.3. The EDPA has determined that Liberty has breached the provisions of the Act in that:

5.3.1. 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.

5.3.2. 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. THE EDPA'S DECISION

6.1. The EDPA, in the exercise of its powers under Section 41(1)(a) of the Act, hereby **imposes a warning** to Liberty Life Swaziland Limited for failure to ensure that all technical and organisational measures put in place to protect personal data are adhered to strictly.

6.2. The Enforcement Notice shall be valid for a period of one (1) year from the date of issue subject to Liberty 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 Liberty to do the following:

6.3.1. Implement procedures and controls on the transfer of information, which includes procedures for protecting communicated sensitive information that is in an attachment:

6.3.1.1. To ensure the encryption of personal data that is shared via emails.

6.3.1.2. Decryption password to the encrypted documents should be shared through different media which can include telephone, call, or SMS.

6.3.2. Ensure that the Organisation's disclaimer and confidentiality note information is presented on the email in summary.

6.3.3. Train all employees regularly on data protection principles and attendance registers kept as evidence.

6.3.4. Implement technical measures that will alert a sender if an email is being sent to an external email.

6.3.5. Document (inbound and outbound) communication processes, and policies that are well-defined and easily accessible. This includes documenting blocked email verification mechanisms to ensure that the managers described in paragraph 2.1.10 above know procedures to follow when reviewing blocked emails, therefore leaving no room for ambiguity.

6.4 Liberty Life Swaziland Limited shall within three (3) months of receipt of notice, submit a comprehensive report to the EDPA of progress in implementing the measures listed in paragraph 6.3 above.

7. RIGHT TO APPEAL

7.1. Liberty Life Swaziland Limited has the right to appeal this decision.

Date of decision……2024

_____

Mvilawemphi Dlamini

Chief Executive