PERSONAL DATA PROTECTION OFFICE

(PDPO)

Abridged Investigation Report of the Data Security Breach at Uganda Securities Exchange (USE)

June 2023

1. INTRODUCTION

1.1 The Personal Data Protection Office

The Personal Data Protection Office is Uganda's data protection and privacy regulator. It is established as an independent office under the National Information Technology Authority, Uganda (NITA-U) and is responsible for overseeing the implementation of and enforcement of the Data Protection and Privacy Act, 2019.

The Personal Data Protection Office's statutory functions include the following;

- Oversee the implementation of and be responsible for the enforcement of the Data Protection and Privacy Act and supporting Regulations;
- Coordinate, supervise and monitor data collectors, data processors, data controllers and data subjects on all matters relating to the Data Protection and Privacy Act, 2019;
- Set, monitor and regulate standards for personal data protection and privacy;
- Establish and maintain a data protection and privacy register;
- Monitor, investigate and report on the observance of the right to privacy and of personal data;
- Receive and investigate complaints relating to infringement of rights of the rights of the data subject under the Data Protection and Privacy Act, 2019;
- Provide guidance to data collectors, data processors, data controllers and data subjects about their data protection and privacy rights, obligations and responsibilities under the Data Protection and Privacy Act, 2019;
- Conduct audits to ensure compliance with the Data Protection and Privacy Act 2019.

1.2 About Uganda Securities Exchange

The Uganda Securities Exchange (USE) is registered with the Personal Data Protection Office as Uganda Securities Exchange Nominees Limited under registration number PDPO-202205-0325.

The Uganda Securities Exchange (USE) was established in 1997 as a company limited by guarantee, and was licensed in 1998 by the Capital Markets Authority to operate as an approved securities exchange. The Exchange is governed by a Board of Directors whose membership includes licensed broker/dealer firms, investment advisors, a representative of investors and a representative of issuers.

1.3 Background to the breach

The Personal Data Protection Office became aware of a letter from the Uganda Securities Exchange (USE) that was addressed to the general public regarding unauthorised access to their technology third-party logging severs. This server receives data from USE's Easy Portal which compromised the privacy of the personal data under USE's custody.

The Office also received notification of the breach through a complaint dated 18th June 2022 from Unwanted Witness, a Civil Society Organisation notifying it of an alleged data breach at Uganda Securities Exchange as reported through a tweet by an individual, in a publication by a security platform and the Daily Monitor publication dated 16th June 2022 https://www.monitor.co.ug/uganda/business/finance/data-breach-puts-hundreds-of-use-investor-details-at-risk-3850096 . The Office also received a complaint from an individual over the same data security breach and requested the Office to carry out an investigation.

2. REVIEW SCOPE AND OBJECTIVES

Purpose and scope of the investigation

The Personal Data Protection Office (PDPO/Office) as the data protection and privacy regulator is required by law to investigate reported data security breaches and complaints against a data collector, data processor or data controller to remedy any breach or take such action as may be required. The Office considered the information received through the aforementioned complainants, the USE internal investigation report and other relevant documents submitted to the Office and sought to assess how the Uganda Securities Exchange applied its ICT policies to safeguard the privacy of personal information in its custody.

3. INVESTIGATION FINDINGS

From the investigations carried out, the Office had two major issues of concern upon which the findings and recommendations were drawn. The issues are;

1) Issue one: Whether the Uganda Securities Exchange (USE/the Exchange) suffered a data security breach?
2) Issue two: Whether the data security breach was occasioned by an action or inaction of the Uganda Securities Exchange and/or its technology partner, Soft Edge Uganda Limited?

3.1 Summary of the findings

3.1.1 Issue one: Whether the Uganda Securities Exchange (USE/the Exchange) suffered a data security breach?

The investigation by the Personal Data Protection Office confirmed that Uganda Securities Exchange had experienced a personal data security breach. After reviewing the documents shared and interviewing representatives from USE and Soft Edge Uganda Limited, it was determined that the breach occurred on the infrastructure of Soft Edge Limited due to an incorrectly configured firewall on the audit logging server created to track all actions during an upgrade of USE's Know Your Customer (KYC) system. This created an open port, from which personal data was exposed for a period of about twelve (12) days.

This information was accessed by persons who were ordinarily not authorised to access the personal data. The accessed information included National Identification Numbers (NINs), names, dates of birth, email addresses, physical addresses, and telephone numbers of individuals that present information from which an individual can be identified. Therefore, the investigation confirmed that USE suffered a data security breach. It was established that the information that was accessed by an authorised person included personal data of USE's data subjects that Soft Edge Uganda Limited had accessed on account of its contractual relationship with USE as a technology partner.

3.1.2 Issue two: Whether the data security breach was occasioned by an action or inaction of the Uganda Securities Exchange and/or its technology partner, Soft Edge Uganda Limited?

a) Policies and procedures on change management

Soft Edge and USE failed to adhere to the change management provisions in the USE Information Systems Policies Manual. It was established in an interview with a representative from Soft Edge that the company lacked its own policies and was bound to follow USE's as stated in the Agreement executed by him on behalf of Soft Edge. This was however not carried out as was established by the PDPO investigation. Soft Edge did not inform USE's help desk or IT Management about changes made, nor did it follow the approved change management procedures outlined in the USE manual. USE on the other hand failed to fulfil its duty as a data collector by not ensuring that Soft Edge complied with its policies to protect individuals' personal data.

A representative from Soft Edge during his interview acknowledged that the compromised audit logging server at Soft Edge interacted with the Easy Portal platform which was hosted by USE hence, the change in

the firewall impacted the USE IT environment and should have been reported to USE as per the guidelines. As a result, both USE and Soft Edge failed to safeguard the personal data they held.

b) Incident response/management

Clause 1.6 of the USE Information Systems Policies Manual version 2.1, which was approved in 2020, conflicts with the Data Protection and Privacy Act 2019, as it grants the USE Chief Executive Officer the sole discretion to decide whether to report a data security breach, contrary to Section 23 of the Act. Additionally, USE's failure to detect the Twitter message from an unnamed individual in this report, about the exposure of personal data was negligent and contributed to the continued exposure for twelve (12) days. Despite being informed of the data security breach, USE and Soft Edge Uganda Limited failed to promptly respond, violating their obligations as data collectors, data controllers, and data processors under Section 20 of the Data Protection and Privacy Act to maintain the security of personal data and Clause 2.6.1 of the Manual which is to the effect that information on a breach may be received through notification from an end user.

3.1.3 Compliance with the Data Protection and Privacy Act and associated Regulations

The PDPO investigation team sought to verify the compliance of USE and Soft Edge with other aspects of the Data Protection and Privacy Act and its associated regulations. A summary of the findings is provided below.

a) Registration with the Personal Data Protection Office (PDPO)

Section 29 (2) of the Data Protection and Privacy Act and Regulation 15 (1) of the Data Protection and Privacy Regulations read together enjoin the data collectors, data controllers and data processors to register with the Personal Data Protection Office. Soft Edge Uganda Limited therefore as a data processor of USE in relation to this matter is obligated to register with the Office. The investigation, however revealed that this was not done either before or even after the breach when the company's representative was made aware of this requirement. It follows therefore that Soft Edge has contravened the provisions of the law regarding this requirement.

b) Data Sharing Agreement

Section 21 (2) of the Data Protection and Privacy Act mandates that a contract between a data controller and a data processor regarding the processing of personal data must require the data processor to establish and maintain confidentiality and security measures to protect the personal data's integrity.

The Agreement between USE and Soft Edge was inadequate in securing the integrity and confidentiality of personal data. It lacked clear definitions of the categories of personal data to be shared, and the respective obligations of the data controller and data processor in ensuring the security and preservation of privacy of the collected, stored and processed personal data. Despite the Agreement being in place prior to the enactment of the Data Protection and Privacy Act, the Act and its subsequent regulations in effect after their passing imposed a responsibility on data collectors, controllers, and processors to align their data processing activities, including agreements, with the standards set by the Act and regulations.

During PDPO's webinars titled "Compliance Beyond Registration" on 31st March, 2022, and "How to Prepare an Annual Privacy Compliance Report" on 8th September, 2022, it was emphasized that registered data controllers and processors (including Uganda Securities Exchange) must review and update their agreements/contracts with clauses related to personal data collection, sharing, and processing. This was to ensure that they align with the Data Protection and Privacy Act, and a compliance assessment tool was provided as further guidance to ensure that their processing operations and documentation comply with the law. Both webinars were uploaded to PDPO's YouTube channel.

4. NEXT STEPS

As determined by the PDPO investigation, the data security breach was caused by a combination of human error (actions, inactions and omissions) and non-compliance with the Data Protection and Privacy Act, its supporting regulations, and the USE Information Systems Policies Manual. The Office therefore will take the following steps to enforce the Act and its attendant Regulations:

a) Prosecution of USE, Soft Edge Uganda Limited, and their accountable representative for the data security breach

Both USE and Soft Edge were negligent in the handling of personal data, incident management and change management which made the personal data in their possession susceptible to the exposure caused by the data security breach. The companies failed to notice the continuous exposure of the personal data for twelve (12) days until it was publicised. This was a contravention of Sections 20 and 21 of the Data Protection and Privacy Act.

Section 35 of the Data Protection and Privacy Act creates an offence of unlawful disclosing of personal data to another person of such data held or processed by a data collector, data controller or data processor. Section 38 further states that when an offence including unlawful disclosing is committed by a corporation, the corporation and every officer of the corporation who knowingly and willfully authorised or permitted the contravention commits the offence. Therefore, in the circumstances, USE, Soft Edge and their accountable representative for the data security breach should be prosecuted for their negligence in the handling of the personal data of USE clients.

b) PDPO has given USE and Soft Edge Uganda Limited a three-month timeframe to rectify all non - compliant areas outlined in this Report to bring them in adherence to the Data Protection and Privacy Act and related Regulations.

Stella Alibateese

National Personal Data Protection Director

PERSONAL DATA PROTECTION OFFICE