Personal DATA Protection OFFICE

REGULATION 45 (2)

FORM 12

THE REPUBLIC OF UGANDA

IN THE PERSONAL DATA PROTECTION OFFICE

COMPLAINT NO. PDPO 061/2024

SIMBWA PHILLIP.....COMPLAINANT

AGAINST

CHIPPER TECHNOLOGIES UGANDA LIMITED.....RESPONDENT

TO: PHILLIP SIMBWA

CHIPPER TECHNOLOGIES UGANDA LIMITED

Having reviewed your complaint lodged with the Personal Data Protection Office (hereinafter referred to as the "PDPO") on 27th November 2024 alleging that Chipper Technologies Uganda Limited (hereinafter referred to as the "Respondent") denied your request for deletion of personal data and infringed upon your rights under the Data Protection and Privacy Act, Cap. 97 (hereinafter referred to as the "Act, Cap. 97"), the decision of the PDPO is as follows:

1. BACKGROUND FACTS

On 27th November 2024, PDPO received a complaint from the Complainant. The complaint alleged that the Respondent had denied the Complainant's request for deletion of his Personally Identifiable Information (PII) and Know Your Customer (KYC) data, contrary to the provisions of the Act, Cap. 97.

Earlier, on 25th November 2024, the Complainant had written to the Respondent, requesting the deletion of his PII and KYC data. In a response dated 26th November 2024, the Respondent required the Complainant to cash out all funds in his account prior to the deletion and committed to addressing the request within 12-24 working hours.

Dissatisfied with the Respondent's response, the Complainant lodged a formal complaint with PDPO. On 27th November 2024, PDPO engaged the Respondent and was informed that the request had been fulfilled in compliance with the Data Protection and Privacy Act, Cap. 97 and the Anti-Money Laundering Act, Cap. 118.

The Complainant, however, contended that the Respondent failed to meet all his conditions for data deletion and raised additional issues, including:

(i) The Respondent's failure to acknowledge that it lacks the Complainant's explicit consent to process, share, or use his data beyond retention during the 10-year period.
(ii) Notifying the Complainant of any data breaches that may impact his data even when he is no longer active on the platform during the next 10 years when the Respondent is required to retain the data as stipulated by Section 8(3) of the Anti-Money Laundering Act, Cap. 118.
(iii) Notifying the Complainant whenever their platform undergoes an update that may result in the exposure of his data to a third party.
(iv) Providing the Complainant with a copy of all data collected about him.

ISSUES FOR DETERMINATION

The issues for determination are as follows:

1. Whether there was an infringement of the Complainant's rights under the Act, Cap. 97.
2. If there was infringement, what remedies are available to the Complainant.

1. ISSUE ONE: WHETHER THERE WAS AN INFRINGEMENT OF THE COMPLAINANT'S RIGHTS UNDER THE ACT

1.1. Request to delete personal data

The Complainant stated that, pursuant to Section 16(1)(b) of the Data Protection and Privacy Act, Cap. 97, and Regulation 29(1)(b) of the Data Protection and Privacy Regulations, 2021, he requested the Respondent via email on 25th November 2024 to delete his Personally Identifiable Information (PII) and Know Your Customer (KYC) data. The request was based on his decision to discontinue using the Respondent's platform.

Personal DATA Protection OFFICE

Subsequently, in an email dated 6th December 2024, the Complainant further requested confirmation of secure deletion of his data upon expiration of the statutory retention period of 10 years, as stipulated by Section 8(3) of the Anti-Money Laundering Act, Cap. 118.

In its response dated 27th November 2024, the Respondent indicated compliance with the deletion request by removing the Complainant's account and wallet from its platform. However, the Respondent clarified that KYC and transactional data could not be deleted due to statutory retention obligations under Section 8(3) of the Anti-Money Laundering Act, Cap. 118. Notably, the Respondent did not provide evidence responding to the Complainant's request for proof of secure deletion after the mandatory retention period.

Upon reviewing the submissions and evidence from both parties, PDPO concluded that the Respondent's retention of the Complainant's KYC and transactional data complies with applicable regulatory obligations and is therefore lawful. Accordingly, there was no infringement of the Complainant's right to request deletion of personal data under the Data Protection and Privacy Act, Cap. 97. PDPO further determined that the Respondent's communication to the Complainant regarding the handling of his data was sufficiently clear. Nonetheless, the Respondent remains obligated to securely delete the data after the legally mandated retention period. This conclusion does not prejudice the Complainant's right to future action if the Respondent fails to delete the information after the prescribed 10-year retention period.

1.2. The Respondent's failure to acknowledge that it lacks the Complainant's explicit consent to process, share, or use his data beyond retention during the 10-year period.

On 6th December 2024, the Complainant informed the Respondent via email that he had not provided explicit consent for the processing, sharing, or use of his personal data for any purpose other than retention, as required for 10 years under Section 8(3) of the Anti-Money Laundering Act, Cap. 118.

In its Privacy Notice submitted to the PDPO on 13th January 2025, the Respondent, under Section 7, correctly identifies the statutory obligation to retain personal data for at least 10 years, citing compliance with Section 8(3) of the Anti-Money Laundering Act, Cap. 118 as the legal basis. However, the Privacy Notice does not explicitly address whether the Respondent intends to process or share the retained data beyond regulatory compliance purposes, nor does it specify how explicit consent would be obtained for any such additional processing during the retention period. Consequently, without explicit disclosure and consent from data subjects, including the Complainant, the Respondent is not permitted to process or share retained data for purposes beyond compliance.

Should the Respondent wish to use or share the Complainant's personal data for any additional purposes beyond regulatory compliance, explicit consent from the Complainant must first be obtained.

1.3. Notification of data breaches to the Complainant

The Complainant, in an email dated 6th December 2024, requested that he be notified of any data breaches involving his personal data. He asked that such notification obligations should continue even when he ceases to be an active user on the Respondent's platform. He further insisted that the Respondent accept unconditional liability for any unauthorized disclosure of his data.

The Respondent in its reply dated 6th December 2024 averred that, as required by Section 23 of the Act, Cap. 97, it will inform the PDPO of any data breaches. However, it did not explicitly address whether it will notify the Complainant directly, nor does it agree to unconditional liability arising out of unauthorised disclosure of his data.

After reviewing the correspondence between the Parties, PDPO has made the following determinations:

(i) Notification of data breaches

Section 23(1) of the Act, Cap. 97, requires that a data controller or processor immediately notify PDPO of any data breaches. The Respondent's position on this matter is consistent with the statutory requirement. Section 23(2) of the Act, Cap. 97 provides that once the

PDPO is notified of a data breach, it is the PDPO's role to assess the situation and, if necessary, instruct the data controller or processor to notify the affected data subject(s), such as the Complainant. As such, the Complainant's request to be directly notified of data breaches involving his personal data is addressed by Section 23(2) of the Act, Cap. 97, which mandates the PDPO to evaluate and guide such notifications. The circumstances of a breach mandate the actions to be taken by the data controller and the PDPO and cannot be determined in advance.

(ii) Unconditional liability for unauthorised disclosure

Section 33 of the Act, Cap. 97, provides that a data subject may seek compensation through a court of competent jurisdiction if a data controller or processor's non-compliance results in damage or distress. Liability is determined by law based on violations of the Act, Cap. 97, leaving the Respondent no discretion to decline liability in such cases. Therefore, the Respondent is bound by the statutory framework, making any agreement to "unconditional liability" unnecessary.

1.4. Notification to the Complainant when the Respondent's subcontractors are granted access to his data

In an email dated 6th December 2024, the Complainant requested to be notified whenever the Respondent engaged subcontractors who were granted access to his personal data, particularly if such access had not been authorized by him during his time as the Respondent's client.

Upon review of the submissions and evidence, the PDPO finds that the Respondent's Privacy Notice sufficiently addresses the obligation to notify the Complainant about subcontractor access. Section 8 of the Privacy Notice outlines the general categories of subcontractors and third parties, such as service providers, professional advisors, financial institutions, and regulators, who may access personal data. This provision ensures the Complainant is informed about the types of entities that may handle his data, meeting the transparency obligations under Section 3(f) of the Act, Cap. 97.

In addition, Section 13 of the Privacy Notice establishes a mechanism for notifying data subjects of material changes, including updates to subcontractors or categories of third parties. It states that such changes will be communicated in advance through email. This ensures the Complainant will be informed before any significant changes take effect.

The PDPO determines that these provisions adequately address the Complainant's request for notification regarding subcontractor access. By providing clear categories of subcontractors and a mechanism for notifying data subjects of changes, the Respondent complies with its transparency obligations under the Act, Cap. 97.

1.5. Providing the Complainant with a copy of all data collected about him.

In an email dated 6th December 2024, the Complainant requested that the Respondent share all data collected about him citing his right to access his data in a portable format.

In their response via an email dated 6th December 2024, the Respondent stated that while the Act, Cap. 97 does not explicitly provide for the right to data portability, the Complainant has the right to access his personal data. In the same email, the Respondent further guided the Complainant to submit a formal request in the format prescribed by the Data Protection and Privacy Regulations, 2021, to facilitate access to his personal data.

The PDPO finds that the Complainant's request to access his personal data aligns with the provisions of Section 24 of the Act, Cap. 97 which grants data subjects the right to access their personal data held by a data controller. The Respondent's position on the absence of a specific right to data portability is also accurate, as the Act, Cap. 97 does not confer this right. We further find that the Respondent's guidance directing the Complainant to follow the prescribed format under the Data Protection and Privacy Regulations, 2021, was appropriate and in line with procedural requirements for accessing personal data.

2. ISSUE TWO: IF THERE WAS INFRINGEMENT, WHAT REMEDIES ARE AVAILABLE TO THE COMPLAINANT

Based on the assessment provided under issue one, PDPO makes the following determination regarding remedies available to the Complainant:

2.1. Retention and use of data

PDPO found no infringement concerning the Respondent's retention of KYC and transactional data as mandated by Section 8(3) of the Anti-Money Laundering Act, Cap. 118. However, it determined that explicit consent is required for any processing or sharing of the Complainant's data beyond regulatory compliance obligations. As such, the Respondent is directed to:

- Amend its Privacy Notice to explicitly state that any processing or sharing of retained personal data beyond regulatory compliance purposes will require prior explicit consent from data subjects, including the Complainant.

2.2. Notification of data breaches

The Respondent's obligation to notify PDPO of data breaches is compliant with the Act, Cap. 97. Given the statutory provisions in Section 23(2), direct notification of breaches to the Complainant is guided by PDPO's assessment of each breach. No infringement was found; thus, no further remedy is required.

2.3. Liability for unauthorized disclosure

PDPO determined that liability for unauthorized disclosure is governed by statutory provisions in Section 33 of the Act, Cap. 97. Consequently, the Complainant retains the right to seek legal recourse in a court of competent jurisdiction should any damage or distress arise from unauthorized disclosures. No additional remedy is necessary.

2.4. Notification regarding subcontractors

The Respondent sufficiently addressed the Complainant's request regarding notification about subcontractors accessing his data through its Privacy Notice. No infringement occurred; therefore, no remedy is required.

2.5. Access to personal data

The Respondent appropriately guided the Complainant to submit a formal request under the Data Protection and Privacy Regulations, 2021, to access his personal data. This aligns with procedural requirements, and thus no infringement was found.

Personal DATA Protection OFFICE

DECISION:

Having considered the submissions and evidence presented by both parties, the Personal Data Protection Office issues the following decisions in accordance with the Data Protection and Privacy Act, Cap. 97, and the Data Protection and Privacy Regulations.

1. PDPO finds no infringement of the Complainant's rights under the Data Protection and Privacy Act, Cap. 97, and thus no additional remedial actions are warranted. However, the Respondent is required to explicitly clarify in its Privacy Notice that processing or sharing of retained personal data beyond regulatory compliance obligations necessitates prior explicit consent from the data subjects, including the Complainant.

2. Should the Respondent breach its commitments as articulated in the Privacy Notice or fail to comply with explicit consent requirements, the Complainant retains the right to seek remedies through legal action pursuant to Section 33 of the Act, Cap. 97.

3. Failure by the Respondent to adhere to this decision constitutes an offence under Regulation 48 of the Data Protection and Privacy Regulations, punishable by a fine of three currency points per day of default or imprisonment not exceeding six months, or both.

4. Any party aggrieved by this decision may appeal to the Minister of ICT and National Guidance within thirty (30) days from the date of receipt of this decision, as stipulated in Regulation 46 of the Data Protection and Privacy Regulations.

Dated this 12th day of March 2025

.....

Baker Birikujja

FOR: NATIONAL PERSONAL DATA PROTECTION DIRECTOR