PERSONAL DATA PROTECTION OFFICE (PDPO)

GUIDANCE NOTE ON THE COMPLETION OF THE ANNUAL DATA PROTECTION AND PRIVACY COMPLIANCE REPORT

Created: May, 2023

Revised: January 2024

Version: 1.2

Personal Data Protection Office (PDPO)
Palm Courts, Plot 7A
Rotary Avenue (Lugogo Bypass)
Office: +256 759 848 259
E-mail: info@pdpo.go.ug
website: www.pdpo.go.ug

A. Background

Regulation 50 of the Data Protection and Privacy Regulations, 2021 requires every data collector, data controller and data processor (collectively referred to as "**organisations**") registered with the Personal Data Protection Office (**PDPO/the Office**) under the Regulations to submit to PDPO within **ninety (90) days** after the end of every financial year, a summary of –

i) all complaints received and the status of such complaints, including whether the complaint was resolved or is still pending; and

ii) all data breaches and the action taken to address such data breaches.

We expect that this summary shall be submitted in a report referred to as the Annual Data Protection and Privacy Compliance Report. To ensure adequate compliance levels, PDPO has expanded the scope of this report by invoking Regulation 4(b) of the same Regulations, which empowers PDPO to coordinate, supervise and monitor data collectors, data controllers, data processors and data subjects on all matters relating to the Act. This expansion aims to provide PDPO with comprehensive overview of organisations' compliance efforts with the Act and its Regulations.

To this end we have developed and made available a template for the Annual Data Protection and Privacy Compliance Report which can be accessed from the "Information Centre" page on the PDPO website (https://www.pdpo.go.ug/). This template outlines our expectations for all organizations required to submit the Annual Data Protection and Privacy Compliance Report at the end of each Government of Uganda financial year and serves as a guide for reporting.

The **financial year** of PDPO alluded to under Regulation 50 above means a period of twelve months (the **Government financial year**) that commences on the 1st day of July and ends on the 30th day of June of the following year as stipulated under Section 3 of the Public Finance Management Act of 2015.

Consequently, the Annual Data Protection and Privacy Compliance Report shall be submitted between **1st July and 30th September** each financial year.

The purpose of this Guidance Note aims to provide Data Protection Officers (DPOs) a detailed, step-by-step process for completing and submitting the Annual Data Protection and Privacy Compliance report to PDPO.

B. Key considerations for completing the Annual Data Protection and Privacy Compliance Report

The template consists of ten (10) sections, with nine (9) covering specific areas of compliance with the Data Protection and Privacy Act and its Regulations, while the tenth section is reserved for feedback to the PDPO. It is mandatory for organisations to fill in these sections correctly and appropriately before submitting the report.

We urge organizations to diligently complete all ten sections of the provided template, ensuring no information is omitted. Even if a specific activity has not been performed, no data protection and privacy-related breaches or complaints have been documented, or there have been no changes to the registered particulars of the organization, it is essential to complete the report accurately, reflecting the current state of the organization or individual, without removing any sections or stating 'not applicable.

The only exception to this rule is the Data Protection Impact Assessment section, where an organization that has not conducted one may respond with 'not applicable'. It is anticipated that when an organization completes this template, it will accurately portray the organization's compliance status and furnish exact details throughout the report. Upon completion, signing, and scanning, the report should be submitted to the PDPO via email to compliance@pdpo.go.ug.

C. Completing and submitting the Annual Data Protection and Privacy Compliance Report

Before you begin completing and submitting your Annual Data Protection and Privacy Compliance Report, it is essential to understand the following key terms:

i) **Data Controller:** means a person who alone, jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.

ii) **Data Processor:** in relation to personal data, means a person other than an employee of the data controller who processes the data on behalf of the data controller.

iii) **Data Protection Officer (DPO):** A designated person within an organization responsible for overseeing data protection and privacy strategy and ensuring compliance with the Data Protection and Privacy Act and its Regulations.

iv) **Data Protection Impact Assessment:** A process to identify and mitigate risks associated with data processing activities that may pose a high risk to individuals' rights and freedoms.

Please follow this step-by-step guidance for completing and submitting your Annual Data Protection and Privacy Compliance Report:

Step 1:

Prepare your report using the provided template which can be accessed from the "Information Centre" page on the PDPO website (https://www.pdpo.go.ug/). Ensure that you maintain the same format and headings.

Step 2:

Complete each section of the report with the required information:

1. Background:

Describe the organization's core activities or Government mandate for public bodies, and how they involve personal data processing. Additionally, state

whether your organization has a data protection and privacy compliance program or strategy approved by its management.

2. Registration with PDPO:

2.1. Renewal status:

Provide the following information regarding your organization's PDPO registration:

i) the registration status,

ii) registration number as specified on the certificate, and

iii) renewal date. Remember that PDPO registration remains valid for a twelve-month period. To maintain continuity, make sure to schedule the renewal date at least three months before the current registration expires.

2.2. Changes in registered particulars:

This section requires you to update us on any modifications made to your organisation's registered particulars. The term 'registered particulars' here refers to the information you provided us during the registration process with the PDPO.

You will therefore be required to notify us of any changes to the organisation's physical address, nature of business, name, phone contact, Data Protection Officer's details, personal data collection details including personal data collected and/or processed, purpose, retention period, third parties with whom personal data is shared, or security measures put in place to ensure the integrity of the personal data collected and processed by your organisation or any other information provided during registration.

Please note that this section does not exempt organisations from the obligation to inform PDPO of any changes to the information in the register within fourteen (14) days of the change occurrence, as mandated by Regulation 27.

3. Leadership and Oversight

In this section of the Annual Compliance Report, you are expected to furnish us with details on the Data Protection Officer (DPO)'s reporting line and the roles of other staff who support the DPO in their leadership and oversight responsibilities within the organisation. Include aspects of the DPO's job description and performance appraisal on their responsibilities as stipulated by the law.

3.1. Reporting line and team of staff supporting Data Protection Officer

You are required to notify us of the position within the organisation to which the DPO reports. We suggest that this information should be guided by a formal communication made to the DPO regarding their reporting line. It is therefore not advisable to presume a reporting line based on the DPO's job description in another capacity within the organisation, if they hold additional responsibilities.

Regarding the staff members supporting the DPO, you are required to inform us whether any officers or staff have been designated to support the DPO in their responsibilities. This implies that these individuals should be aware of their assignment. It is sufficient for you to provide us with their positions and not the names of the individuals.

3.2. Job description of the Data Protection Officer

Clearly articulate whether the DPO has a job description addressing specific responsibilities as detailed in Regulation 47 (3) of the Data Protection and Privacy Regulations.

3.3. Performance Appraisal of the Data Protection Officer

Describe how the most recent performance appraisal of the DPO evaluated their effectiveness in fulfilling the responsibilities mentioned in Regulation 47 (3) of the Data Protection and Privacy Regulations. Report any key achievements, challenges faced, and areas for improvement identified in the appraisal.

4. Notices, Policies and Procedures

In this section, you are expected to provide us with updates on the various notices/statements/disclosures, policies and procedures that your organisation has developed and approved by management. Data protection and privacy notices/statements/disclosures and policies are crucial for compliance with the Data Protection and Privacy Act and its Regulations, which mandates the appropriate handling and protection of personal data. These documents assist organisations in complying with relevant regulatory requirements.

We expect you to provide us with the titles of the notices/statements/disclosures and policies, their approval dates, and their review dates, where applicable. It is recommended that the dates mentioned here are consistent with the dates provided in the different notices/statements/disclosures and policies. The notices/statements/disclosures, policies and procedures to be included in this section should primarily focus on privacy, information security, and records management. They should be presented using the exact names approved by the management.

5. Training and Awareness

5.1. Training of DPO, staff and third-party contractors

This section consists of three parts and should be completed separately to indicate the training received by the Data Protection Officer, the staff and third-party contractors on data protection and privacy. Regulation 47(4) mandates organisations to provide appropriate training to their designated Data Protection Officer to enable them to perform their duties efficiently. It is equally important to conduct training and awareness sessions for staff and third-party contractors to help them understand their responsibilities in safeguarding the privacy of personal data.

To complete this section, you are required to provide information on whether the Data Protection Officer has received the necessary training. This training could include any trainings/ webinars organized by the Personal Data Protection Office, certifications on data protection and privacy, and any in-house training that the officer has undertaken. You should indicate the scope of the training, the date it was received, and the facilitator.

When reporting on data protection and privacy training and awareness of staff, you are required to provide us with a breakdown of the total number of staff in each department and the number that completed the training.

It is important to note that any training that covers aspects of data protection and privacy may be included in this section.

5.2. Commemoration of the International Data Privacy Day

Provide a comprehensive report on how your organization observed the International Data Privacy Month. This report should detail the initiatives undertaken to enhance awareness of the Ugandan Data Protection and Privacy Act, along with its Regulations, among staff, third-party contractors/agents, and customers. It is imperative that the report not only addresses the awareness of the legislation but also encompasses the data protection and privacy commitments asserted by your organization in its policies and notices. Please ensure to attach any relevant photographic evidence supporting these activities.

6. Complaints related to data protection and privacy

Under this section, we require you to report on any complaints received by your organisation during the reporting period from individuals who believe that their rights or the rights of another individual have been infringed upon by the organisation. The Data Protection and Privacy Act empowers an individual who believes that their rights or those of another individual have been infringed upon by an organisation to make a complaint.

Data Protection Officers (DPOs) are also required to provide information on the complaint handling mechanisms they have implemented within their organizations. DPOs should outline the clear and well-defined procedures in place for addressing privacy-related complaints, demonstrating their commitment to safeguarding personal data and ensuring compliance with the Data Protection and Privacy Act and accompanying Regulations.

PDPO's Guidance Note on lodging complaints with PDPO directs complainants to first bring their complaints to the attention of the organisation before submitting them to PDPO. The Guidance Note also provides examples of complaints related to data protection and privacy.

We expect therefore that you will provide us with details of the complaints received by the organisation, including their status of resolution, as either resolved or pending in this section. The total number of complaints received should tally with the number of complaints resolved and pending. Additionally, you should identify the most frequent type of complaint and provide us with the percentage of resolution for this category of complaints.

7. Data Security Breaches

A data security breach occurs when an organisation's safeguarding of personal data is compromised, resulting in its unlawful destruction, loss, alteration or unauthorized access. A breach may manifest in various forms, including access to an organisation's personal data, its disruption, modification, or destruction by an unauthorized person.

You are required to update PDPO under this section with information regarding any data security breaches that your organisation may have experienced during the reporting period. We expect that you will disclose the total number of data security breaches that have occurred, the number of

breaches reported to PDPO in compliance with section 23 of the Data Protection and Privacy Act, and the number of breaches that have been resolved. Furthermore, you are expected to provide us with details about the most common cause of these breaches.

Organizations are also required to provide information on the measures they have taken to address gaps that contributed to data breaches. This includes outlining the remedial actions implemented by management to prevent future breaches.

Please be aware that this section does not relieve organizations of their responsibility to promptly notify PDPO of any breaches, as required by Section 23.

8. Data Protection Impact Assessment

The Data Protection and Privacy Regulations require a Data Protection Impact Assessment (DPIA) to be carried out where the collection or processing of personal data poses a high risk to the rights and freedoms of the individuals. This section of the template requires an organisation to report on whether it conducted a Data Protection Impact Assessment during the reporting year.

Where the organization has conducted a DPIA, it is required that you provide details on the data collection or processing activity that required it, as well as the date the assessment was completed. Please note that the aforementioned details should only be included in this section if a DPIA was conducted during the reporting year.

9. Data Protection and Privacy Audits

Under the Data Protection and Privacy Regulations, Data Protection Officers are required to conduct regular assessments and audits to ensure compliance with the Act. To assist you in conducting these audits, we have developed self-assessment tools which were shared with registered DPOs that outline our expectations for all organisations that collect and process personal data and

are subject to the provisions of the Data Protection and Privacy Act, 2019 and its corresponding Regulations.

The information on audits required under this section concern those assessing your organisation's procedures for data collection and processing, as well as information security procedures to ensure compliance with the Data Protection and Privacy Act and the regulations thereunder. These audits could have been conducted internally or externally by the Personal Data Protection Office or any other external persons qualified to conduct privacy audits or assessments. You can still report on an audit even where it did not explicitly refer to data protection and privacy audit as long as it covered aspects of your organisation's compliance with data protection and privacy laws.

We recognize that audits and assessments have the potential to uncover instances of non-compliance and provide recommendations for corrective action. Therefore, please ensure that, along with the number of internal or external assessments conducted, you also report the percentage of audit recommendations that have been implemented.

10. Major take-ways, general observations and challenges in relation to ensuring compliance with the Data Protection and Privacy Act

We consider this section as a suggestion box. You may provide us with information on your major takeaways, observations and challenges with compliance with the data protection and privacy laws within the reporting year.

This section enables us to understand generally your compliance journey and informs our decisions on how to better provide you with support to ensure your compliance with the Data Protection and Privacy Act.

D. Submission of the Annual Data Protection and Privacy Compliance Report

Once completed, we expect that the report will be signed to indicate ownership of the information that was shared with us. We recommend that the report is

signed, sealed/stamped by an authorized officer with the ability to bind the organisation who may hold any of these positions; Chief Executive Officer, Managing Director, Director, Manager, or Company Secretary, among others. The organization should provide his/her name, title, and the date of submission when signing the report.

The completed, signed, sealed/stamped and scanned report shall then be submitted to the Personal Data Protection Office through this email address compliance@pdpo.go,.ug.

Note:

We may update this Guidance Note. If we make changes, we shall let you know through indication of our version control referencing number, month and year when the changes were effected on our cover page.

This Guidance Note contains practical guidance on how to complete the Annual Data Protection and Privacy Compliance Report Template provided by the Personal Data Protection Office. It does not have the status of legal advice but aims to help you ensure compliance with the Data Protection and Privacy Act, 2019 and the Data Protection and Privacy Regulations, 2021.