'creating a level playing field'

CYBER AND DATA PROTECTION IMPLEMENTATION GUIDELINE ON CROSS BORDER TRANSFER OF PERSONAL INFORMATION

CDPG 5 OF 2024

1. PURPOSE AND EFFECTIVE DATE

This guideline is issued in terms of Sections 6(1) (a) and 28 (3) of the Cyber and Data Protection Act [*Chapter 12:07*] (hereinafter referred to as "the CDPA") which provides that the Authority shall lay down the conditions and circumstances for cross border transfer of personal information. The guideline seeks to give general guidance to data controllers and data subjects on conditions for cross-border transfer of personal data. It shall be read in conjunction with the CDPA and regulations. The guideline shall be effective from the date of publication.

2. INTRODUCTION

The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) is the designated Data Protection Authority. According to Section 28, POTRAZ is responsible for specifying the categories of data that can be transferred outside of Zimbabwe and the conditions thereof. The reason for restrictions under cross-border transfer provisions in sections 28 and 29 is to guarantee that the personal data being transferred will receive a level of protection comparable to that afforded in Zimbabwe under the CDPA. It is highly recommended that data controllers adopt the practices outlined in these guidelines as a crucial aspect of their statutory responsibility to safeguard personal data.

3. REQUIREMENTS FOR TRANSFER

Data controllers are prohibited from cross-border data transfers unless they have notified the Authority. The data controller must first notify the authority of their intention to transfer data and must satisfy the following conditions before transferring data from Zimbabwe:

3.1 Conduct a Data Protection Impact Assessment (DPIA)

Before transferring personal information outside of Zimbabwe, a data controller must first perform a data protection impact assessment to identify any potential risks associated with the transfer. The results of the DPIA must be submitted to the Authority when notifying the Authority of the cross-border data transfer.

3.2 Obtain Consent from the Data Subject before transfer

No data can be transferred outside Zimbabwe without the express consent of the data subject. The data subject must be informed about:

- the impending data transfer.
- the reasons for the transfer.
- the destination country and organization.
- the security measures that will be used by the third-party recipient.
- where the data will be stored and duration.

The data subject will then have the right to either consent to or decline the transfer.

3.3 Demonstrate Data Security Adequacy

A data controller is not allowed to transfer personal data to a third party in a foreign country unless they can show that the foreign country provides an adequate level of protection for the personal data. When evaluating the adequacy of protection, the Authority will consider the following:

3.3.1 The laws and regulations in the foreign country, including data protection rules, professional standards, and security measures, as well as the effectiveness of these measures in protecting individuals' rights and providing legal remedies.

3.3.2 The existence and effectiveness of a data protection supervisory authority in the foreign country responsible for enforcing data protection rules. The authority should have sufficient enforcement powers and be able to help and advise individuals on their data protection rights.

3.3.3 The international agreements and legal obligations of the foreign country or international organization, particularly those related to data protection.

3.4 Organisational & technical measures

The data controller must have measures in place to protect the personal data being transferred. These measures include but are not limited to the following:

a. Security measures;
b. Procedures for notifying data breaches, policies, and procedures;
c. Data breach incidence response plans; and
d. Data protection policies and compliance frameworks.

3.5 Data Protection Sharing Agreement

Every data controller must enter into a data-sharing agreement with any third-party recipient to whom they intend to transfer data. This agreement should include the third party's concessions as outlined in clause 4 of this guideline. The agreement must specify how the data will be transferred, the condition of the data during transfer, where the data will be stored, and the security measures that will be used to protect the data.

4. MEASURES TO BE IMPLEMENTED BY THIRD-PARTY RECIPIENTS TO SAFEGUARD PERSONAL DATA

Third-party recipients of data must commit to protecting the personal data they receive. The data controller is responsible for ensuring that the third party has implemented appropriate safeguards to secure the personal information. This can be achieved through several techniques such as:

4.1 Agreement on Data Protection Safeguards

The data controller and the third-party recipient must enter into a formal agreement specifying the data protection safeguards that the third party will implement. This agreement should detail the measures and protocols that will be put in place to ensure the data's security and privacy.

4.2 Data Protection Clause in the Data Sharing Agreement

The data-sharing agreement between the data controller and the third-party recipient must include a specific data protection clause. This clause should outline the responsibilities of the third party regarding the protection of personal data, including compliance with relevant data protection laws and the implementation of security measures.

4.3 Understanding the Rules of the Destination Country

The data controller must thoroughly understand the legal and regulatory framework of the country to which the data will be transferred. This includes familiarizing with the data protection laws, security measures, and enforcement practices in that country. By doing so, the data controller can ensure that the third-party recipient can adhere to the necessary standards and that the personal data will be adequately protected.

5. STORAGE OF PERSONAL INFORMATION

5.1 Before transferring data outside Zimbabwe, it is crucial for the data controller to have a clear understanding of the storage location and potential processing methods. The data controller must conduct a thorough due diligence exercise to identify and prepare for potential data breaches before the transfer of data. This also enables the data controller to implement sufficient safeguards to protect data subjects' personal information which they intend to transfer.

5.2 In the letter requesting prior authorization, the data controller or processor who intends to transfer data outside must demonstrate to the Authority fulfillment of the requirements above.

5.3 Data controllers that transferred personal information prior to the CDPA must regularise such transfer by notifying the Authority in writing and adhering to the above requirements.

6. ADHERENCE TO DATA PROTECTION PRINCIPLES

6.1 Transferring data outside the borders of Zimbabwe constitutes a type of data processing. When transferring data to other countries, it is important for data controllers to adhere to the data protection principles, just as they would do with any other form of processing locally. Personal information may not be used for a new purpose. “New purpose” means in essence any purpose other than the one for which the personal data was originally collected or a directly related purpose.

6.2 In addition, it is becoming more and more common for data controllers to outsource and delegate personal data processing tasks to data processors. When a data controller enlists the help of a data processor to handle personal data outside Zimbabwe, it is important for the data controller to establish contractual or other measures. These measures serve two purposes:

6.2.1 ensuring that the personal data transferred to the data processor is not retained for longer than necessary for processing, and

6.2.1 safeguarding against unauthorized or accidental access, processing, erasure, loss, or use of the transferred data by the data processor.

6.3 Where a data controller shares data subjects' personal data with a controller/processor located outside Zimbabwe, they must still adhere to the Zimbabwean data protection principles. Thus, the responsibility for the actions carried out by an agent with the authority of the data controller ultimately falls on the data controller.

7. CIRCUMSTANCES WHERE DATA MIGHT BE TRANSFERRED WITHOUT THE CONSENT OF THE DATA SUBJECT

The law allows for certain exceptions where data may be transferred outside Zimbabwe without the consent of the data subject. It is imperative however that, in such circumstances, the authority must be notified. These circumstances are:

7.1 **Cross border transfer pursuant to a contractual obligation between the data controller and data subject**

A data controller is not required to seek consent of the data subject when transferring data outside Zimbabwe when it is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures in response to the data subject's request. Data controllers are still encouraged to inform the data subject before data is transferred especially before entering into an agreement so that the data subject can make an informed decision.

7.2 **Public interest or legal reason**

The transfer is necessary or legally required for important public interest reasons or the establishment, exercise, or defense of legal claims.

7.3 **Information contained in public registers.**

The transfer is made from a register that is specifically designed to provide information to the public. This register is open for consultation by the public or any person who can show a legitimate interest. However, the transfer can only take place if the conditions specified in the law or prior consultation are met in the specific case.

8. WHO IS REQUIRED TO COMPLY WITH CDPA SECTIONS 28 AND 29?

Every data controller is required to comply with CDPA. A data controller is a person who either alone or jointly or in common with other persons, controls the collection, holding, processing, transfer or use of personally identifiable information.

9. TYPES OF CROSS BORDER TRANSFER

Transfer of data may occur as follows:

9.1 Transfer of personal data from Zimbabwe to a place outside Zimbabwe, and transfer of personal data between two jurisdictions where the transfer is controlled by a Zimbabwean data controller and or involves the personal information of Zimbabwean data subjects.

9.2. Engaging a processor located outside Zimbabwe to process personal data on its behalf, regardless of where the personal data is stored.

9.3. Storing personal data of customers and/or employees in a centralized database and sharing it with sister companies within the same holding company worldwide.

9.4. Storing personal data in the cloud also constitutes a transfer outside Zimbabwe if the cloud server is accessible outside Zimbabwe.

9.5. Situations that may involve cross-border transfer of personal data include the adoption of an offshore database system, outsourcing of data processing and/ or storage functions, and intra-group (members located outside Zimbabwe) sharing of data. There are many other instances where the transfer of personal data outside Zimbabwe occurs. Data controllers should assess whether such activities are necessary prior to such transfer.

9.6. For the avoidance of doubt, the transfer of personal data by a data controller located in Zimbabwe, but because of Internet routing through a place outside Zimbabwe (without being accessed or stored as part of the transmission mechanism), to a recipient also located within Zimbabwe does not constitute a cross-border transfer of data. However, the position will be different where the targeted recipient is located outside Zimbabwe. In addition, if a multi-national corporation stores personal data in an internal server located in Zimbabwe but its employees working in offices outside Zimbabwe are allowed to download the personal data, it is a cross-border transfer of data and this guideline must be followed.

10. PRACTICAL TIPS AND BEST PRACTICES

Below are some recommended steps for data controllers to comply with the CDPA when transferring personal information outside Zimbabwe:

10.1 **Establishing or reviewing data transfer arrangements**

Data controllers should have in place data transfer agreements and where these were already in place before the CDPA, there is a need to review existing data transfer arrangements to identify any cross-border transfer of personal data.

10.2 Control cross-border data flow activities

Data controllers should control activities that involve unintended or unnecessary cross-border data flow to avoid non-compliance data protection laws. It is not uncommon for data controllers to exercise control through configuring their information technology systems. One way is for international companies to structure the information technology system so that certain types of data cannot be accessed or downloaded by employees working in offices outside Zimbabwe.

10.3 Keep inventory of personal data

Another important aspect is for data controllers to keep an inventory of the personal data being transferred outside Zimbabwe. Data controllers must always bear in mind that they remain responsible and accountable to the data subjects for possible contraventions of the CDPA. It is in the interest of controllers to monitor the data handling process of the transferees, to keep abreast with the whereabouts of the personal data, and to assess the associated privacy risks. Also, data controllers should be transparent about their data handling policies and practices regarding any transfer of personal data outside Zimbabwe.

10.4 Conduct regular data transfer impact assessments, audits, and inspection

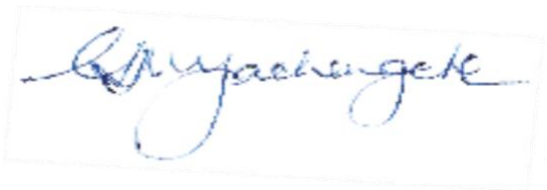
An effective monitoring tool for adequate and continued protection offered to the personal data transferred outside Zimbabwe is regular transfer impact assessments, audits, and inspections on the transferees' operations to ascertain compliance with their obligations under the data transfer agreement.

11. PENALTIES

Any data controller, his or her representative, agent or assignee who contravenes section 28 on cross border transfer requirements shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.

For complaints and further guidance, contact the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) on dataprotectionunit@dpa.zw; regulator@potraz.zw or call +263 242 333032/46/48.

ISSUED ON THIS 13th DAY OF NOVEMBER 2024.



POTRAZ DIRECTOR GENERAL