'Creating a level playing field'

CYBER AND DATA PROTECTION IMPLEMENTATION GUIDELINE ON PROCESSING CHILDREN'S PERSONAL INFORMATION

CDPG 2 OF 2024

1. PURPOSE AND EFFECTIVE DATE

This guideline is issued in terms of section 6 (1) of the Cyber and Data Protection Act [*Chapter 12:07*] ('the CDPA') which mandates the Postal and Telecommunications Regulatory Authority of Zimbabwe as the Data Protection Authority, to create conditions for the lawful processing of personal information, including that of minors. The guideline seeks to provide detailed requirements to be met by data controllers when processing children's information and shall be read in conjunction with the CDPA and the regulations, Statutory Instrument 155 of 2024. The guideline is effective from the date of publication.

2. INTRODUCTION

2.1 According to Section 57 of the Constitution of Zimbabwe, all persons enjoy the right to privacy, including children, that is anyone below the age of eighteen years in accordance with section 81 of the Constitution. This fundamental right must be upheld in all data processing activities by both controllers and processors.

2.2 Children enjoy the same data subject rights outlined in section 14 of the CDPA as adults. When processing children's personal data children's right to privacy must be at the forefront from the outset and systems must reflect the need to protect children by design and by default.

2.3 Section 26 of the CDPA, provides that children's rights to privacy must be exercised by their legal guardians as they do not have the legal capacity to give consent to the processing of their personal information. Therefore, data controllers and processors must obtain written consent from the children's legal guardians before processing personal information of minors.

3. KEY CONDITIONS FOR PROCESSING CHILDREN'S DATA

The Authority is committed to ensuring a high standard of data protection for all citizens, especially children due to their increased vulnerability in the digital age. To this end, the following conditions must be met by data controllers and processors when processing personal information of minors:

3.1 Consent:

3.1.1 The CDPA prohibits the processing of children's data without obtaining the written consent of the parent. The law aims to protect children from possible abuse arising from the imbalance of power between a child and a data controller or processor.

3.1.2 Data controllers must verify the legal status of the parent or legal guardian by requesting relevant documentation such as birth certificates, adoption orders, custody orders, or guardianship orders that prove the guardianship of the child concerned.

3.1.3 The data controller must ensure that children and their parents/ guardians understand what they are consenting to. The request for consent must be clear and easy to understand and must be in an age-appropriate manner.

3.2 Best Interests of the Child:

When processing children's personal information, data controllers must always prioritize the

best interests of the child which may be demonstrated through:

3.2.1 promoting the rights of children as data subjects through age-appropriate privacy notices, policies, and awareness.

3.2.2 introducing robust organisational and technical mechanisms to secure children's data and to ensure privacy including the formulation of data protection policies.

3.2.3 desisting from processing children's personal information even if the information has been made public by the child.

3.2.4 implementing data protection by design/default for services and platforms that involve collection of children's personal information.

3.2.5 carrying out due diligence with organisations that a controller intends to share children's data with.

3.2.6 implementing upfront age verification systems and enforce age restrictions.

3.2.7 putting in place proportionate measures to prevent or deter children from providing their personal data.

3.2.8 embedding deletion mechanisms in data that is collected from children in case it becomes inappropriate to hold such data at a later stage such as, when the children become adults and capable of consenting.

3.3 Prior authorisation from the Authority

In cases of cross border transfer of personal information of minors to countries that do not have an adequate level of protection, the data controller is required to seek prior authorisation from the Authority. In addition, in cases where the processing has a high risk of infringing on the fundamental rights of the child, prior authorisation is also required unless an exemption is granted by the Authority. High risk data processing includes but is not limited to:

3.3.1. Using new technologies such as surveillance systems and tracking.

3.3.2. transferring data outside Zimbabwe.

3.3.3. processing data that could lead to discrimination or damage to reputation.

3.3.4. processing data that could lead to identity theft, fraud, or financial loss.

3.3.5. Processing data of children or other vulnerable groups.

4. INSTANCES WHEN A CONTROLLER MAY PROCESS CHILDREN'S PERSONAL DATA WITHOUT CONSENT

Whenever a data controller processes children's data without consent, the data controller must notify the Authority in writing. Instances where the controller may process children's data without consent include:

4.1 Lawful basis for processing (Authorisation by law)

The data controller may process information of minor children if they have a lawful basis or legal basis to do so in terms of an Act of Parliament or any other applicable law.

4.2 Public and vital interest

The data controller may also process information belonging to children if it is in the public interest or where it is in the vital interest of the minor.

4.3 **Legitimate interests**

A data controller may process children's data pursuant to the data controller's legitimate interest if they can demonstrate that the data controller will balance the need to protect the privacy of the minor data subject and the controller's legitimate interest in processing the data.

4.4 **Contractual obligation**

In Zimbabwe children do not have the capacity to contract. A controller may rely on a contractual obligation arising out of a contract between them and the parent or legal guardian of the minor child as a basis for processing a minor's personal data. The contract must have clear provisions on how data will be processed and shared with third parties.

5. CAN CHILDREN'S DATA BE SUBJECTED TO AUTOMATED DECISION MAKING?

Data controllers should not subject children's personal information to automated decision-making without human intervention if this will have a legal or similarly significant effect on them.

6. PRACTICAL STEPS FOR PROCESSING CHILDREN'S DATA

When processing children's personal data, a data controller must:

6.1 Put in mechanisms to obtain parental consent for the processing of children's data.

6.2 Verify the parental authority presented by the alleged parent or guardian over the child.

6.3 Use age-appropriate language and ensure that the children and their parents/guardians understand the purpose and means of processing the personal data.

6.4 Embed processing confirmation once the child becomes a major to allow for the data subject to give or revoke their prior consent which had been given on their behalf.

6.5 Embed data protection by design and by default for services and platforms that entail the processing of children's personal information.

7. KEY CONSIDERATIONS WHEN PROCESSING CHILDREN'S DATA

Some key considerations by data controllers when processing children's information:

7.1 Does a service/platform/website target children and verifies the ages of users?

7.2 What type of information does service provision/ platform/website or app collect?

7.3 Does the service/platform/website have protective measures in place to help children avoid excessive disclosure of personal data, for example: whether the platform/website prompts for parental involvement and whether the warnings are linguistically tailored for children?

7.4 Whether the platform/website/service or app provides simple ways for users including children to delete information already submitted?

7.5 Whether the privacy policy is easily accessible to users of the platform/website or service?

7.6 Whether the platform/website offers third-party advertising?

7.7 Whether all data protection principles have been implemented?

7.8 Does the controller conduct regular data protection impact assessments on platforms, products or services that involve the collection of children's data?

8. CONCLUSION

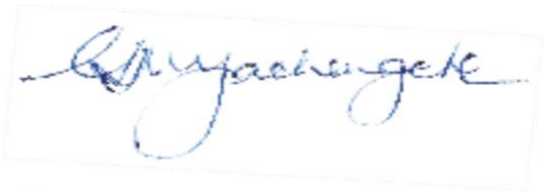
The Authority shall take appropriate regulatory action to ensure compliance with this guideline to uphold children's right to privacy. Data controllers and processors are encouraged to familiarize with these provisions and implement the necessary measures to comply with the CDPA.

9. PENALTIES

A data controller who contravenes the provisions of the Act and regulations in relation to processing of children's data as provided in this guideline 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