'creating a level playing field'

CYBER AND DATA PROTECTION IMPLEMENTATION GUIDELINE ON THE RIGHT TO CONSENT

CDPG 4 OF 2024

1. PURPOSE AND EFFECTIVE DATE

The guideline is issued in terms of section sections 6(1) (a),10, 11, 12, 13, 14, 15, 25, 28 & 29 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 consent when processing personal information. The guideline seeks to give general guidance to data controllers and data subjects on the requirements for consent prior to processing personal information. It shall be read in conjunction with the provisions of the CDPA and the regulations. The guideline is effective from the date of publication.

2. WHAT IS CONSENT?

Section 3 of the CDPA defines "Consent" as any specific clear, freely provided, informed statement of will by which the data subject or his or her legal, judicial, or legally appointed representative accepts that his or her data be processed by a data controller.

3. WHY IS CONSENT IMPORTANT?

3.1. For data controllers, consent is one of the lawful bases for processing personal information. Consent is appropriate if the controller can offer data subjects real choice and control over the use of their data. Explicit consent also enables the legitimate use of special categories of data. Consent may be relevant where the individual has exercised their right to restriction, and explicit consent can legitimise automated decision-making and cross border transfers of data. Relying on inappropriate or invalid consent has the potential to destroy trust and harm to the data controllers' reputation - and may make data controllers liable to large fines.

3.2. Public authorities, employers, and other organisations in a position of power over individuals should avoid relying on verbal consent unless they are confident, they can demonstrate it was freely given.

3.3. From the perspective of data subjects, explicit consent puts individuals in control, builds trust and engagement, and enhances the data controller's reputation.

4. LEGAL REQUIREMENTS OF CONSENT

4.1. For consent to be valid, it must meet the following requirements:
freely given, this means, controllers must give people genuine ongoing choice and control over how their data is used. It should require a positive action to opt-in and opt-out. If a data controller would still process the personal data without consent, asking for consent would be misleading and inherently unfair.

4.2. specific, this means, it must be, unbundled from other terms and conditions, concise and easy to understand, and user-friendly. If the granting of consent is a precondition of a service, it is unlikely to be the most appropriate lawful basis.

4.3. informed, this means, the data subject must be adequately informed on the reasons for processing, including further processing and their rights.

4.4. unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

4.5. confirmed in writing in instances of processing sensitive personal information and automatic data processing.

NB: The onus to prove that consent was given is on the data controller. Data controllers should keep records of consent. However, there is no set time limit for consent. How long it lasts will depend on the context. Data controllers should review and refresh consent as appropriate.

5. TYPES OF PROCESSING THAT REQUIRE CONSENT

A data controller must obtain consent from data subjects before processing the following types of data:

5.1. **Processing of non-sensitive data (CDPA Section 10)**

Personal information may only be processed if the data subject or a competent person, where the data subject is a child, consents to the processing of such data. The consent referred to above may be implied where the data subject is an adult natural person and has full legal capacity to consent. The catch is for the data controller to prove that indeed verbal consent was given.

5.2. **Processing of sensitive data (CDPA Section 11)**

No data controller shall process sensitive data unless the data subject has given consent in writing for such processing.

NB# The Authority shall determine, the circumstances in which the prohibition to process sensitive data cannot be lifted even with the data subject's consent (considering the factors surrounding the prohibition and the reasons for collecting the data).

5.3. **Processing of genetic, biometric, and health data (CDPA Section 12).**

In general, the processing of genetic data, biometric data, and health data is prohibited unless the data subject has given consent in writing to the processing.

5.4. **Automatic Data Processing (CDPA Section 25)**

If a data controller is desirous to use automated means of data processing and decision making, they must first obtain the express consent of the data subjects concerned. The data controller may process the data by automated means if the processing is necessary to comply with a legal provision requiring them to conduct such processing.

5.5. **Processing of personal data of incapacitated data subjects (CDPA Section 27)**

A data subject who is physically, mentally, or legally incapable of exercising the rights given under the COPA and who is not a child, may exercise such rights through a parent or guardian or as provided for by law or as designated by a Court of competent jurisdiction.

5.6. **Transfer of personal information outside Zimbabwe (CDPA Section 29)**

A data controller must obtain explicit consent from data subjects if they wish to transfer personal information to a country outside Zimbabwe which does not assure an adequate level of protection.

6. OBTAINING, RECORDING AND MANAGING CONSENT?

6.1. Data controllers must make consent requests prominent, concise, separate from other terms and conditions, and easy to understand. The request for consent should include the

following:

6.1.1. the name of the organisation.

6.1.2. the name of any third parties to whom the controller may rely on the consent;

6.1.3. reasons for the data collection and processing; and

6.1.4. that data subjects can withdraw consent at any time.

6.2. Data subjects must actively opt in and data controllers must not use pre-ticked boxes. Wherever possible, data subjects must be given separate options to consent to different purposes and several types of processing.

6.3. Data controllers must keep records of evidence of consent - who consented, when, how, and what they consented to.

7. WITHDRAWAL OF CONSENT

7.1. The CDPA stipulates that data subjects have the right to withdraw their consent to the processing of their personal data.

7.2. Data controllers should know that data subjects can withdraw their consent at any given time without having to meet any conditions for withdrawal nor should they give any reasons for the withdrawal of consent.

7.3. Consent must be given and withdrawn with the same ease. If consent is obtained via electronic means through only one mouse click, swipe, or keystroke, or an application then it is recommended that the data subjects must use the same or similar means to withdraw their consent.

7.4. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means that a controller must make withdrawal of consent possible free of charge or without lowering service levels.

8. LEGAL BASES FOR PROCESSING PERSONAL DATA WITHOUT CONSENT

8.1. **Contractual Obligations**: Personal data may be processed when it is essential for the performance of a contract to which the data subject is a party. For this to apply, the processing must be necessary for fulfilling the specific obligations of the contract for the benefit of the data subject. The contract must clearly outline the purpose for which the data will be used. Example: Processing payment information to fulfill an online purchase agreement.

8.2. **Legal Obligations**: Data processing is permissible when required to comply with a legal obligation to which the controller is subject. This applies when processing is mandated by a specific law or regulation. Example: Retaining employee tax records to comply with tax laws.

8.3. **Public Interest**: Processing is allowed if necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller. The task, function, or authority must have a clear basis in Zimbabwean law and not rely solely on the controller's subjective interpretation of public interest. Example: Processing census data for national statistics.

8.4. **Legitimate Interest:** Processing may occur to advance the core business or objectives of the controller unless these interests are overridden by the data subject's rights or freedoms. Controllers must conduct a Legitimate Interest Assessment (LIA) to demonstrate:

a. The necessity of the processing.
b. That the controller's interest outweighs the data subject's rights. Example: Using customer data for sending them notifications in the change in operating times.

8.5. **Vital Interests**: Data processing is allowed to protect the vital interests of the data subject or another individual, typically in situations of life or death. Example: Sharing medical information in an emergency to save a patient's life.

8.6. **Scientific Research:** Personal data can be processed by public bodies for purposes such as scientific research, statistical analysis, or historical research, provided appropriate safeguards are in place to protect the data subject's rights. Example: Anonymizing patient data for clinical trials.

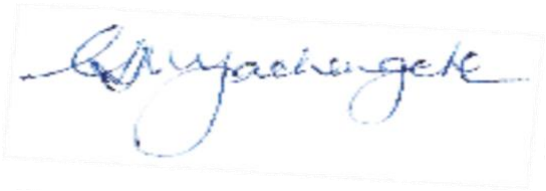
9. PENALTIES

A data controller shall take all necessary measures to comply with the principles and obligations set out in the Act and must have the necessary internal mechanisms in place for demonstrating such compliance to both the data subjects and the Authority in the exercise of its powers.

Any data controller, his or her representative, agent or assignee who contravenes sections 11, 13 and 28 in relation to the requirements for consent 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 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