

Lawful Basis for Processing under the Tanzanian PDPA

Lawful basis for processing simply means legal justification or reason that allows a person or an organization to collect, use, or otherwise process personal data. It outlines the circumstances under which processing of personal data is considered legitimate and compliant with the law.

Imagine you have developed a social media platform. Users sign up, create profiles, and share posts with their friends. They trust that their information will be used for the purpose of connecting with others and sharing content.

However, without clear and informed consent, you start using their data to create targeted advertising profiles. This means that you are collecting information about their interests, activities, and connections to show them personalized ads. This is a clear violation of the lawful basis for processing personal data because you are using it for a different purpose (advertising) without authorization.

The Personal Data Protection Act, 2022 (“**the PDPA**”) and its regulations require all data controllers and processors to have what's called a "**lawful basis**" for any collection or processing of personal data.

What is data processing? And what do you need to do to make sure you use data legally?

What is Data Processing?

Section 3 of the PDPA defines “**processing**” in relation to data to mean analysis of personal data, whether or not by automated means, such as obtaining, recording or holding the data or carrying out any analysis on personal data, including:

- a) organization, adaptation or alteration of the personal data;
- b) retrieval or use of the data; or
- c) alignment, combination, blocking, erasure or destruction of the data

So, under the PDPA, processing basically means doing things with people's personal data include things like collecting, recording, organizing, or even analyzing the data. It doesn't matter if this is done by a computer or by hand. It also covers actions like changing or using

the data in some way, as well as finding or retrieving it when needed. So, if you are doing anything with someone's personal information, you are "*processing*" it under the law.

But before you can even think about collecting data, you need to determine whether you have a right to process it under the law. You can use one or several of the lawful bases, but they must be rooted in your actual data processes.

Why is it important to have a valid reason for processing data?

It goes back to the principles of being open, responsible, and only collecting the data you actually need. For a long time, some organizations gathered data carelessly, amassing vast warehouses of data that they never intended to use. Keeping hold of unnecessary data is risky in itself. Storing large volumes of data, especially data that won't be used, increases the risk to everyone's privacy. This includes the potential for breaches and overall privacy concerns. It also cracks down on the sale and sharing of data with third parties, which also risks the data subject's right to privacy.

So, what are the lawful bases identified by the law? (**Sect. 5(a) of the PDPA & reg. 23(a) of GN 449C**)

Sect. 5(3) of the PDPA provides as follows:

“A data controller or data processor shall ensure that personal data is- (a) processed lawfully, fairly and transparently”.

Equally, **reg. 23(a) of GN 449C (Translated Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023)** provides as follows:

“The data controller or data processor when collecting or processing personal data shall ensure that the personal data are:-(a) collected or processed lawfully, fairly and transparently”.

Both **sect. 5(a)** and **reg. 23(a)** provide the legal basis for processing personal data. However, **reg. 23(a)** goes further by adding a requirement that not only must the processing be lawful, but the *collection* of the data must also be done in a lawful, fair, and transparent manner. This

emphasizes the importance of ensuring that personal data is obtained and handled ethically and in accordance with the law.

The chart below shows the lawful basis for all categories of data, excluding special category data.

S/N	Lawful basis	Applicable provision	Applicability (exceptions)
1.	Consent	<p>Reg. 25(d) of GN 449C</p> <p>Reg. 25(d).</p> <p>The data controller or data processor shall, in implementing the principle of lawfulness during the processing of personal data, consider the following important factors:</p> <p>(d) the data subject possesses an understanding of what he consented to and there is a simplified means to withdraw consent.</p> <p>Sect. 25(2)</p> <p>Where a data controller holds personal data that was collected in connection with a particular purpose, he may use that personal data for other purposes if:-</p> <p>(a) the data subject authorises the use of the personal data for that other purpose.</p> <p>Sect. 36(3)(c)</p> <p>Sect. 36(3) is quoted in item 2 regarding the legal obligation aspect</p> <p>(c) based on the data subject's explicit consent</p>	<p>This provision can be regarded as a basis for obtaining consent in the processing of personal data. It emphasizes the importance of ensuring that individuals fully understand what they are consenting to and have an easy way to withdraw that consent if they wish to do so. This is a fundamental aspect of obtaining lawful consent for data processing under the regulations.</p> <p>The person's authorization for using their personal data for another purpose can be seen as a form of consent. It means the individual has agreed to the new use of their data beyond the original purpose for which it was collected.</p> <p>The processing by automated means is only allowed with the explicit consent of the data subject.</p>

2.	Legal obligation	<p>Sect. 36 provides:</p> <p>(1) A data subject may, through the procedures prescribed in the regulations, require the data controller to ensure that any decision taken by or on behalf of the data controller which significantly affects a data subject shall not base solely on the processing by automatic means.</p> <p>(2) Without prejudice to subsection (1), where a decision which significantly affects a data subject is based solely on automated processing:</p> <p>(3) This section shall not apply if the decision is-</p> <p>(b) authorised by any written law; or</p> <p>Sect. 25(2)(f)</p> <p>Where a data controller holds personal data that was collected in connection with a particular purpose, he may use that personal data for other purposes if-</p> <p>(f) use of personal data for that other purpose is necessary for compliance with the laws</p>	<p>Sect. 36(1), (2) &(3)(b) enables a data subject to contest decisions significantly impacting them that are made solely through automated means. However, this provision exempts decisions mandated by written law, indicating a legal obligation to make such determinations automatically. Similarly, Sect. 25(2)(f) permits a data controller to repurpose personal data collected for one specific intent if required for legal compliance, affirming that legal obligations can dictate the usage of personal data for specific purposes outlined by the law.</p>

3.	Contractual obligation	<p>Sect. 36(3)(a)</p> <p>36(1) A data subject may, through the procedures prescribed in the regulations, require the data controller to ensure that any decision taken by or on behalf of the data controller which significantly affects data subject shall not base solely on the processing by automatic means.</p> <p>(2) Without prejudice to subsection (1), where a decision which significantly affects a data subject is based solely on automated processing:-</p> <p>(a) the data controller shall, as soon as practicable, notify the data subject that the decision was taken on that basis; and</p> <p>(b) the data subject may require the data controller to reconsider the decision.</p> <p>(3) This section shall not apply if the decision is:-</p> <p>(a) necessary for entering into, or performance of, a contract between the data subject and a data controller</p>	<p>The provision specifies an exception to the requirement that decisions significantly affecting a data subject should not be based solely on automated processing. This means that if a decision is necessary for entering into or performing a contract between the data subject and a data controller, it can be based solely on automated processing without violating the law. In other words, in certain contractual situations, automated processing can be used as the sole basis for decision-making.</p>
4.	Legitimate interest	<p>Reg. 25(e) of GN 449C</p> <p>25. The data controller or data processor shall, in implementing the principle of lawfulness during the processing of personal data,</p>	<p>If there's no longer a valid legal reason or a legitimate interest for processing that data, processing should stop. This is to ensure that personal data is only used when there's a clear and valid justification for doing so.</p>

		<p>consider the following important factors:</p> <p>(e) restriction of processing of personal data where the legal basis or legitimate interest ceases to apply</p>	
5.	Vital interests	<p>Sect. 25(2)(f)</p> <p>Where a data controller holds personal data that was collected in connection with a particular purpose, he may use that personal data for other purposes if:</p> <p>(e) the data controller believes on reasonable grounds that use of the personal data for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the data subject or other person, or to public health or safety</p>	<p>The provision allows data controller who initially collected personal data for a specific purpose, to use that data for a different purpose if they have a reasonable belief that doing so is necessary to prevent or mitigate a serious and imminent threat to someone's life or health, or to public health or safety.</p>

Conclusion

The legal bases outlined under the PDPA, encompassing both the main Act and its regulations, establish a robust foundation for the lawful collection and processing of personal data. These provisions not only emphasize transparency, fairness, and accountability but also ensure that data subjects' rights are respected and protected. The law strikes a crucial balance between enabling legitimate data usage and upholding individuals' privacy rights.