ARTICLES
Tanzania's Personal Data Protection Act: A Harbinger for the Realisation of the Right to Privacy?

Frank Mchomvu
Lecturer, Faculty of Law, Mzumbe University
fmchomvu@mzumbe.ac.tz

Abstract
Protecting privacy is critically important, as it is a fundamental part of personal freedom and dignity. In an era marked by increasing digital connectivity, safeguarding this right has become even more crucial. Although Tanzania has enshrined the right to privacy in its Constitution for many years, it did not have a data protection law until 2022. This article examines whether the Personal Data Protection Act (PDPA) effectively promotes the realization of the right to privacy. Using a doctrinal legal research approach, it evaluates the PDPA's effectiveness against internationally recognised data protection standards, with a focus on principles, rights, and limitations. The evaluation reveals that while the PDPA represents a significant advancement in safeguarding the right to privacy, it also has the potential to undermine it. This is because it incorporates fundamental principles and rights related to personal data, alongside vague limitations that could compromise the right to privacy. Consequently, the PDPA appears to grant the right to privacy on one hand, while taking it away with the other. Therefore, this paper recommends amending the PDPA to enhance its role in safeguarding the right to privacy in Tanzania.

Keywords: *Data processing, data protection, personal data, principles of data protection, right to privacy.*

1.0 Introduction

Privacy is not a new concept. According to Rengel, the idea is as old as human civilization.[1] The right to privacy is a fundamental human right, universally recognised as essential to upholding human dignity and promoting individual autonomy. Privacy refers to the establishment of a personal space for individuals, often described as the right to be left

1 A. Rengel, 'Privacy as an International Human Right and The Right to Obscurity in Cyberspace,' *Groningen Journal of International Law*, Volume 2, No. 2, 2014 (33 – 54), p 37.

alone.[2] It is indispensable for the enjoyment of human dignity.[3] Privacy is closely connected with meaningful personal autonomy. As such, its infringement threatens the enjoyment of other rights, such as freedom of movement, association, and religion.[4] Although many states have committed to respecting the right to privacy by ratifying relevant instruments, they sometimes act inconsistently with this right by employing technologies that infringe upon it.[5]

With the advent of the digital age, the need for robust data protection laws has become paramount. In Tanzania, enacting the Personal Data Protection Act (PDPA) marks an essential step in safeguarding personal data and, by extension, the right to privacy. This article explores whether the PDPA effectively contributes to realizing the right to privacy in Tanzania. Following this introduction, the paper examines privacy law at the international, regional, and domestic levels. Subsequently, it provides an overview of the PDPA before analysing whether it signifies an important step towards the realization of the right in question. The article concludes with final thoughts and some suggestions for future directions.

2.0 Legal framework on the right to privacy

This part discusses the law pertaining to privacy. It begins by examining the framework at the global level, followed by the regional level, with a special focus on Africa, and concludes with an analysis of the law in Tanzania.

2.1 International legal framework

A variety of international human rights instruments safeguard the right to privacy, including the International Covenant on Civil and Political Rights (ICCPR) of 1966. ICCPR prohibits arbitrary or unlawful intrusions into a person's privacy, family, home, or correspondence and unauthorized assaults on an individual's reputation.[6] In clarifying the extent of this right, the United Nations (UN) Human Rights Committee emphasizes that privacy must be protected against any unlawful or

2 *Justice K.S. Puttaswamy (Retd.) and another v Union of India and Others* [2018] AIR SC (SUPP) 1841, para 287, p 356.
3 *Ibid*, p 356.
4 See J.A. Cannataci, 'Right to Privacy: Report of the Special Rapporteur on the Right to Privacy,' A/HRC/40/63, 2019, para 4, p 3.
5 *Ibid*, pp 3 & 4.
6 Art, 17 (1).

arbitrary intrusions and assaults by state authorities and legal and natural persons.[7] The term 'unlawful' implies that interference is allowed under certain circumstances as defined by law, but it is still subject to the provisions, aims, and principles of ICCPR.[8]

Arbitrary interference with privacy can include situations where this interference is sanctioned by law.[9] As such, even if interference is legally permitted, it must not violate the essence of the right protected under ICCPR and must always be reasonable in the specific context.[10] It is also noteworthy that even where a law provides for interference that conforms with ICCPR, it must clearly define the situations in which such interference is permitted.[11] This requirement is essential as it aims to prevent abuse of the limitation, thus unjustifiably infringing on the right to privacy.

Protecting the right to privacy also implies that 'integrity and confidentiality' of correspondence must be protected as a matter of law and fact.[12] As such, compliance with Article 17 of ICCPR also requires prohibiting any form of interception of communication and surveillance.[13] For example, if a letter is written by A to B, it should reach A without being opened, read, or intercepted. Furthermore, home search should only be permitted if necessary for evidence collection and if it does not amount to harassment.[14] Also, considering the dignity of the person being searched, it should only be undertaken by persons of the same sex.[15]

Like other human rights, the right to privacy entails a corresponding duty to protect. In this regard, ICCPR requires state parties to establish legal safeguards against unacceptable violations of the right.[16] This includes not only enacting comprehensive data protection laws but also ensuring

7 Human Rights Committee, General Comment 16: The Right to Respect Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, HRI/GEN/1/Rev.1 para 1.
8 *Ibid*, para 3.
9 *Ibid*, para 4.
10 *Ibid*.
11 Human Rights Committee, General Comment 16 (note 7), para 8.
12 *Ibid*, para 8.
13 *Ibid*. See also G. Rona & L. Aarons, 'State Responsibility to Respect, Protect and Fulfil Human Rights Obligations in Cyberspace,' *Journal of National Security Law & Policy*, Volume 8, No. 3, 2016 (503 – 530), pp. 511 – 512.
14 Human Rights Committee, General Comment 16 (note 7), para 8.
15 *Ibid*.
16 Art 17 (2).

that accessible and effective remedies are available for individuals whose privacy rights have been violated.[17] The legal protection of personal privacy is critically important, as breaches can have significant repercussions, including damage to an individual's reputation, emotional distress, and potentially even harm to their personal and professional relationships. Therefore, it is essential for governments to prioritize these safeguards to uphold dignity and integrity in an increasingly interconnected world.

Universal Declaration of Human Rights (UDHR) of 1948 is another international instrument that guarantees the right to privacy. Like ICCPR, UDHR prohibits arbitrary interference with one's privacy, family, home, or correspondence.[18] It also prohibits any attack on a person's honour and reputation and requires states to enact a law protecting individuals' privacy from such attacks.[19]

Other international instruments that guarantee the right to privacy include the Convention on the Rights of the Child (CRC) of 1989 and the International Convention on the Protection of All Migrant Workers and Members of Their Families (Convention on Migrant Workers) of 1990.[20] It is also worth noting that CRC and the Convention on Migrant Workers protect the right to privacy in terms similar to those employed by ICCPR and UDHR.

2.2 The right to privacy under regional human rights frameworks

2.2.1 The African human rights system

Two instruments within the African human rights system explicitly guarantee the right to privacy, namely the African Charter on the Rights and Welfare of the Child (African Children's Charter) of 1990 and the African Union (AU) Convention on Cyber Security and Personal Data Protection (AU Data Protection Convention) of 2014. According to the African Children's Charter, children have the right to privacy in their family life, at home, and in their correspondence.[21] It is essential to underscore that the African Children's Charter generally affords

17 Human Rights Committee, General Comment 16 (note 7), para 11.
18 Art 12.
19 *Ibid*.
20 Art 14.
21 Art 10.

protection similar to that accorded by the UDHR and ICCPR. However, in addition to such protection, it understandably includes a provision allowing parents or guardians to oversee their children's conduct reasonably.[22]

The oversight by parents or guardians is significant because they have a legal obligation to uphold and ensure the development of their children. Given this, it is essential to grant parents and guardians the right to exercise reasonable supervision over their children's conduct. Without this oversight, parents and guardians will likely lose control of their children, failing to effectively discharge their obligation to raise and guide them in the right direction. It is essential to acknowledge that the supervision required in the context of child welfare is not merely a blanket standard, but rather one that must be deemed 'reasonable'. The determination of what constitutes reasonable behaviour can vary based on numerous factors, including the child's age, maturity, and the particular context in which actions are taken. Furthermore, it is crucial to understand that the African Children's Charter does not grant parents or guardians the authority to violate children's rights to privacy. This underscores the importance of respecting children's autonomy and ensuring that their rights are upheld, even while they are under parental or guardian supervision.

Insofar as the AU Data Protection Convention is concerned, the right to privacy is addressed under chapter two of this instrument. In this regard, states commit to establishing a strong legal framework for fundamental rights and freedoms, including penalizing privacy violators while ensuring the free flow of personal data.[23] States are also required to establish a framework that considers the fundamental freedoms and rights of both legal and natural persons.[24]

The AU Data Protection Convention plays a vital role in enhancing data protection across Africa, representing a significant advancement in the ongoing efforts to uphold privacy rights within the regional human rights framework. By establishing clear standards and guidelines, this instrument aims to address the growing concerns surrounding personal

22 Art 20.
23 Art 8 (1).
24 Art 8 (2).

data security, enabling individuals to safeguard their personal information against misuse and unauthorized access. Furthermore, it underscores the commitment of African nations to align with global privacy standards while fostering a culture of respect for human rights in the digital age, ultimately contributing to the protection of personal dignity and autonomy in an increasingly interconnected world.

It is worth noting that the African Charter on Human and Peoples' Rights (African Charter) of 1981, which serves as Africa's primary human rights framework, lacks an explicit provision for the protection of the right to privacy. In this context, Singh and Power argue that the omission of the right to privacy in the African Charter suggests that, prior to the digital age and the subsequent rise in privacy infringements, both online and offline, the internationally recognised right to privacy held minimal, if any, importance within the African human rights system.[25] In this context, Makulilo argues that the concept of privacy is a Western construct that has undergone significant evolution over time.[26]

The absence of a standalone provision in the African Charter for protecting the right to privacy makes it challenging, but not impossible, to protect this right in Africa. As previously mentioned, a link exists between the right to privacy and other fundamental rights. This connection enables the right to privacy to be derived from related rights. Notably, the right to life and human dignity, specifically safeguarded in the African Charter, serves as the primary foundation for inferring the right to privacy.[27] Consequently, one can argue that any unlawful or arbitrary breach of an individual's privacy constitutes a violation of their personal life and integrity. This perspective highlights the fundamental importance of privacy as a crucial component of personal dignity and autonomy within contemporary societal frameworks.[28]

25 A. Singh & M. Power, 'The Privacy Awakening: The Urgent Need to Harmonise the Right to Privacy in Africa,' *African Human Rights Yearbook*, Volume, 3, 2019 (202 – 220), pp. 202-203.
26 A. B. Makulilo, 'Data Privacy in Africa: Taking Stock of its Development after two Decades,' in L. A. Abdulrauf & H. Dube (eds), Data Privacy Law in Africa: Emerging Perspectives, 2024, pp. 41–77, 41. Also, see generally P. Boshe, 'A Quest for an African Concept of Privacy,' in L. A. Abdulrauf & H. Dube (eds.), Data Privacy Law in Africa: Emerging Perspectives (2024), pp. 13–40.
27 See art 4.
28 For more details, see generally A. Mavedzenge, 'The Right to Privacy v National Security in Africa: Towards a Legislative Framework Which Guarantees Proportionality in Communications Surveillance,' *African Journal of Legal Studies*, Volume 12, No. 3-4, 2020 (360-390).

2.1.1 Right to privacy under other regional human rights systems

The right to privacy is also safeguarded in other regional human rights frameworks. For instance, the European Convention on Human Rights of 1950 protects individuals' privacy and prohibits any unjustified interference with this right by public authorities.[29] It states further that the circumstances under which interferences may be allowed must not only be provided by law but also be necessary in a democratic society in the interest of national security, public safety, or economic well-being of a country, or those aimed at preventing crimes, protecting health and morals, or protecting the rights and freedoms of others.[30] The right is also well entrenched in the American Convention on Human Rights of 1969, whose wording is in *pari materia* with that of ICCPR and UDHR.[31] Other instruments at the regional level include the Arab Charter on Human Rights of 2004,[32] and the Human Rights Declaration of the Association of Southeast Asian Nations of 2012.[33]

The presence of various instruments protecting the right to privacy highlights the inherent significance of this fundamental right. This essential protection, recognized by numerous domestic constitutions, aims to empower individuals with control over their personal information and private lives. These measures emphasize privacy as a cornerstone of individual autonomy and dignity. Additionally, they reflect a commitment to personal freedoms while acknowledging the evolving challenges posed by technology and globalization in preserving the sanctity of personal privacy.

3.0 Legal protection of the right to privacy in Tanzania

3.1 Constitutional protection

In Tanzania, the right to privacy is firmly established in the Constitution of the United Republic of Tanzania of 1977, hereinafter referred to as the Constitution. Specifically, the Constitution provides that everyone is entitled to respect and protection regarding their person, the privacy of their person, family, and matrimonial life.[34] The Constitution also

29 Art 8(1).
30 Art 8(2).
31 See art 11.
32 Arts 16 & 21.
33 Art 21.
34 Art 16.

guarantees everyone the right to protect their residence and private communications.[35] To ensure this right is realized, the Constitution requires authorities to establish a legal framework for the circumstances and procedures under which the right to privacy can be interfered without prejudicing it.[36] This right was recently reaffirmed by the High Court of Tanzania, which stated clearly that the Constitution and various key international human rights instruments, including the ICCPR, unequivocally protect it.[37]

3.2 Statutory protection

The central law regulating data protection in Tanzania is the PDPA.[38] Before 2022, the country lacked a specific law on personal data protection, despite the right to privacy having been enshrined in the Constitution for almost four decades. As such, the enactment of the PDPA brought into operation the constitutional provision on the right to privacy.[39] It came into operation in 2023 upon the publication of a government notice by the minister responsible for the matter. The PDPA's enactment and entry into effect marked a remarkable milestone in enforcing the right to privacy and personal security as enshrined in the Constitution. The PDPA is a crucial embodiment of Article 16 of the Constitution, which intensifies its principles and guarantees their practical application.

3.2.1 An overview of the PDPA

The PDPA has 65 sections divided into nine parts. The first part outlines preliminary provisions, including the definition of key terms, objectives, and principles of personal data protection. It has five goals, which include regulating the protection of individuals' privacy, establishing mechanisms for protecting personal data, and providing remedies in the event of a violation.[40] It also enshrines principles that should govern the collection and processing of data.[41] Such principles include ensuring that data is collected and processed for explicit, specified, and legitimate purposes, in accordance with a data subject's rights.

35 *Ibid*.
36 Art 16 (2).
37 See *Tito Magoti v Honourable Attorney General*, miscellaneous civil cause no. 18 of 2023, available at https://tanzlii.org/akn/tz/judgment/tzhc/2024/1939/eng@2024-05-08 (last accessed 12 March 2025).
38 Chapter 44 of the laws of Tanzania.
39 The High Court also acknowledged this fact in Magoti's case (note 37).
40 Sec 4.
41 Sec 5.

The second part establishes the Personal Data Protection Commission (PDPC) as the primary authority responsible for supervising the implementation of the PDPA.[42] The PDPC is mandated, among other things, to ensure compliance with the provisions of the PDPA, handle complaints relating to alleged violations of personal data protection and the privacy of individuals, and investigate and take measures against any matter that it considers affects personal data protection and violates privacy.[43] The PDPC is overseen by a Board established to ensure it performs its functions as required by law.[44] It was officially launched by the President of the United Republic of Tanzania in April 2024.[45] In her address, the President noted that the commencement of the PDPC was a significant milestone for personal data protection and emphasized the importance of strict regulations in this area.[46] Launching the PDPC, the central body responsible for implementing the PDPA, was a significant step toward realising the right to privacy and personal security in Tanzania. The third part sets requirements for the registration of all data controllers and processors[47] as a prerequisite for collecting and processing personal data.[48] In this respect, the PDPC is mandated with the power to administer registration and deregistration of all data controllers and processors.[49] It is an offence for anyone to supply false or misleading information during the registration or renewal application.[50] Any decision the PDPC makes regarding registration can be appealed to the minister responsible for communication.[51]

Part four of the PDPA deals with collecting, using, disclosing, and retaining personal data. In this respect, it sets the threshold requirements for personal data collectors, including the lawfulness of the collection purpose, necessity, and the incidental or direct relationship between the

42 Sec 6 (1).
43 Sec 7.
44 Secs 8 & 9.
45 J. Mosenda, 'Tanzania launches commission to oversee personal data protection,' (4 April 2024) The Citizen (online), available at https://www.thecitizen.co.tz/tanzania/news/national/tanzania-launches-commission-to-oversee-personal-data-protection-4577912, (last accessed 11 April 2025).
46 *Ibid*.
47 A Data controller is anyone who determines the purposes and means of processing personal data, whether in isolation or jointly, and a data processor is anyone authorized to process personal data for and on behalf of the controller, save for those under the direct authority of the controller (See sec 3 of the PDPA).
48 Sec 14.
49 Secs 14, 15 & 18.
50 Sec 19.
51 Sec 20.

data collected and the lawful purpose.[52] Additionally, it prohibits the collection of data through unlawful means.[53] It also requires the data collector to comply with specific procedures before collecting any data and provides exceptions under which these procedures may be waived.[54] It also imposes certain restrictions on a data collector who has obtained data from a data subject. These restrictions include using collected data for the intended purpose and restrictions on disclosure.[55]

Part five contains provisions on transboundary data flow. In this regard, the PDPA empowers the PDPC to restrain data transfer from Tanzania to another country.[56] Generally, the PDPA permits data transfer to a country with an adequate legal framework for data protection, provided two conditions are met.[57] The first condition is that the data recipient must demonstrate that the requested data is essential for carrying out a task that serves the public interest or fulfils a lawful function of the data collector.[58] The second condition is that the recipient must establish the necessity of the data transfer, provided there are no grounds to believe that such transfer or data processing could be detrimental to the data subject.[59] It is worth noting that the PDPA also allows the transfer of personal data to a jurisdiction without an effective data protection law as long as an undertaking is made to ensure the protection of such data and its processing by the authorized controller.[60] The law provides for factors to be considered in determining the adequacy level of the protection to be afforded by the data recipient, including the country in question, the nature of the personal data, and the prevailing circumstances surrounding the transfer.[61] Furthermore, the PDPA empowers the respective minister, in consultation with the PDPC, to enact regulations specifying situations under which the transfer of personal data is not allowed.[62]

52 Sec 22 (2) (a) & (b).
53 Sec 22 (3).
54 Sec 23.
55 Secs 25 & 26.
56 Sec 31 (1).
57 Sec 31 (2).
58 Sec 31 (2) (a).
59 Sec 31 (2) (b).
60 Sec 32 (1).
61 Sec 32 (2) (a-f).
62 Sec 32 (3).

Consequently, the Personal Data Protection (Personal Data Collection and Processing) Regulations were promulgated, providing procedures for transferring data outside the jurisdiction, among other things.[63] It is interesting to note that the Regulations in question impose additional conditions for the transfer of data outside the country and empower the PDPC to refuse an application for data transfer where certain conditions are not met, including where it is not satisfied that there is adequate protection in the recipient country and on any other ground it deems fit for public interest.[64] When submitting an application for personal data transfer, the applicant must satisfy the PDPC that the recipient country has ratified an international instrument relating to personal data protection, that an agreement on personal data protection exists between Tanzania and a recipient country, or that a contractual agreement exists between the person requesting such data and the recipient of such data outside the country.[65]

Part six enshrines the rights of data subjects. It should be noted that the PDPA guarantees data subjects' rights to access, rectify, cancel, or oppose the processing of personal data, commonly referred to as the ARCO rights of data subjects.[66] In this vein, it, for example, gives data subjects the right to be informed about access to personal data, the right to be informed about the purpose for accessing personal data, the right to know recipients of accessed personal data, and the right to prevent access to personal data where such access might be injurious to the data subject.[67]

Furthermore, the PDPA explicitly states that the data subject can request the PDPC to delete personal data if it is inaccurate, known as the right to erasure. The right to have personal data protected, including the right to erasure, was upheld by the Court of Justice of the European Union, which, among other things, held that even search engine operators have

63 Government Notice No. 449c, published on 4 July 2023. See Regulations 20, 21, and 22.
64 Reg 22.
65 Sec 20 (3) (a-c).
66 See A. J. Carrillo & M. Jackson, 'Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America, *Vienna Journal on International Constitutional Law*, Volume 16, No. 177, 2022, p. 194 available at https://www.degruyter.com/document/doi/10.1515/icl-2021-0037/html, (last accessed 30 April 2025). See also D. J. Solove, 'The limitations of Privacy Rights,' *Notre Dame Law Review*, Volume 98, No. 3, 2023 (975 – 1036), p. 981.
67 For more on the rights, see Secs 33, 34, 35, 36, 37 and 38.

an obligation to comply with personal data protection requirements.[68] In this case, Mr Costeja González filed a complaint with the Spanish Data Protection Authority (AEPD), demanding the erasure of his personal information from a newspaper available online that was published in 1998. He also sought an order against Google Spain and Google Inc. for the removal or cancellation of his data from the search engine, so that it would not be included in the search results. While the complaint against the publisher of the information in the newspaper was dismissed on the grounds that the publication was legally justifiable, the complaint against Google was successful. Being discontented, Google challenged the decision before the Spanish High Court. The High Court sought a preliminary ruling from the Court of Justice of the European Union regarding the proper interpretation of the issue in the light of the European data protection rules. The Court, among other things, noted that personal data that was lawfully processed might later become unnecessary in the light of the purpose for which they were collected. In such a situation, the personal data in question should be erased from search results upon request by the data subject. This is what is referred to as the right to be forgotten. Although the decision has received several criticisms, it laid a critical foundation for the right to privacy.

It is also worth noting that the PDPA provides for the right to compensation in the event of damage incurred by a data subject due to a contravention of the law while accessing personal data.[69] Upon reviewing the provisions of the Act, it cannot be overstated that the rights enshrined in it align with the minimum threshold internationally accepted in terms of personal data protection, including the European Union (EU) General Data Protection Regulation, 2016 (GDPR).

The seventh part of the PDPA enshrines provisions on investigating complaints made to the PDPC regarding personal data violations. In this context, the PDPC holds the authority to launch investigations into suspected violations proactively whenever necessary.[70] When an investigation is deemed necessary, the PDPC is required to complete it within 90 days of receiving a complaint.[71] Considering the prevailing

68 *Google Spain SL & Google Inc. v Agencia Española de Protecccíón de Datos* (*AEPD) & Mario Costeja González,* Case C-131/12, 13 May 2014, ECLI:EU:C:2014:317.
69 Sec 50.
70 Sec 39 (2).
71 Sec 39 (3).

circumstances, the law permits an extension of up to 90 additional days.[72] This provision underscores the flexibility and understanding inherent in the legal framework, ensuring that all parties have the opportunity to navigate challenges effectively.

Furthermore, the PDPA makes it an offence to act in a way that obstructs the PDPC from carrying out its mandated functions.[73] The crimes include providing false or misleading information and obstructing the PDPC from exercising its powers.[74] In addition to offences, the PDPA empowers the PDPC to take administrative actions when it discovers violations. In this regard, it may issue an enforcement notice requiring correction of the breach, and if not complied with, it may impose penalties on the violator.[75] It is also allowed to order compensation for a person affected by a violation.[76] It is worth noting that the PDPC is empowered to review its decisions on its own initiative or upon application by an aggrieved person.[77] The application for review is made in a prescribed manner and must be made within 21 days.[78] The decision on the review application must be rendered within 14 days of receipt.[79]

The PDPA also establishes the crucial right to appeal to the High Court for individuals dissatisfied with the PDPC's decisions.[80] Like the application for review, the appeal should be lodged within 21 days of the decision.[81]This right of appeal serves as a fundamental safeguard, providing a structured and authoritative channel for individuals to seek justice and redress when they believe the PDPA has not adequately handled a complaint. By allowing for an oversight mechanism through the High Court, the PDPA promotes transparency and accountability within the PDPC's operations, empowering individuals to challenge decisions that may adversely affect their rights.

72 Sec 39 (4).
73 Sec 43.
74 Sec 43.
75 Sec 45, 46 & 47.
76 Sec 50.
77 Sec 48.
78 Reg 25 (1), Personal Data Protection (Complaints Settlement Procedures) Regulations, Government Notice No. 449B published on 4/7/2023.
79 *Ibid*, Reg. 25 (2).
80 Sec 49.
81 Re 26 of the Personal Data Protection (Complaints Settlement Procedures) Regulations.

Part eight includes provisions regarding finances. This section outlines, among other things, the sources of PDPC's funding, financial management practices, budget preparations, expenditures, and account auditing. The last part contains miscellaneous provisions. These provisions include exceptions under which personal data may be accessed without compliance with the PDPA. These exceptions include processing data for the data subject's personal use, where such access is necessary for national security, public interest, or the prevention of crimes, and where such access is required by law or a court order.[82] In addition to the exceptions stipulated expressly under the law, the respective minister can also prescribe other circumstances where compliance with the PDPA may be dispensed with.[83]

Apart from providing for exceptions, this part also establishes several offences concerning the breach of provisions of the PDPA. For instance, it is an offence for a data processor or controller to make an unlawful disclosure of personal data.[84] It is also an offence for any person to have unauthorized access to personal data kept by the data controller or processor, or for any person to offer for sale personal data unlawfully.[85] Interestingly, in instances where a company or corporation commits an offence, such a company and any of its officers who knowingly and intentionally are involved in committing the offence are held liable.[86] The law also requires any data controller to adopt a code of ethics or policy to govern the collection and processing of personal data.[87] The requirement to enact a code of ethics is also recognized under GDPR.[88]

3.2.2 How far does the PDPA promote the right to privacy in Tanzania?

It has already been indicated that the right to privacy is a fundamental human right enshrined in the Constitution of Tanzania and various international human rights instruments. A comprehensive guarantee of the right to privacy is essential for the enjoyment of both online and

82 Sec 58.
83 Sec 58(3).
84 Sec 60(1) & (2)
85 Sec 60(3) (4).
86 Sec 62.
87 Sec 65.
88 See Art 40.

offline human rights. Additionally, this right significantly impacts the exercise of other
rights, including freedom of expression, assembly, and association. Consequently, violations of the right to privacy can hinder the enjoyment of these related rights, exacerbating issues of inequality and discrimination, among others.

However, since the right to privacy includes the right not to have one's personal data unlawfully revealed, a robust data protection legal framework is indispensable. In this regard, Solove argues that the right to privacy is fundamental to information privacy and data protection laws.[89] No wonder, for many years, the realization of the right to privacy in Tanzania remained a distant goal owing to the absence of statutory law on personal data protection.[90] That is why this paper contends that the enactment and implementation of the PDPA represent a significant step forward in fully realizing the right to privacy.

> This section evaluates how effectively the PDPA upholds the right to privacy within the country. This analysis examines the PDPA's key provisions, including those that establish principles and those that limit the right to privacy, to assess their alignment with internationally recognised standards and principles of data protection. By doing so, it can determine whether the PDPA fosters a robust framework for privacy protection that resonates with global norms.

3.2.2.1 Data Protection principles under the PDPA

This paper finds it pertinent to briefly underscore the key principles of personal data protection law to determine whether the PDPA supports the right to privacy. These principles are outlined in the EU GDPR, among other instruments. Although this instrument is not legally binding on Tanzania, it has exerted a significant influence on data protection worldwide. Even the High Court of Tanzania, in its decision on Tito Magoti's case, referred to the GDPR in relation to the international data protection regime.

89 D.J. Solove, 'The limitations of privacy rights,' (note 66), p. 977.
90 See U. John, 'Privacy-a Forgotten Right in Tanzania,' *Tanzania Lawyer*, Volume 1, No. 2, 2012, (72-114), pp 24 – 25.

The GDPR sets out seven fundamental principles to govern data processing. **[91]** The principles are lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.[92] Lawfulness, fairness, and transparency require that the processing of personal data be conducted under a legal basis.**[93]** The fairness principle requires that personal data be processed fairly and not in a manner that is detrimental, misleading, or deceptive.[94] Transparency means that personal data should be processed in a clear and transparent manner.[95] Transparency also implies that data subjects should be informed about the processing of their data in a concise, easily accessible, and understandable manner.[96]

The principle of purpose limitation implies that the data processor must be clear about the purpose for collecting data from the outset and that the data must be used for that particular purpose.[97] Using data for any new purpose is only acceptable if it is in line with the original purpose, with the data subject's consent, or as required by law.[98] This requirement ensures transparency regarding the motives for collecting personal data and guarantees that its usage aligns with the reasonable expectations of the individuals involved.[99]

The data minimisation principle entails indicating the minimum amount of personal data needed to fulfil the processor's purpose and only holding such information.[100] This means the data processor cannot hold more data than is needed to achieve the intended purpose. For instance, if a company collects personal information relating to a particular creditor and gathers information on many creditors with similar names, but later it is

91 Art 5.
92See Data Protection Commission, "Quick Guide to the Principles of Data Protection" available at https://www.dataprotection.ie/sites/default/files/uploads/201911/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf (last accessed 29 April 20205).
93 *Ibid* p 2.
94 *Ibid*.
95 *Ibid*.
96 *Ibid*.
97 Information Commissioner's Office (ICO) (United Kingdom), 'Principle (b): Purpose limitation' available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the data-protection-principles/purpose-limitation/, (last accessed 30 April 2025).
98 *Ibid*.
99 *Ibid*.
100 ICO., 'Principle (c): Data Minimisation,' available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/ (last accessed 30 April 2025).

noted that other individuals are not connected to the debt, it is not supposed to process such information; instead, it should be deleted. Dealing with other irrelevant details would amount to processing excessive information, thereby contravening the principle of data minimisation.

The principle of data accuracy requires that personal data be accurate and, where appropriate, be kept up to date.[101] It also entails that personal data should not be incorrect or misleading. To avoid inaccuracy, the data processors must be transparent about what personal data they intend to share.[102] For example, if a person has moved from Mbeya to Dar es Salaam, it is inaccurate to say that they currently reside in Mbeya, but accurate to say that they once lived in Mbeya.

The storage limitation principle states that personal data should not be stored for an unnecessary period unless for a legitimate, specific, and explicit purpose.[103] This means that personal data should not be kept longer than necessary, even if such data was collected lawfully and for a legitimate purpose. The essence of this principle is to ensure that personal data that is no longer needed can be either erased or anonymized to prevent it from becoming outdated, which can lead to irrelevance, excessiveness, or even inaccuracy.[104]

The principle of integrity and confidentiality, also known as the security principle, entails establishing robust mechanisms to safeguard personal data from various threats.[105] This includes unlawful or unauthorized access, processing, and dissemination, as well as the risks of accidental damage, data loss, and other vulnerabilities associated with handling

101 Office of the Data Protection Commissioner (Kenya), 'Personal Data Protection Handbook,' p 6, available at https://www.odpc.go.ke/wp-content/uploads/2024/02/PERSONAL-DATA-PROTECTION-HANDBOOK.pdf (last accessed 30 April 2025).
102 ICO, 'Principle (d): Accuracy.' available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/accuracy/ (last accessed 30 April 2025).
103 UN High-Level Committee on Management, 'Personal Data Protection and Privacy Principles,' available at https://indico.un.org/event/1013308/attachments/17363/50495/UN%20Principles%20on%20Personal%20Data%20Protection%20Privacy.pdf (last accessed 30 April 2025).
104 ICO, "Principle (e): Storage limitation". Available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/storage-limitation/ (last accessed 30 April 2025).
105 UN High-Level Committee on Management, (note 103).

personal data. To uphold this principle, organizations must implement stringent access controls, encryption techniques, and regular audits to ensure data remains protected throughout its lifecycle.[106] Additionally, comprehensive training for personnel on data protection protocols is crucial to cultivate a culture of security awareness, thereby minimizing the potential for human error and enhancing the overall resilience against various data processing risks.[107]

Lastly, the principle of accountability necessitates the establishment of robust mechanisms designed to guarantee compliance with the previously outlined principles of personal data protection. This principle calls upon those individuals and organizations responsible for managing personal data to take full ownership and responsibility for their actions. This includes adhering to relevant legal frameworks and regulations, as well as ensuring transparent practices that uphold the integrity of personal data throughout its lifecycle. Accountability also involves implementing comprehensive policies and procedures that promote responsible data handling, conducting regular audits to assess conformity with data protection standards, and fostering a culture of employee awareness and responsibility. Additionally, this principle emphasizes the importance of timely reporting and addressing any data breaches or violations, ensuring stakeholders can trust that their personal information is safeguarded per established data protection norms.

As hinted above, the data protection principles are also outlined under the PDPA.[108] For example, regarding the principles of lawfulness, fairness, and transparency, it categorically obliges data controllers and processors to ensure that personal data is collected lawfully, fairly, and transparently.[109] The paper argues that the PDPA aligns with international principles and standards for personal data protection. This alignment marks a significant step forward in safeguarding the right to privacy, which is firmly established under the country's Constitution. The PDPA underscores the commitment to protecting individuals' personal information from misuse by adhering to these standards. This proactive approach demonstrates Tanzania's commitment to upholding human

106 *Ibid*.
107 *Ibid*.
108 See Sect 5.
109 Sect 5 (a).

rights and refining the legal framework surrounding privacy in the digital age.

3.2.2.2 Rights of data subjects under the PDPA

As underscored above, the PDPA enshrines several rights to which a data subject is entitled.[110] The fundamental rights associated with personal data protection include the right of access, which enables individuals to request access to the data being processed. Additionally, there is the right to prevent processing that could adversely affect the data subject. This is crucial in enabling individuals to halt activities that may lead to negative consequences in their personal or professional lives.

Another significant right is the right to restrict processing for direct marketing purposes, which enables individuals to opt out of having their data used in marketing campaigns or promotional activities without their explicit consent. Also, there is the right to rectification, which empowers data subjects to request corrections to any inaccurate or incomplete personal data, thereby safeguarding the accuracy of the information. Moreover, the PDPA incorporates the right to erasure, which allows individuals to request the deletion of their data under specific circumstances, such as when the data is no longer necessary for the purposes for which it was collected or if the individual withdraws consent.

Various personal data protection laws, such as the GDPR, enshrine these rights across jurisdictions. The rights seek to ensure that the processing of personal data is conducted in a manner that respects and upholds the fundamental rights of data subjects, particularly their right to privacy. By delineating these rights, the PDPA safeguards individuals against the misuse of their personal information and promotes greater transparency and accountability in data processing practices. Like the data protection principles, these rights are also fundamental in protecting individuals' right to privacy.

3.2.2.3 Restrictions on data subject rights under the PDPA

Like many other human rights, the right to privacy is not absolute. International human rights law acknowledges that this right may be

110 See Part VI.

restricted under specific conditions. However, unlike other provisions within ICCPR, Article 17 does not explicitly outline circumstances under which the right to privacy can be limited. However, as explained above, any limitations on this right must comply with the standards established by international human rights law.

It is also important to highlight that the provisions regarding the right to privacy discussed previously do not specify detailed exceptions under which this right may be limited. As noted earlier, the Human Rights Committee has clarified the scope of this right through its General Comment 16. In this context, it has been emphasized that unlawful interference does not merely encompass the prohibition of any form of interference not authorized by law; the law itself must also align with the provisions, aims, and objectives of ICCPR. Furthermore, even when the law permits interference, it may still be considered arbitrary if it contradicts the spirit of ICCPR.

In one of its resolutions, the Human Rights Council reiterated that any measures to limit the right to private life must comply with the principles of legality, necessity, and proportionality.[111] The principle of legality implies that any limitation to the right to privacy must be stipulated in law. The law must be sufficiently accessible, clear, and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances.[112] Insofar as necessity and proportionality principles are concerned, they require that the limitation of the right to privacy must not only be necessary for reaching a legitimate purpose but also be proportional to the purpose to be attained.[113]

111 Human Rights Council, 'the Right to Privacy in the Digital Age,' Resolution adopted by Human Rights Council on 26 September 2019, A/HRC/RES/42/15. The applicability of these principles in testing the validity of limitations to the right to privacy was also acknowledged by the High Court of Tanzania in Magoti's case (note 37).

112 Office of the United Nations High Commissioner for Human Rights (OHCHR), "The right to Privacy in the Digital Age," Report of OHCHR, para 23.

113 Human Rights Committee, General Comment No. 31 [80], 'The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add. 13, para 6. See also A. Rengel, 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace,' (note 1), pp. 40 – 41; *Media Council of Tanzania, Legal and Human Rights Centre & Tanzania Human Rights Defenders Coalition v the Attorney General of the United Republic of Tanzania,* EACJ, reference no. 2 of 2017, para 60.

The Court of Appeal of Tanzania also alluded to the issue of appropriate rights limitation in *Julius Ishengoma Francis Ndyanabo v the Attorney General*.[114] In this case, the Court stated that any limitations of fundamental rights should not be arbitrary, unreasonable, or disproportionate.[115] As far as the right to privacy is concerned, it implies that any measure to limit the right must ensure that, apart from enacting a law to that effect, the limitation is justified by a legitimate aim, such as national security or public interest. The extent of the interference must also be commensurate with the purpose to be achieved.

The PDPA contains specific provisions that limit the right to privacy, a limitation not uncommon in many data protection laws. To determine whether the limitations contained therein align with international human rights law, one needs to assess the exceptions in light of the principles elucidated above. The PDPA provides seven instances under which personal data may be accessed and processed without compliance with the procedures outlined under the law.[116] These instances are: first; where the data subject does the processing for his/her personal use, second; where the processing is done in compliance with any law or court order, third; where the processing upholds national safety and security and public interest, fourth; where the processing aims at preventing or detecting crimes, fifth; where the processing aims at addressing the question of tax evasion, sixth; where the processing aims at investigation of misappropriation of public funds and lastly; where the processing aims at vetting for appointment to any public service position.

Upon careful examination of the above outlined restrictions, it becomes evident that most of them serve a legitimate and significant purpose within the framework of data protection. For instance, the allowance for the processing of personal data without adhering to established legal procedures when such processing is aimed at combating criminal activities represents a crucial objective aligned with public safety and welfare. These exceptions are designed to thwart unscrupulous individuals or entities from exploiting the law on personal data protection to evade taxes, perpetrate fraud, engage in other illicit activities, or

114 Civil Appeal No. 64 of 2021, Court of Appeal of Tanzania at Dar es Salaam, available at https://media.tanzlii.org/media/judgment/260483/source_file/julius-ishengoma-francis-ndyanabo-vs-the-attorney-general-2002-tzca-14-14-february-2002.pdf, (last accessed 13 April 2025).
115 *Ibid* p 127.
116 Sec 58

otherwise undermine public interests. They are not arbitrary; instead, they seek to strike a balance between safeguarding the individual right to privacy and ensuring the stability and security of society as a whole. The Indian Personal Data Protection Law, for example, explicitly provides for these types of exceptions, recognizing that there are circumstances in which the greater good necessitates a temporary relaxation of data protection norms.[117]

Despite including provisions that legitimately limit the right under study, the PDPA includes a concerning provision that ties the right to personal data protection to adherence to any existing law. This broad exception creates an environment that may facilitate the abuse of the right to privacy. The term 'any law' is quite vague, which raises important questions about whether it must align with the right to privacy. For instance, what if a law permits data processing without complying with the PDPA and disregards the right to personal data protection that is integral to privacy rights?

It is now broadly accepted that any restrictions on fundamental human rights should satisfy three key criteria: lawfulness, necessity, and proportionality. In this connection, the Supreme Court of India noted that any law infringing the right to privacy must withstand the touchstone of permissible restrictions on fundamental rights.[118] While it may be contended that this exception serves a legitimate purpose, its broad scope may be detrimental to the enjoyment of the fundamental right to privacy. In this regard, the Indian Supreme Court remarked that:

The whole object of guaranteed fundamental rights is to make those basic aspects of human freedom, embodied in fundamental rights, more secure than others not so selected. In thus recognizing and declaring certain basic aspects of rights as fundamental by the Constitution of the country, the purpose was to protect them against undue encroachments upon them by the legislative, or executive, and, sometimes even judicial for example Article 20) organs of the State. The encroachment must remain within permissible limits and must take place only in prescribed modes.[119]

117 Digital Personal Data Protection Act, No. 22 of 2023, See sec 17.
118 Justice K.S. Puttaswamy's case (note 2), para H, p 264.
119 *ADM Jabalpur v Shivakant Shukla* [1976] 2 SCC 521 para 183.

Furthermore, it is essential to recognize that even when the government enacts legislation driven by noble intentions, the legitimacy of such laws cannot be evaluated solely on their stated objectives or underlying motivations. Instead, a comprehensive assessment must take into account the tangible effects these laws have on the realization and enjoyment of fundamental rights. This involves examining both the direct and indirect consequences of the legislation on individuals' freedoms, access to justice, and overall well-being, thereby ensuring that the law promotes, rather than infringes upon, the core principles of human dignity and equality.

Given how the above limitation provision is couched, it can be effectively argued that it fails to meet the three-stage test. Moreover, the section mentions 'any law' without regard to its implications for the right to privacy. The provision could have been deemed legitimate had it been formulated with consideration for the necessity of upholding the right to privacy. To illustrate this point, one can refer to the provisions of the GDPR, which also permit the enactment of laws that may infringe upon the right to privacy. This is articulated in the following terms:

> …[p]rocessing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[120]

Unlike the provision under the Tanzanian law, the above provision contains adequate safeguards to ensure it does not become subject to abuse. While the provision allows Member States to enact legislation that permits the processing of personal data without adhering to the principles enunciated in the GDPR, it obliges them to establish a law that meets the principles of legality, necessity, and proportionality. In this regard, it states categorically that such a law should not only be proportional to its objective, but also consider the essence of the right to privacy. Additionally, such a law requires appropriate mechanisms to ensure that the data subject's fundamental rights and interests are respected. These safeguards are essential as they seek to ensure that states do not use this

120 Art 9 (2) (d).

exception to trample upon an individual's right to privacy. The safeguards not only impose upon states the obligation to ensure exceptions are provided by law, but also ensure that such law does not negatively affect the essence of the right to privacy by listing requirements to be complied with.[121]

Along with GDPR provisions, South African data protection law specifies certain limitations that are clearly and justifiably outlined. In this context, it allows personal data to be processed without full compliance, as long as it is done in accordance with relevant provisions of the law protecting personal information.[122] It is important to emphasize that although this law authorizes the regulator to identify situations where personal data may be processed without following standard procedures, it also restricts such powers.[123] The Regulator must consider various factors when granting these exemptions, including public interests and scenarios that may benefit the public. Unlike provisions in Tanzania's PDPA, which provide an open limit on the right to personal data protection, the South African legal framework sets safeguards to prevent abuses that could undermine the fundamental right to privacy.

Additionally, Botswana's Data Protection Act stands out as a robust framework for safeguarding personal data while imposing essential limitations to balance individual rights and societal interests. This legislation explicitly stipulates that any law restricting rights and obligations related to personal data processing must be harmonized with the fundamental rights and freedoms recognised in a democratic society.[124] Furthermore, the Act stipulates that such restrictions must be both necessary and proportionate, ensuring that any limitations imposed are justified within the context of legitimate objectives.[125] These objectives include the protection of national security, the maintenance of public order and defence, as well as the advancement of the public interest and other specified categories that require careful

123 G.G. Fuster, 'Study on the Essence of the Fundamental Rights to Privacy and to Protection of Personal Data, (December 2022), pp 36 & 37, available at https://www.edps.europa.eu/system/files/2023-11/edps-vub study_on_the_essence_of_fundamental_rights_to_privacy_and_to_protection_of_personal_data_en.pdf (last accessed 13 September 2024).
122 The Protection of Personal Information Act, No. 4 of 2013, sec 36.
123 *Ibid*., sec 37.
124 The Data Protection Act, No. 18 of 2024, sec 50 (2).
125 *Ibid*.

consideration.[126] This careful delineation of limits not only reinforces the protection of individual privacy but also recognizes the need for certain exceptions that align with the overarching goals of societal welfare and safety. The Act's emphasis on necessity and proportionality serves to uphold democratic values while enabling the responsible management of personal data in various contexts.

Another concerning aspect of the PDPA is the provision that empowers the relevant minister to impose additional restrictions on the handling of personal data unilaterally. This clause signifies a considerable and far-reaching discretionary authority vested in the minister, which is strikingly devoid of clear guidelines or criteria regarding the rationale for these potential exemptions. There is a lack of clarity not only about the specific categories of personal data that may be subject to such exemptions but also regarding the duration for which these exemptions might remain in effect. This absence of defined parameters raises significant concerns about the potential for misuse of power and the implications it poses on the right to privacy. Without a transparent framework governing these restrictions, there is a risk of arbitrary decision-making that could undermine the fundamental principles of data protection.

This paper contends that the limitation clauses found in sections 58(2)(b) and 58(3) of the PDPA can significantly compromise the right to privacy. These provisions permit the enactment of laws that may overlook the right to privacy, effectively justifying unlawful intrusions that weaken the protections afforded to data subjects under both the Constitution and the PDPA. It can be argued that these clauses undermine the core principles and rights under the PDPA by allowing unjustifiable infringements on the rights it seeks to protect. In essence, while the PDPA grants specific rights, it also facilitates their infringement. The Court of Justice of the European Union has emphasized the necessity of considering the essence of a right when imposing limitations, acknowledging that while fundamental rights may be subject to restriction, such limitations must not distort the very nature of those rights.[127]

126 *Ibid*.
127 *Hubert Wachauf v Bundesamt für Ernährung und Forstwirtschaft* Case 5/88 ECLI:EU:C: 1989:321, para 18.

It is worth underscoring that the validity of some provisions of the PDPA was, for the first time, put to the test by a human rights activist, Tito Magoti who filed a constitutional petition before the High Court of Tanzania challenging the constitutionality of sections 8 (1)(2)(3), 11(1), 14(5), 19, 20, 22 (3), 23(3)(c) (d)(e), 25(2)(e)(f), 26, 30(5), 31(2), 33(2) and 34.[128] In his petition, he contended that Sections 8(1), (2), and (3), which empower the President to appoint the chairperson and vice chairperson of the PDPC without specifying the required qualifications, violate the rights to equality and privacy, among others. The petitioner also argued that Section 11(1), which provides for the appointment of the General Director of the PDPC without a transparent procedure, infringes the rights to equality and privacy, among others. In addition, the petitioner alleged that section 14(5) which requires the PDPC to notify in writing and with reasons a data controller or processor whose application for registration has been refused, is against the constitutional right to fair trial and the right to be heard as it does not specify time within which an application should be rejected or registered as well as the time within which the applicant should be informed about rejection if any.

The other issue raised by the petitioner against the Act was that Section 19, which establishes offences relating to registration, such as furnishing false information, is unconstitutional for lacking *mens rea*. Equally, Section 20, which provides for an appeal to the minister was challenged because the PDPC falls under the ministry, as well as the fact that it does not provide an appeal procedure. Section 22(3), which prohibits a data controller from unlawfully collecting personal data, was also criticized for lacking clarity. Another provision that was challenged is section 23(3)(c), (d), and (e), which provide exceptions to the principle that personal data must be collected from the data subject, arguing that they are broader and more ambiguous.

The petitioner also challenged the provisions of sections 25(e) and (f), which allow a data controller to utilise data for purposes other than those intended, as violating the right to privacy. Furthermore, Section 26 was also impugned on the ground that it allows disclosure of personal data without any specific procedures. The provision of section 30(5), which allows for exceptions under which sensitive personal data may be processed, was also challenged for being overly broad, ambiguous, and

128 See Magoti's case (Note 37).

lacking prescribed procedures. Similar grounds were maintained against the provision of Section 33(2). Lastly, the petitioner alleged that Section 34(2), which permits the processing of harmful information, is couched in broader, ambiguous, and unclear terms, thereby infringing the right to privacy. Consequently, the petitioner requested that the Court declare the above provisions unconstitutional for violating the rights to equality and privacy, as well as personal security, among others, and expunge them from the PDPA.

In its detailed judgement rendered by the full bench on May 2024, the High Court only agreed with the petitioner in respect of sections 22(3) and 23(3)(c) & (e). In respect of section 22(3), the Court generally agreed with the petitioner that the provision is vague. In this regard, the Court noted that the section should have provided the so-called 'unlawful means' of collecting data, irrespective of the fact that the law cuts across all sectors, as well as changes in science and technology. The Court further argued that the provision is unclear, as it does not explain the implications of unlawful data processing, and therefore, it is open to abuse.[129]

Insofar as section 23(3)(c) & (e) is concerned, the Court also agreed with the petitioner's submissions that they are vague as they do not stipulate circumstances under which obtaining consent is impracticable or where such consent might prejudice the lawful purpose of data collection. The Court believed that the PDPA should have envisaged situations where obtaining consent would be impractical, as well as the so-called lawful purposes that might be prejudiced if the data subject were informed about the processing of their data. As such, the Court held that these exceptions fell short of the criteria for determining appropriateness of limitations to fundamental rights.[130] Consequently, the Court declared the provisions to be violative of the right to privacy and directed the government to amend them within a year; failure to do so will render them liable to be struck out from the PDPA. For the remaining impugned provisions, the Court declined to agree with the petitioner that they violate the Constitution.

It is essential to note, albeit briefly, that more than a year has passed since the High Court rendered its decision in Tito Magoti's case. However, the

129 See pp 17 &18 of the judgement.
130 See pp 20 & 21.

PDPA remains unamended, failing to adhere to the Court's directives. It is highly concerning that this delay undermines the rule of law and the integrity of judicial authority. It is anticipated that the government will soon take action to introduce the necessary amendments to the PDPA, in alignment with the Court's decision. A continued failure to implement these changes would not only reflect poorly on the government but could also be perceived as a blatant disregard for the judiciary, an unsettling prospect for a democratic society that champions the protection of fundamental human rights. Amending the PDPA in line with the High Court's decision would reinforce the government of Tanzania's commitment to upholding the principles of justice and accountability.

Based on the detailed analysis presented in this section, this paper takes the position that the of Tito Magoti, reveal a troubling lack of clarity and precision in their formulation. Moreover, the general limitation under the PDPA falls short of adhering to established international standards that govern the restriction of fundamental rights. This raises critical concerns about the efficacy of the PDPA in safeguarding individual privacy and highlights the necessity for a more robust framework that aligns with global best practices in human rights protection. The Court's decision in Tito Magoti's case underscores the urgent need for revisions to the PDPA to ensure that it does not inadvertently compromise the very right it aims to protect.

4.0 Conclusion and Way Forward

It cannot be denied that the enactment of the PDPA marks a significant milestone in Tanzania's legal framework for protecting the right to privacy. This legislation incorporates many essential principles and rights that align with international data protection standards, signaling a transformative era for privacy safeguarding in Tanzania, especially in our increasingly digital landscape. Notably, the PDPA introduces measures aimed at enhancing the right to privacy, including stipulating the necessity for consent before processing personal data and granting individuals the right to access their data. These provisions represent a significant step towards aligning Tanzania with global standards for personal data protection. They also demonstrate a commitment to safeguarding the right to privacy in an era when personal information is increasingly vulnerable to misuse and exploitation.

However, it is crucial also to underscore that the PDPA contains provisions that impose questionable restrictions on the fundamental right to privacy. These limitations, as previously articulated, create a precarious environment in which authorities may encroach upon personal data, thereby jeopardizing individuals' right to privacy and ultimately undermining the realization of this constitutionally protected right. This problematic scenario inherent in the PDPA poses a significant threat to the already vulnerable right to privacy in the context of increasing digitalization. Consequently, this paper asserts that the PDPA simultaneously confers the right to privacy while significantly undermining it. This duality could ultimately compromise, rather than enhance, the actual realization of the right to privacy within the country.

As a way forward, the PDPA should be amended in line with the High Court's decision in Tito Magoti's case. Furthermore, the PDPA should include a limitation clause that complies with internationally recognized standards for restricting fundamental rights. Additionally, to ensure the practical realization of the right to privacy in Tanzania, simply enacting a proper law will not suffice. Therefore, it is vital to have a strong political will that will ultimately lead to the effective implementation of the PDPA. To this end, empowering the PDPC with the necessary resources and authority to enforce the law effectively, as well as conducting public awareness campaigns to inform individuals and organisations of their rights and responsibilities under the PDPA, can play a pivotal role. Moreover, regular reviews and updates of the PDPA are necessary to address emerging challenges and incorporate best practices from around the world. By taking these steps, Tanzania can genuinely uphold and reinforce the right to privacy for all.

PDPA imposes significant limitations that have the potential to undermine the right to privacy substantially. These limitations, as also exemplified by the High Court's decision in the case
.