



Data privacy and security in E-health: African and European perspectives

The example of post data protection legislation in Tanzania

Alex Makulilo · Doreen Mwamlangala · Rindstone Ezekiel ·
Benedikt Buchner · Elena März · Merle Freye

Accepted: 11 February 2025

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2025

Abstract The regulation of personal health data poses many challenges across different jurisdictions. This article offers analysis of legal framework in the field of E-health sector from the personal data protection point of view. African and European perspectives of data privacy and security are considered through an illustration of the Tanzania's post data protection legislation and practice.

Keywords Personal health data · Privacy · Security · E-health · Tanzania

1 Introduction

The pace of global breakthroughs in health information technology is rapidly increasing. In the era of digital health, an increasing number of hospitals and health-care institutions are adopting information and communication technologies (ICTs) to enhance and progress their healthcare operations. It is now customary to access the internet to seek health-related information.¹ Within this framework, a diverse

¹ Chi, Y.; He, D.; Han, S.; Jiang, J. What Sources to Rely on: Laypeople's Source Selection in Online Health.

Information Seeking. In Proceedings of the 2018 Conference on Human Information Interaction & Retrieval.

New Brunswick, NJ, USA, 11–15 March 2018; ACM: New York, NY, USA; pp. 233–236.

✉ Alex Makulilo · Doreen Mwamlangala · Rindstone Ezekiel
The Open University of Tanzania, Dar es Salaam, Tanzania
E-Mail: alex.makulilo@out.ac.tz

Benedikt Buchner · Elena März
University of Augsburg, Augsburg, Germany

Merle Freye
University of Bremen, Bremen, Germany

array of e-Health products and services have surfaced. Telemedicine and electronic health records have the capacity to greatly enhance the efficacy of medical therapies. The medical industry's advancement relies heavily on data, particularly health data. Healthcare professionals, scientists, and innovators require access to health data to enhance diagnostic accuracy, tailor treatment plans, and discover novel remedies. People universally acknowledge the significance of electronic health records (EHR) in improving healthcare quality. Only recently (Jan 2025), in Germany the official rollout of the electronic patient record ("Elektronische Patientenakte") has started in several so called "model regions", however, followed by broad public discussions about data privacy and security.² However, while EHR offers promising advantages, it also raises certain technological and legal concerns. Although EHR offer the advantage of secure digital access and require fewer physical safeguards compared to paper records, the integration of patient data within a telematics infrastructure (TI) poses significant challenges and risks that are difficult to manage. Similarly, digital health has numerous valuable applications and its heavy reliance on sensitive patient health data can inevitably lead to data security issues. A significant volume of personal health data has been frequently gathered without the knowledge of individuals. Not only must the legislator establish high protective standards in a theoretical sense, but also medical practitioners and operators of the TI must continuously adhere to the legal requirements for ensuring e-Health data protection and security.

1.1 Lessons from Portugal

Despite careful planning and having data protection legislation in place, GDPR enforcement in Portugal exemplifies the potential for serious data protection and security issues. In this example, a hospital was one of the first to confront GDPR enforcement in July 2018. The hospital was fined €400,000 by the Portuguese regulator, Comissão Nacional de Protecção de Dados ("CNPD"), for multiple violations of the GDPR. Three justifications underpinned the enforcement action. Initially, there was a violation of the data minimisation principle at the hospital, whereby clinicians from all specialties had unrestricted access to all patients' clinical data. In addition, nine technical staff members had medical clearance, which granted them access to patients' data beyond the scope of staffs' job responsibilities. Furthermore, the CNPD discovered that the act of providing access to all patients' clinical data, independent of a doctor's specialisation, violated the principles of confidentiality and integrity. The personal data was accessible to a broader audience than was suitable given the circumstances. The third violation pertains to persistent and extended lapses in data security, specifically regarding the continuous assurance of confidentiality, integrity, availability, and resilience of processing systems and services. Additionally, there was a failure to establish a procedure for regularly testing, assessing, and evaluating the efficacy of technical and organisational measures, as mandated by Art. 32 of the GDPR. The hospital neglected to regularly update user credentials to avoid unlawful access to personal data. Furthermore, it neglected to

² Ärzteblatt, "Ärzte sorgen sich um Datenschutz bei elektronischer Patientenakte", <https://www.aerzteblatt.de/nachrichten/156770/Aerzte-sorgen-sich-um-Datenschutz-bei-elektronischer-Patientenakte> (07.01.2025).

establish and enforce suitable technical and organisational protocols that would have mitigated the associated risks. There were increased hazards due to the availability of special categories of personal data (such as health-related data) and the high number of individuals whose data was included.

This article critically examines the legal and ethical constraints involved in the regulation of e-Health. It looks at whether the current legal framework adequately protects e-Health personal data in Tanzania. It analyses e-Health policy frameworks considering the new rules of the Tanzanian Personal Data Protection Act (PDPA) for personal data processing. Furthermore, understanding the current policy gaps is crucial to facilitating the development of data protection guidelines specific to the health industry. It does this by analysing the current literature, legislation, regulations and policies that are implemented by the government. It also draws relevant examples and experiences from European Data Protection Law.

1.2 Enactment of the PDPA in Tanzania

Tanzania enacted the PDPA on November 27, 2022. The legislation became effective on May 1, 2023. The primary purpose of enacting the PDPA was to establish a legal framework for acknowledging and safeguarding personal data. The law provides a wide array of obligations for data controllers and processors in order to guarantee a high level of data protection. In addition, it delineates the rights of the individuals whose data is processed and establishes the Personal Data Protection Commission (PDPC) and its governing board, tasked with the management and enforcement of the PDPA.³

Section 3 PDPA defines personal data as any information pertaining to an identifiable individual that is documented in any format, including but not limited to data about education, medical, criminal and employment backgrounds. Furthermore, the definition of sensitive personal data encompasses genetic data, information about children, criminal records, financial transactions, security, and biometric data, particularly when processing reveals personal details like race or ethnic origin, political views, religious or philosophical beliefs, trade union membership, gender, health data, or sexual relationships. Section 3 PDPA also includes any personal data that, according to the national laws, poses a significant risk to the individual's rights and interests.

It is worth noting that because personal health data is categorised as sensitive data, they call for stringent conditions of processing of that category of data. Interestingly, the PDPA does not provide clear definitions for either health data or biometric data. The Act includes provisions for safeguarding personal data, establishing basic criteria for the collection and usage of personal data, and enhancing the protection of personal data handled by both public and private entities. It governs the handling of sensitive data, including e-Health data.

³ Sect. 4 PDPA.

2 The context of e-Health

The categorisation of e-Health is difficult due to its varying degree of context. In recent years, in particular, Tanzania has found its way in handling the area between medicine and information technology.

2.1 Definition of e-Health

E-health has been variably defined by scholars as a concept in information and communication technology spheres that uses web-enabled systems and processes to provide more improved health care services that includes electronic medical services, nursing, and health professional services.⁴ E-Health is an emerging field in the intersection of medical informatics, public health, and business, which refers to health services and information delivered or enhanced through the Internet and related technologies. In other words, e-Health may be described as a coordinated effort pioneered by leaders in health care and high tech industries to fully control and make use of the benefits available through convergence of the Internet and health care services. With all potential threats to patients' data, e-Health is still regarded as a cost-effective and relatively secure way of use of information and communication technology in support of health and health-related fields. Essentially, e-Health ensures delivery of digital health services using networks both at a distance and locally. As a result, various countries in the world have developed high tech systems for healthcare services which include application of e-Health technologies in the e-search and electronic recording of patients' information, sharing of patients' medical records and diseases surveillance, among others.

Some scholars argue that e-Health is a broader term used beyond mere electronic medical records, telecare, telehealth or telemedicine and use of the Internet. These scholars maintain that e-Health is a concerted effort between health care service providers and professionals with high tech experts to deploy digital technologies in management of health data or information, diseases prevention, treatment, care, monitoring/surveillance and management of health services and varieties of illnesses.^{5,6} Through e-Health system, various medical laboratory samples and referrals by medical and laboratory practitioners are sent to different medical health practitioners and personal health records are processed and stored without guarantee of safety of personal health data.

⁴ Singhal, Arvind and Cowie, Martin, What is e-Health? *e-Journal of Cardiology Practice*, Vol. 18, N° 24–10, Jun 2020.

⁵ Eysenbach G. What is e-Health? *J Med Internet Res*. 2001 Apr-Jun; 3(2): E20. <https://doi.org/10.2196/jmir.3.2.e20>. PMID: 11720962; PMCID: PMC1761894.

⁶ Oleg S., and Vicente A., et al., Remote Health/Vital Sign Monitoring, in *Mobile Health: A Technology Road Map*, Sasan Adibi (editor), Springer Series in Bio-/Neuroinformatics, Volume 5, 2015, 221–243.

2.2 Tanzania's e-Health strategy

In the last decade, the Ministry of Health published two strategy documents. The Tanzania National health strategy 2013–2018 focused on the infrastructure and technologies needed to support the transformation of the health sector. In contrast, the latest digital health strategy July 2019 to June 2024 attempts to address, among other aspects, challenges that have not been addressed or solved and the best use of technology to improve patient care. Similarly, different Apps were developed and adopted in the health sector. Currently there are over 160 digital health or health related systems in Tanzania. Some of the systems have national coverage while others are institution based. For instance, “PIGIA DAKTARI APP”, a new telemedicine mobile app for android phones, helps Tanzanians access specialist care safely in both urban and remote areas from the comfort of their homes. In recent years, the Tanzanian government has intensified the expansion of information and communication technologies and focused intently on expanding the use of mobile health (m-Health) and telemedicine. It also recognises the enormous potential of processing large data.

3 Law and regulation on protection of personal data in Tanzania

The incomplete and inconsistent regulation of health data prior to the enactment of the PDPA shows the urgent need of a law which improves data handling and reduces data privacy risks. With similar core principles to the GDPR, the PDPA has improved data privacy. Nevertheless, there are challenges to overcome.

3.1 Pre PDPA in Tanzania

Before the dawn of PDPA in 2022 in Tanzania, there was literally little or no realistic legal protection against abuse of patients' electronic health data. Claims related to violation of health personal data breaches were not easily or practically enforceable. Existing legislation such as the Pharmacy Act, 2019, Medical, Dental & Allied Health Professionals Act 2017, Human DNA Regulations Act, 2009 and HIV & AIDS (Prevention and Control) Act, 2008 did not provide for protection against unlawful processing of patients' personal data. The mentioned health related laws have some aspects of general medical confidentiality requirement but lacks specific legal regulations to address the challenges of application of emerging technologies. Contrary to the principle of confidentiality in Tanzania and Zanzibar Islands, a doctor would send patients' health information by a text message or via WhatsApp platform or by email to a pharmacist or any hospital showing all details and medical prescription without any regard to protection of health.⁷

⁷ Merle Freye, Dennis-Kenji Kipker, Rindstone B. Ezekiel, Doreen F. Mwamlangala. Strengthening Protection of Personal Data in Health Sector: A comparative analysis of the Tanzania and German ehealth System, DUD 2020, 393–397.

In 2022, Tanzania adopted the Policy Framework for Artificial Intelligence (AI) in Health Sector. The policy has recognised the significant role played by digital technologies in facilitating delivery of high-quality health care services. These technologies include mobile health (m-Health) System, Electronic Health Records System, Telehealth platform, AI technology, wireless communications and the Internet, and other digital applications. These digital technologies have been instrumental in efficient provisioning and management of health care services due to timely availability of quality health information. However, for a long time and through these electronic health delivery systems, personal health data have been massively processed by health services providers and traded off without considering the security of personal data. This affected in many ways persons' rights to privacy due to absence of comprehensive data protection law.

3.2 Post PDPA

Tanzanian law, as well as European data privacy law, has formulated a core set of overarching principles in order to provide individuals with legally enforceable rights over their personal data and establish specific obligations for those who process and control data. Under Tanzanian law, these fundamental principles are regulated in Sect. 5 of the Act which are similar to the European Union General Data Protection Regulation (GDPR). Data controllers and processors must comply with these principles because they are responsible for processing personal data.

The first principle requires the processing of personal data to be legitimate, equitable, and transparent (sec. 23 PDPA, Art. 5(1) lit. a GDPR). The principle explicitly addresses the rules governing legal processing. In order to lawfully process personal data, it is necessary to inform the data subject in advance about the authorised purpose of the processing, as well as provide information about the intended recipients.

Obtaining authorisation from the data subject is necessary prior to processing their personal data. In addition, when handling sensitive data, the law (sec. 30 PDPA, Art. 9(1) GDPR) stipulates the necessity of obtaining written consent (Art. 9(2) lit. a GDPR: "explicit consent"). However, consent may not be required for certain reasons, one of which is when processing is necessary for medical purposes in the best interest of the individual (sec. 30 (5), similar Art. 9(2) lit. c, h GDPR). A healthcare professional handles the sensitive personal data in this case, adhering to the relevant laws governing healthcare services.

The second principle is purpose limitation, (Art. 5(1) lit. b GDPR). It involves processing personal data for explicit, legitimate, and specified purposes. In addition, it prohibits further processing of personal data in a manner incompatible with the original purposes. However, the use of personal data for additional purposes is allowed if the data subject consents, if it is authorised or required by law, if the data is anonymised and used for statistical or research purposes, and if the data is pseudonymised (sec. 25(2) PDPA; Art. 4 no. 5 GDPR; recital 26 sentence 5 to the GDPR).

Adequacy is the third principle. It entails that the personal data processed should be adequate, relevant, and limited to what is necessary in relation to the stated purpose of processing. The principle requires the data processor to limit the amount

of personal data collected to only what is relevant for the intended purposes. Additionally, data processors must pseudonymise personal data when it is no longer necessary to have direct identifiable personal data, and delete or anonymise data when it is no longer needed (reg. 28 of the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023; Art. 5(1) lit. e GDPR).

Two further principles are those of accuracy and storage limitation. Data controllers must ensure that personal data in their custody is complete, accurate, not misleading, and, where necessary, kept up-to-date (“accuracy”—sec. 24 PDPA, Art. 5(1) lit. d GDPR). Also, personal data must be stored in a way that allows data subjects’ identification for a duration no longer than necessary for data processing (“storage limitation”—sec. 28(1) PDPA, Art. 5(1) lit. e GDPR). The sixth principle states that processing personal data must adhere to the data subject’s rights as outlined in the PDPA. It is crucial to align this concept with Part VI of PDPA, which delineates the rights of individuals whose data is under processing. These rights include, among other things, the right to access personal data held by the data controller or processor. This is crucial and necessary in order to exercise additional rights, such as the right to object to the processing, the right to have false or misleading data corrected, the right to have false or misleading data deleted, the right to compensation, and the right to know how their personal data will be used.

One more common principle of Tanzanian and European law is that of integrity and confidentiality. It places an obligation on data controllers to ensure the security of personal data during processing. Data controllers and processors are required to apply security safeguards that are reasonable in the circumstances for personal data protection against negligent loss, unauthorised destruction, alteration, or access (sec. 27 PDPA, Art. 5(1) lit. f GDPR).

Another significant aspect recognised by both legal systems is the international transfer of personal data. This principle is particularly relevant in the healthcare sector in Africa, as patient treatment generally takes place across national borders. In a nutshell, according to PDPA and GDPR, data controllers and processors must refrain from transferring collected personal data outside of Tanzania (resp. Europe) if the receiving country does not offer an adequate level of protection safeguards. PDPA and GDPR clarify this principle further by specifying the obligations of data controllers and processors and outline further specific conditions for transferring personal data across borders (sec. 31 and 32 PDPA, Art. 44 et sequ. GDPR).

From a comparative law perspective, the two legal systems show a similar approach. Hence, the same core principles lead to a comparable data privacy standard under Tanzanian law and the GDPR. Overall, for Tanzania, the PDPA supports regulatory progress and will result in improved personal data security in Tanzania’s expanding digital health sector, while being in greater conformity with international data privacy norms. In addition to implementing measures to protect data collection, the law establishes entities responsible for monitoring and holding data collectors and processors accountable in the event of a violation of the established standards. Section 6 of the PDPA creates the Personal Data Protection Commission (the Commission), which is a legal entity with ongoing existence and an official seal. The Commission is responsible for several functions, including overseeing the adherence of data collectors and processors to the Act, registering data collectors and proces-

sors, receiving, investigating, and addressing complaints regarding data protection and privacy breaches, as well as conducting research and monitoring technological advancements in data processing.

4 Specific challenges of processing personal health data

As alluded to, personal health data breaches pose significant risks to healthcare providers as well as patients. Accordingly, a regime for its protection is more often required to be as rigorous as possible. As mentioned before, the PDPA does not define what personal health data is, but it classifies personal health data as sensitive personal data. This classification calls for more stringent conditions to be applied whenever processing of health personal data is in question.

Sec. 30 PDPA provides a regime for protection of sensitive personal data. As a general condition, this section prohibits processing of personal data in the absence of prior written consent obtained from a data subject. However, it provides for circumstances where processing of personal health data is possible without the requirement of a prior written consent obtained from the data subject: where processing is necessary for compliance with other written laws, it is necessary for protection of vital interests of the data subject, processing is necessary for the institution, trial or defence of legal claims, processing relates to personal data previously made public by the data subject, processing is necessary for purposes of scientific research, or processing is necessary for medical reasons. To further protect the interests of the data subject, the Minister responsible for information, communication and information technology may determine circumstances in which prohibition to process sensitive personal data cannot be waived even with the data subject's consent. In addition, the Minister may make further regulation prescribing conditions for processing sensitive personal data. So far, the Minister has not issued any of the two sets of the regulations.

4.1 Consent

As the first legal challenge, the PDPA does not generally provide for the requirement of consent as a legal basis for processing of personal data. Consent is generally implied from the overall intention and objectives of the PDPA. In particular, personal data must be collected directly from the data subject and the requirements of full disclosure under Sec. 23 of the PDPA. The requirement of prior written consent applies only in case of processing sensitive personal data such as personal health data. Even in such cases, the PDPA fails to provide for conditions for such consent. For instance, the PDPA does not condition consent to be freely given even if it is in the written form and it has been obtained prior to processing of personal data. In addition, the PDPA is silent on how the data controller may be required to demonstrate that the data subject has consented to the processing of his or her personal data. Furthermore, where a declaration of written consent concerns other matters, the PDPA does not expressly demand that the request for consent should be presented in a manner which is clearly distinguishable from other matters, in

an intelligible and easily accessible form, using clear and plain language. This is in sharp contrast to Article 7 of the EU GDPR which provides for all these requirements.

Nevertheless, high requirements for consent do not necessarily lead to more autonomy and more informational self-determination, as the information model of the German and European legislators shows: Despite the requirements of Art. 7 GDPR, the data subject is still facing extensive, complicated and manipulative information. With its ambitious requirements for voluntary and informed consent, the German and European model is unrealistic and needs to be revised. Even broad consent, dynamic consent, and meta consent, which represent alternatives to the classic consent solution, cannot completely overcome the information overload of consent forms [Freye/Buchner, *Bundesgesundheitsbl.* 2024, 285, 286].

Consequently, the solution probably lies between too few requirements and too high requirements. To guarantee the informed consent research should concentrate on the question of which information should be presented at all—not with a view to a minimum but rather with a view to a maximum amount of information. Which information is elementary for an informed decision should be clarified by incorporating the findings of other research disciplines. Such an interdisciplinary approach is in line with the efforts of the European Commission to incorporate empirical decision research into its regulatory activities (Sousa Lourenço et al. (2016) Behavioral insights applied to policy: European report 903938 27; European Commission, Joint Research Centre (2022) Ex post evaluation of the activities of the Joint Research Centre under Horizon 2020 and Euratom 2014–2020: final report of the ex post evaluation panel <https://doi.org/10.2760/25731526>, 27).

In particular, the transfer of behavioral science theories to consent behavior can provide conclusions about appropriate information for consent. For example, promising approaches refer to Rogers' Protection Motivation Theory (PMT) (Rogers RW (1983) Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo/Petty (Hrsg), *Social psychophysiology: a sourcebook*, S. 153–177) and demand that information obligations must be designed based on PMT (Boerman SC, Kruikemeier S, Zuiderveen Borgeisius FJ (2018) Exploring motivations for online privacy protection behavior: insights from panel data. *Communic Res* 7:953–977; Helberger N, Lynskey O, Micklitz H-W, Rott P, Sax M, Strycharz J (2021) EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets; Strycharz J, van Noort G, Smit E, Helberger N (2019) Protective behavior against personalized ads: Motivation to turn personalization off. *Cyberpsychology* 13(2):1). However, research in this area just started, and there are only a few studies that design specific information obligations in this sense, for example, on cookie consent (Chennamaneni A, Gupta B (2022) The privacy protection behaviours of the mobile app users: exploring the role of neuroticism and protection motivation theory. *Behav Inf Technol*) or consent for health apps (Freye, *Gesundheits-Apps—Diktierte Selbstbestimmung*, 2025).

4.2 Scientific research

The second legal challenge which is an issue for legal debate across many jurisdictions relates to scientific research involving personal health data.⁸ This problem has become more complex in recent years due to the requirements of data sharing. To share or not to share health personal data has in most cases called for data sharing policies. Quite few educational and research institutions in Tanzania have put in place such data sharing policies. Muhimbili University of Health and Allied Sciences (MUHAS) is one of such institutions with a data sharing policy that applies to its staff, students, research collaborators, and other entities that use MUHAS data. This Policy was adopted in 2020 prior to the enactment of the PDPA. Overall, such data sharing policies fail to provide expressly for the protection of personal health data. Perhaps to mitigate this challenge, a review of such policies in line with the PDPA is recommended. Sec. 65 PDPA provides a mandatory requirement by data controllers to draw and put in place codes of ethics or policy for personal data protection which must prescribe for ethics and conduct to be complied with during collection or processing of personal data. This provision is a starting point to mitigate this challenge.

The other problem is based on sec. 64(2) PDPA which gives power to the Minister to prescribe conditions for processing sensitive personal data. As presented earlier, the Minister has not so far prescribed such conditions. In any case such conditions are going to be over and above the conditions and requirements prescribed in sec. 30 PDPA. If care is not well exercised there is a danger that the regime for processing sensitive personal data, and in this case personal health data, is going to be overregulated.

4.3 Anonymisation

Just like the GDPR, the PDPA applies to personal data. This necessarily means that non-personal data falls outside the purview of the PDPA. Concomitantly, the definition of personal data is crucial to determine if processing of personal data by a data controller is subject to legal constraints. However, the question as to whether a particular dataset constitutes personal data is sometimes difficult to determine. More so, with the advent of Big Data, the utility and value of personal data require to be balanced with the data subject's right and expectation of protection of his or her privacy. In such a situation the requirement for consent prior to processing personal data for secondary use can be maneuvered through technical methods. Broadly speaking this is achieved through de-identification of personal data. As both the GDPR's and PDPA's central focus of defining personal data is identifiability of a natural person, once personal data is de-identified in such a way that it is no longer possible to identify a natural person, the legal constraints attached to the data controller cease to apply. In other words, the data controller will no longer be obliged to obtain consent from data subjects, give access to and/or rectify personal

⁸ For the discussion in Germany see e.g. NFDI4Health White Paper: Improving Record Linkage for Health Research in Germany (in German), <https://repository.publisso.de/resource/frl:6461895>.

data held by him or her. In short, any obligation that is imposed by the law on data controllers will not be applicable.

Likewise, under the GDPR, to use data freely, it must fall outside the scope of the GDPR, requiring anonymisation so that individuals are no longer identifiable. While personal data is defined in Article 4 (1) No. 1 GDPR, there is no explicit definition of anonymisation, recital 26 sent. 5 simply states that anonymous data is not subject to the GDPR. The key question, therefore, is what qualifies as anonymous data.

There are various perspectives in literature and among data protection authorities, thus creating legal uncertainty about the required level of anonymity.⁹ The key point is whether anonymisation must be irreversible or if it is sufficient that the likelihood of re-identification is low by the recipients of the data. The latter view is supported in particular by recital 26 sent. 3 to the GDPR, which assumes that whether a person can still be categorised as identifiable depends on what means are likely to be used to identify a person. Relevant for these means are all objective factors, such as the costs of and the amount of time required for identification, available technology at the time of processing and technological advancements, as noted in recital 26 sent. 4 to the GDPR. The decisive factor in this assessment is always the group of recipients of the anonymised data, to estimate the expected efforts, resources and capabilities required for re-identification.

Anonymisation poses a particular challenge with health data because the information relevant for research often derives from information elements such as age, region of residence, occupation and behaviours such as smoking and drinking. Whereas with other data, it is often sufficient to delete direct identifiers such as name and indirect identifiers such as telephone number or addresses, with health data, it may still be possible to identify an individual due to the many attributes mentioned above. In general, in health research, the goal is to retain as many attributes as possible without unnecessarily reducing the informational value of the dataset.

An example of an anonymisation technique is k-anonymity. This technique works by grouping records with the same attribute in a data set, such as gender, to ensure that a person cannot be singled out¹⁰ or identified based on an indirect identifier.¹¹ For instance, k-anonymity is achieved if the attributes “female” or “male” each appear at least 10 times in the dataset. However, this method requires a dataset to be large enough to form such groups. By applying techniques like this, datasets can be anonymised, reducing the risk of re-identification while still enabling data analysis.

In contrast to GDPR, the PDPA does not provide directly and in detail for the de-identification techniques particularly data anonymisation. Nonetheless this requirement may be impliedly read within certain provisions of the PDPA. For example, sec. 5(g) of the PDPA refers to use of appropriate technical or organisational mea-

⁹ Aufschläger/Folz/März et. al., Anonymization Procedures for Tabular Data: An Explanatory Technical and Legal Synthesis, *Information* 2023, 14, 487, p. 24; see also Lettieri/Kipker, *Synthetische Daten in der medizinischen Forschung: Eine datenschutzrechtliche Bewertung*, *DuD* 2024, 284.

¹⁰ Article 29 Data Protection Working Party, Opinion 5/2014 on Anonymisation Techniques, WP216, 10 April 2014.

¹¹ Aufschläger/Folz/März et al., Anonymization Procedures for Tabular Data: An Explanatory Technical and Legal Synthesis, *Information* 2023, 14, 487, p. 26.

asures as far as appropriate security of the personal data is concerned. This may include the de-identification technique of anonymisation. Similarly, sec. 25(1)(d) of the PDPA permits the secondary use of personal data if it is used in a form in which the data subject is not identified, or for statistical or research purposes if they may not be published in a form that could reasonably be expected to identify the data subject. In addition, regulation 28(d) and (e) of the Personal Data Protection (Personal Data Collection and Processing) Regulation 2023 requires data controllers and processors to consider pseudonymisation and anonymisation techniques in implementing the principles of proportionality and necessity. It is arguable that the absence of clear provisions on de-identification techniques in the PDPA leaves many questions unanswered: what is the scope of the PDPA as far as de-identification techniques are concerned? Does sec. 25(1)(d) of the PDPA envisage the application of anonymisation technique? This question becomes more valid as the PDPA defines personal data in terms of “identifiable person”. Most of these questions would require clarification by a court of law.

5 Conclusion

The introduction of the PDPA has significantly improved the data protection landscape in Tanzania and is an important step forward in addressing data protection issues. This progress emphasises the necessity of establishing a legal framework that has provided greater clarity and accountability in the handling of personal data. However, challenges and legal uncertainties remain, not only within the PDPA but also with the GDPR in Europe.

As has been shown, the anonymisation of data as an important factor of data security is a cross-border challenge in Tanzania as well as in the EU. Anonymisation techniques offer a promising way to mitigate these challenges, as they can enable the use of data while reducing legal risks by removing the data from the scope of strict legal frameworks. However, even with the possibility of anonymising personal data, the legal foundation created by the PDPA and GDPR remains invaluable. They provide clear benchmarks for what constitutes safe and ethical data practices, providing a baseline of trust and security. Future efforts should focus on refining the existing legal frameworks to address the challenges revealed in this article, while advancing anonymisation methods. This dual approach could reconcile innovation and strengthen personal data protection.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.