LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Data Protection in Employment: Implications of the Personal Data Protection Act in Tanzania

MARK MALEKELA
Alistair Group
Government Liaison
malekelamark@gmail.com

ALIKO SIMON
Clyde & Co Tanzania
Partner – Employment, Immigration
aliko.simon@clydeco.co.tz

ABSTRACT

Innovations in technology, their varied uses, and the widespread use of social media have all advanced more quickly than in the past, both globally and in the workplace, where employee and customer data is constantly being collected and digitally documented. For this reason, the need for regulatory compliance on protecting personal data in the workplace is paramount. Based on critical analysis of the relevant legislation, case laws, and literature, this article reviews the current state of privacy and data protection in the employment context in Tanzania.

This article discusses the implications of the new data protection legislation in Tanzania with a focus on privacy and data protection rights and employee monitoring issues that human resource professionals, managers and employers must be aware of. As it is common for employers to keep employment records, which amount to data, employment is one of the numerous areas and facets in Tanzania that are impacted by the PDPA, 2022. In accordance with the PDPA, employers have a responsibility to protect employee data as data controllers who process sensitive personal data to satisfy the condition that the processing is necessary for the purposes of compliance with the

ELRA. Finally, this article recommends that like the EU's W29 opinion on protection of employee personal data, a special guidance note tailored on employee personal data protection from the PDPC will improve employee privacy in Tanzania.

Keywords: labour law; employee; personal data protection; PDPA; employment.

https://doi.org/10.6092/issn.2421-2695/22368

Data Protection in Employment: Implications of the Personal Data Protection Act in Tanzania

1. Introduction

Tanzania is one of the fifty-four (54) independent states in Africa, and among the rising economies in East Africa. The growth of technology and innovations has led to gradual economic growth in Tanzania with the rural to urban migration being one of the factors for this growth. ([1]) People are thought to migrate from rural areas to cities due to projected opportunities, lack of employment, and service accessibility. Once employed, Tanzanians also face the reality that technology has advanced to the point that nearly all information may now be kept electronically, improving data operations. Employers are required by law to retain employee's data, either for the purpose of managing their human resources or to comply with social security or employment regulations. Specifically, section 96 of the Employment and Labour Relations Act (ELRA) mandates Tanzanian employers to create and maintain one or more registers with details about each of his employees. According to Section 96, the employer must provide the Labour Commissioner with various information including, wage-related information upon request. Employers are required by section 98(2)(o) of the ELRA to provide the Labour Commissioner with returns that include information about each employee. The ELRA would also apply to foreign employees, and it mandates that the employer of a foreign employee provide the relevant information to the Labour Commissioner.

This information often constitutes personal data, which includes any details that can identify an individual such as names, contact details, identification numbers, job titles, salaries, and employment history; making it particularly sensitive in the context of employment. Even though personal data primarily belongs to the individuals who provide it, employers become in charge of data in a workplace context. In that context, employers are now legally required to retain and manage employees' personal data, either for human resource purposes or to comply with national laws, including social security and tax laws. Historically, there was little legal oversight governing the handling of personal data, leaving employees' personal data vulnerable to misuse. However, the enactment of the Personal Data Protection Act (**PDPA**) in 2022 brought significant changes, mandating more stringent control over how personal data is stored, processed,

([1]) A. Makulilo, *African Data Privacy Laws*, Springer, 2016, 4.

and shared. Since employers are both data controllers and data processors, it is imperative that they and their management team understand the provisions of the Act.

Thus, it is sufficient to enquire as to whether the PDPA protects employment records. Application forms and work references, payroll and tax records, social benefits data, sick leave and sickness records, annual appraisal and assessment records, records pertaining to disciplinary actions, transfers, and promotions, and records pertaining to workplace accidents are among the records that are covered by data protection laws.([2]) These documents are classified as 'sensitive data,' which is shielded under the recently enforced PDPA.

This article thus seeks to explore the implications of the PDPA on employee personal data protection in Tanzania. Specifically, it addresses how the PDPA balances the need for companies or legal entities to manage employees' personal data with the fundamental right to privacy. The central research question guiding this study is: *How does the PDPA safeguard employee personal data to balance the right to privacy in the Tanzanian legal context?*

To answer this question, this article is structured as follows: the first part introduces the legal landscape of employee personal data protection in Tanzania. The second part explores the right to privacy under Tanzanian law, discussing the balance between privacy rights and data protection obligations. The third part examines employee data protection, focusing on the responsibilities of employers and employees in managing personal information. The fourth part further addresses the contract of employment and its relation to personal data, outlining how employment agreements intersect with data protection laws. The fifth part specifically delves into analysis of the PDPA, discussing its key provisions, and examining the rights of employees as data subjects. Part six discusses 'Sensitive Personal Data' in connection with employment, highlighting the types of data that require heightened protection under the PDPA. Finally, part seven offers a conclusion, summarizing the findings and implications of the research.

2. Right to Privacy under Tanzanian Law

The intersection of data protection and the right to privacy is a critical issue under the Personal Data Protection Act (PDPA) in Tanzania. This section explores the balance between these two legal principles. In Tanzania, the right to privacy is enshrined in the Constitution of the United Republic of Tanzania, specifically under Article 16, which guarantees the protection of personal privacy.([3]) However, this right is not absolute and

([2]) See section 3 of the Personal Data Protection Act R.E. 2022.

([3]) The Constitution of the United Republic of Tanzania, 1977; J. Ubena, *Privacy - a forgotten right in Tanzania, Tanzania Lawyer*, I/2JTLS 2012, 72-114.

may be subject to limitations, especially when it intersects with national security, public interest, or other legal obligations. (4)

Data protection, which involves the regulation of how personal information is collected, stored, and used, is a narrower concept than privacy but is intrinsically linked. While privacy law encompasses a broader range of issues, including physical intrusion and publication of personal matters, personal data protection specifically addresses the management of recorded personal information. This distinction is crucial in understanding how the PDPA seeks to protect employee data while acknowledging other interests, such as business operations and compliance with legal requirements.

International frameworks, such as the European General Data Protection Regulation (**GDPR**) (5) provide useful guidance in this area, demonstrating how data protection laws can be harmonized with privacy rights. For example, the GDPR emphasizes the necessity of transparency, accountability, and consent in data processing, which are principles that the Tanzanian PDPA also aims to uphold. (6) However, the enforcement and practical application of these principles in Tanzania are still evolving.

Despite that Tanzania recently enacted the PDPA to fill the gap on privacy laws that once existed, the public's understanding and compliance with data protection laws remains limited.(7) With the advent of modern digital technologies, there is a growing need for further training, sensitization and more robust enforcement mechanisms to ensure that Tanzanians fully appreciate the significance of personal data protection and privacy. (8)

(4)A. Makulilo, *African Data Privacy Laws*, *cit.*; J. Ubena, *Privacy - a forgotten right in Tanzania.* cit.; P. Boshe, *Interceptions of communications and the right to privacy: Commentary on Zitto kabwe's political saga*, in *Open University Law Journal*, Vol. 4, No. 2:1-5.

(5) The General Data Protection Regulation, Regulation (EU) 2016/679 in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.

(6) C. Delbar et al., *New technology and respect for privacy at the workplace*, European Industrial Relations Observatory, 2003.

(7) P. Boshe, *Interceptions of communications and the right to privacy* cit.

(8) P. Wahlgren, *Information and Communications Technology Legal issues: Data protection and Privacy*, in *Scandinavian studies in law*, 2010, 153.

3. Employee Data Protection

Working circumstances have evolved over time along with tools and equipment. From a historical perspective, the industrial revolution replaced manual labour with machine labour, which has resulted in the largest transformation to date. Nowadays, digital revolution is reshaping almost every workplace. Working conditions have altered because of digital technologies in terms of response time, multitasking, knowledge availability, and most importantly for issues pertaining to fundamental rights monitoring capabilities. ([9]) In many countries, employees' personal information is used for business purposes. Digital technologies are used at the corporate level to generate and manage employees' data. Examples of digital technologies used in personnel administration include personal information systems, email and internet usage, video camera data, working time records, attendance, and sickness records, and many more. More data is proactively processed by employers than is required to satisfy legal or contractual obligations. ([10])

Employees as data subjects frequently suffer double harm, first as workers and secondly as citizens and consumers—data protection is, therefore, an issue that affects everyone, not just employees. There are situations where being an individual and an employee are interconnected in relation to the personal data in use. For instance, when a person works at a hospital and has their personal medical records kept there, or when they are required to have a bank account with the same bank. The fact that personal data is occasionally created automatically, without the consent of the data subject or even their knowledge, when looking at dynamic data, connection data, or simply log files, makes it clear that employees often have limited access to and rights to their personal data. As argued by Fritsch, 'the disparity in information is obvious. Employers may use this information without disclosing to workers, which could lead to an unexpected termination of the employment relationship.' ([11])

Employees are now able to operate from anywhere at any time thanks to cloud services, unified communication systems, and shared documents. They can also be readily tracked and traced. Digital technologies are currently acquiring and retaining employee personal data at a rapid pace. Due to the abundance of data and its continuous growth, information is used without consideration for the PDPA's data processing conditions, which include, among other things, data minimisation, storage limitation, and transparency.

This begs the question: are Tanzanian employees aware of data protection and its relevance in the workplace? This could be responded with a factual reality and as seconded by Makulilo, that, most Tanzanians do not exhibit caution when it comes to

([9]) B. Mujtaba, *Digital Literacy on Privacy Rights Policies in the American Workplace* in *Multidimensional and Strategic Outlook in Digital Business Transformation. Contributions to Management Science*, Springer, 2023.

([10]) B. Mujtaba, *Digital Literacy on Privacy Rights Policies in the American Workplace*, *op. cit.*

([11]) S. Gutwirth et al. (eds.), *Reforming European Data Protection Law,* Law, Governance and Technology Series, Springer, 2015, 149.

data protection or personal privacy. Ignorance is rampant in society, particularly among the younger generation, especially on social media. The quantity, variety, and kind of personal information shared on social media show a lack of personal consideration for how one's activities may affect one's own privacy and the security of one's own and other people's data. ([12]) For instance, despite the ongoing exposures to sensitive images of individuals in intimate situations online, widely known as. 'pornographic content', a survey conducted by REPOA and Afrobarometer once revealed that more than 54% of Tanzanians are reported to support unrestricted access to social media and the internet. One third, that is 33% of Tanzanians want access to be regulated by the government – these include, educated citizens, youth, men, and urban citizens. ([13])

Now, does the lack of personal consideration for how one's activities may affect one's own privacy and the security of one's own and other people's data extend to the workplace? Indeed, to an extent, it does extend. However, the public is now becoming aware of the importance of their personal privacy, including in relationships with their current or former employers. This was exemplarily evident in the High Court of Tanzania case of *Deogras John Marando v. Managing Director, Tanzania Beijing Huayuan Security Guard Service Co. Ltd*, ([14]) where the appellant, a former employee of the respondent claimed that the respondent breached their privacy by using attributes (images) of the appellant's identity or likeness to advertise his security company without his permission. The appellant had argued among others, that, 'in his employment contract, none of the clauses allowed use of his image rights for advertisement.' However, since the case was filed when there was no employment relationship between the parties, the Court only acknowledged the matter as a liability emanating from the likeness or invasion on the right to privacy of the appellant and no employment relationship existed.

In determining whether there is any employment relationship between the parties when a case on liabilities on invasion of privacy, the Court relied on the observation by Her ladyship Nyerere, J (as she then was) in the case of *Noah Musangile v. Tanzania Breweries Ltd*, ([15]) that:

"In strengthening the removal of the complexity in determining existence of the employment relationship "...protection for workers in an employment relationship, the determination of the existence of such a relationship should be guided primarily by the fact relating to the *performance of work and remuneration of the worker*, notwithstanding how

([12]) P. Boshe, *Data Privacy Reforms in Tanzania*, in *African Data Privacy Laws*. Springer, 2016.

([13]) REPOA, Afrobarometer, *Majority of Tanzanians want unrestricted access to social media but are wary of fake news and intolerance*, Afrobarometer, 2021; See also, J. Maricha, *Internet body slams proposed 'X' platform ban in Tanzania*, The Citizen, 6th July 2024. Available at: https://www.thecitizen.co.tz/tanzania/news/national/internet-body-slams-proposed-x-platform-ban-in-tanzania-4682016 Accessed on 25th August 2024.

([14]) *Deogras John Marando v. Managing Director, Tanzania Beijing Huayuan Security Guard Service Co. Ltd*, Civil Appeal No. 110 of 2018 [HCTZ, 2019], 4-6.

([15]) *Noah Musangile v. Tanzania Breweries Ltd,* (2015) LCCD 148, 149.

the relationship if characterized in any contract arrangements, contractual or otherwise, that may be agreed between the parties."

The Marando case thus shows that, privacy, and data protection awareness by employees in Tanzania is increasingly growing – even though gradually with time. This is specifically backed up with the enacted PDPA in 2022, and the establishment of the Personal Data Protection Commission (**PDPC**) which works in educating and training the community on the relevance of personal data protection and requires companies and organizations to have Data Protection Officers (**DPO**s) – which are obviously employees in the same entities.

After the PDPA was enforced in 2023, companies and organisations must comply with the law, by having adequate levels of data protection. However, in the context of employment research studies and legal updates by for instance, law firms demonstrate very few important details on data protection in the employment context and from PDPC standards. ([16]) Research findings are also confined to comparing legal standards pertaining to the use of email and the internet at work; and not data processing and protection. Some authors of these studies and updates deal with the diverse application of data protection laws or their international scope, but they do not concentrate on labour law. ([17])

Comparatively, in order to address the data protection obligations within employment relations, numerous national data protection authorities globally, such as those in the United Kingdom, Ireland, Italy, Austria, or France developed detailed guidelines and related publications. ([18]) Opinions regarding electronic communication in the workplace have been voiced by certain national data protection authorities, such as those in Denmark, Germany, Ireland, Italy, France, or Belgium.([19]) However, even though the legal force of these documents is quite weak, their authorities have nonetheless tried to fill a legal gap,([20]) bearing the fact that most data protection laws including Tanzania's PDPA are in most cases tailored as multi-sectoral legislations.([21])

Tanzania's ELRA is silent on employees' data privacy and protection. In essence, there is also no specific legislation that covers on employees' privacy and data protection at the workplace in Tanzania. Despite a lack of specific legislation, the general legal framework – that is, the PDPA and its principles on personal data protection are interpreted as having implication on employees' internet, email use, records and personal data. ([22]) On the other hand, countries like, Finland, Germany, Norway, and

([16]) L. Mitrou & M. Karyda, *Employees' privacy vs. employers' security, Can they be balanced?* Elsevire Ltd., 2005.

([17]) C. Delbar et al., *New technology and respect for privacy at the workplace*, *op. cit.*

([18]) H. Frank, *Protection of workers' personal data in the European Union*, Leuven/Tilburg, 2002.

([19]) H. Frank, *Protection of workers',* cit.

([20]) *Ibid,* note 20.

([21]) Tito Magoti v. Attorney General, (Misc. Civ Cause No. 18 of 2023) [TZHC 2024].

([22]) C. Delbar et al., *New technology and respect for privacy at the workplace*, *op. cit.*

Sweden have worked on specific legislations in a move to alter the status quo; for improved employee data privacy laws. ([23])

Does Tanzania need to make the same move? Context-wise, it is not necessary except where the PDPC as the relevant authority does not provide for specific guidelines on employee data protection as ruled by the High Court of Tanzania in the recent case of *Tito Magoti v. Attorney General.*([24]) Furthermore, as most employers collect numerous amounts of personal data from applicants (successful and unsuccessful), former applicants (successful and unsuccessful), employees (current and former), agency staff (current and former), casual staff (current and former), contract staff (current and former); it would be necessary for both, employers and employees as parties to the employment contract to consider placing data protection clauses in the contracts of relevant staff in a company or organisation as discussed further in the section below.

4. Contract of employment and Personal Data

With the absence of specific legislation or guidelines by the PDPC on employee data protection in Tanzania, a framework on personal data protection can be developed from the basis of performance of duties of parties under contracts of employment.([25]) A contract of employment contains terms and conditions, and duties which parties must perform based on the principles of good faith, and loyalty.([26]) A violation of certain terms, conditions and obligations will result in a breach of contract and consequently a litigation instituted by an aggrieved party in court. With Tanzania as one of the common law jurisdictions that rely and apply the doctrine of precedents, courts' decisions might form the basis of developing the duty to protect the employees' personal data.

Before the PDPA came into force in 2023, it was unusual for an employment contract between an employer and an employee to include a provision on privacy rights or the protection of the employees' personal data. Most contracts do not contain such explicit stipulations. This is perhaps because, as Olsen asserts, the definitions of the rights to privacy and data protection may change in the context of employment relationships. Employees cannot expect a high degree of privacy protection when performing work unless agreed via an employment contract – as employers have a legitimate justification and right to know certain personal data about their employees, to the extent that such information is relevant for the performance of work at the workplace.([27]) As a result, some employers may use the loophole to create systems and

([23]) *Ibid,* note 23.

([24]) Tito Magoti v. Attorney General, (Misc. Civ Cause No. 18 of 2023) [TZHC 2024].

([25]) K. Hassan, *Personal data protection in employment: New legal challenges for Malaysia,* in *Computer Law & Security Review*, Volume 28, Issue 6, 2012, 696-97.

([26]) *Jordan University College vs Flavia Joseph* (Labour Revision No. 23 of 2019) [2020] TZHCLD 3822

([27]) C. Olsen, *To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR*, in *International Data Privacy Law*, 2020, Vol. 10. No. 3, 241

technologies that monitor employees' performance,([28]) such as their work presence, productivity, and private e-mail correspondences.([29]) Nevertheless, with the current prevalence of personal data protection and privacy rights disputes knocking the doors of the Tanzanian courts,([30]) it is pertinent to note that, employment contract law would acknowledge the existence of privacy rights and personal data protection in the form of implied terms of contracts. Employment contract law allows the employee to take civil action against his employer and seek for appropriate remedy where a breach of a contractual obligation has transpired. ([31])

On the other hand, employees are obliged under the purview of employment contracts to not disclose confidential information that qualifies as sensitive trade or commercial information belonging to the employers.([32]) An employee is obligated to act faithfully to his employer during the duration of employment. Certain employment contracts have explicit clauses that forbid workers from suing employers that reveal their personal information. Courts have developed and applied this duty to encompass other implied duties of employers that are deemed have been incorporated in the contract by implication.

Examining cases pertaining to "employment records and breach of contractual obligations" is pertinent in this context since the duty to preserve personal data is the subject matter under discussion, and this concept can be easily applied. An employee may have recourse against his employer for breach of personal data if the employer fails to uphold its implied duty to "keep and maintain employment records." For instance, in *Koba Said Mdoe v. R and K Trucking Co. Limited* ([33]) the application was filed to challenge the decision of the Commission for Mediation and Arbitration (**CMA**) involving unfair termination claims. In this case, the court reiterated that it is the employer's duty to maintain employment records and provide evidence of termination dates in disputes. In this case, the employer failed to provide documentation proving that the applicant's employment contract was terminated on the said date. Hon. Opiyo, J. further reiterated

([28])G. Swell, *Nice Work? Rethinking Managerial Control in an Era of Knowledge work*. 12 Organization 2005, 685, 691; H. Braverman, *Labor and Monopoly Capital; The Degradation of Work in the Twentieth Century*. NYU Press, 1998, 80-82

([29]) A. Rosemblat - T. Kneese & D. Boyd, *Future of Labor: Workplace Surveillance*, in *Data & Research Institute*, 2014, 1 https://www.datasociety.net/pubs/fow/WorkplaceSeurveillance.pdf

([30]) Several decisions have been rendered by the High Court of Tanzania with respect to privacy rights as seen in *Abdallah Shabani Madege v. The Republic,* Crim. Appeal No. 101 of 2020 [2021]; *Tito Magoti v. Attorney General,* (Misc. Civil Cause No. 18 of 2023) [TZHC 2024]; *Safari automotive Limited v. Godwin Danda,* (Civil appeal no. 978 of 2024) [2024] TZHC; *Deogras John Marando v. Managing Director, Tanzania Beijing Huayuan Security Guard Service Co. Ltd*, Civil Appeal No. 110 of 2018 [HCTZ, 2019]; *Safari automotive Limited v. Godwin Danda,* (Civil appeal no. 978 of 2024) [2024] TZHC and others, just to mention a few.

([31]) In *Jordan University College vs Flavia Joseph* (Labour Revision No. 23 of 2019, 2020, TZHCLD 3822 the High Court observed that, «the contents of a contract are its terms, which define the rights, obligations, and rules by which the parties are to be bound in the contract. Thus, a contractual term is any provisions forming part of the contract. Each term gives rise to a contractual obligation, breach of which can give rise to litigations».

([32]) K. Hassan, *Personal data protection in employment: New legal challenges for Malaysia, op. cit.*

([33]) *Koba Said Mdoe vs R and K Trucking Co. Limited* (Revision 410 of 2022) [2023] TZHCLD 1252

that in any legal proceedings, the employer has a duty to prove or disprove the employment in accordance with section 15(6) of the ELRA.

In yet another case of *Amsons Industries (T) Ltd v. Mashaka Marusu*([34]) the applicant failed to produce a written contract leading to the presumption that the respondent was employed under a permanent contract. This finding was based on the employer's legal duty to maintain and provide employment records. The applicant failed to present a written employment contract for the respondent. The court highlighted that maintaining employment records is crucial for employers to establish the terms of employment. The absence of such records automatically shifts the burden of proof to the employer. Hon. Muruke, J. referenced the case of *Ramadhan H. Ramadhan v. Andro Roofing Product Ltd,* Rev. No.347/2009 where it was held that it is the duty of employer to keep an employment record. With the present development of technologies as aforementioned, keeping and maintenance of employment records to establish the terms of employment would have to go hand in hand with the duty to preserve and protect personal data. This is relevant as these records would normally contain a variety of personal data, including name, age, permanent residence address, sex of the employee, place of work, renumeration, and details of any benefits or payments.([35])

Thus, the above cases are relevant and important as they give rise to the duty and principle to keep and maintain employment records which can form the basis of employers" duty to protect the personal data of the employees. Put simply, the employer has an obligation to protect employee's right to privacy in the context of personal data, and not to share or handle personal information in a way that might harm the workers.([36]) These instances demonstrate that employment contracts recognise the obligation to maintain and keep employment records in addition to the legislative recognition of personal data in the PDPA, including employees' personal data. With the enactment of the PDPA, this duty may now be further recognised in the form of explicit or implied obligations in employment contracts.

5. The Personal Data Protection Act 2022

The Harmonisation of the ICT Policies in Sub-Saharan Africa (HIPSSA) project marked the drawing of the first comprehensive data protection law in Tanzania as a 'Draft Privacy and Data Protection Bill 2013.' After the Bill was examined by International Technology Union (ITU) and local experts, and following multiple rounds of consultation and revisions, it was decided to rename it the "Draft Personal Data Protection Bill."([37]) Fast forward, in 2022, the Tanzanian parliament enacted the PDPA with the UK Data Protection Act serving as the inspiration of a law to regulate the

([34]) *Amsons Industries (T) Ltd vs Mashaka Marusu*, Labour Revision No. 735 of 2019, 2020, TZHCLD 1

([35]) See section 15 and 96 of the Employment and Labour Relations Act, [CAP 366, R.E. 2019]

([36]) K. Hassan, *Personal data protection in employment: New legal challenges for Malaysia, op. cit.*, 697.

([37]) A. Makulilo, *African Data Privacy Laws*, *cit.*, 176.

acquisition, storage, processing, or application of personal information by any person in order to protect that person's personal information and preserve that person's right to privacy. This promotes customer trust and levels the playing field so that improper use of personal data cannot provide an unfair advantage to individuals, including employees in different institutions, companies, and organisations.([38]) Tanzanian employers and employees would thus be one step ahead to familiarise themselves with the PDPA and its requirements.

The PDPA's requirements and guidelines permit the lawful handling of personal data. To protect personal data, processing must only be done so in a way that is transparent, legal, and respects the rights of the data subject. The PDPA recognises that while protecting data subjects' rights is crucial, it's also critical to strike a balance between their right to privacy and their right to information access.([39]) Similar to the European Union's (EU) GPDR, Tanzania's PDPA is a general or multi-sectoral legislation that covers a broad range of data processing activities, actors, and definitions.([40]) As mentioned in recital 15 of the EU GDPR, the PDPA's provisions are thus observed and considered to be comprehensive, with their application extending to numerous industries and embracing the idea of technology neutrality. This includes information that is either directly or indirectly gained in the course of employment, such as biometric information collected by human resource teams in an organisation or company, documents, addresses, gender information, and employment histories.([41])

To maintain its scope of application, the Tanzanian legislator likewise chose to employ a rights-based and principled approach, from which the processing organisations must infer compliance. As a result, institutions or organisations that maintain or manage data may be considered "data controllers or processors" under the PDPA; so, "natural or legal persons" in this context applies to both individuals and corporations. This implies that an official or the management within an organisation may be the "person" in charge of the data. This "person" works for the employer, as probably an employee or is their representative.

The implication is that companies, institutions, and organisations that hire employees – in this context as data subjects, must evaluate their own operations and implement the required procedures and systems as data controllers or processors to abide by the PDPA. The notion of accountability, which requires organisations, companies, and private or public institutions processing personal data, to ensure compliance with the PDPA, is a fundamental component and pillar of the data protection law.

([38]) Clyde & Co, *Tanzania: The Personal Data Protection Act of 2022,* 16th February 2023.

([39]) See PART VI of the Personal Data Protection Act [CAP 44 of 2022]

([40]) PM. Schwartz - KN. Peifer, *Transatlantic data privacy* (November 7, 2017), in *The Georgetown Law Journal*, 2017, 106-115, UC Berkeley Public Law Research Paper. Available at SSRN: https://ssrn.com/abstract=3066971.

([41]) See section 3 of the Personal Data protection Act, 2022 read together with sections 15 and 96 of the Employment and Labour Relations Act, [CAP 366, R.E. 2019]

5.1 The PDPA and its relation to employment

Section 3 of the PDPA defines personal data as information that relates to an identifiable person including, their race, ethnicity, religion, age, or marital status, education details, medical, criminal or employment history, address, biometrics, genetic data, correspondences sent to a data controller by the data subject hat is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence, and the views or opinions of any other person about the data subject.(42) In the employment context, this would imply that all these information, as collected by the employers and required to be kept for record under labour laws,(43) amount to personal data.

In this respect, it becomes easy to apply the PDPA in an employment setting as the term "employment history" in that part refers to a document that includes pertinent details about a person's prior work experiences. The words "correspondences sent to a data controller by the data subject" could be inferred to mean for instance, every e-mail correspondence between an employer and the employee that are of confidential nature; including any opinions of any other person about the employee as the data subject. Whether the employment agreement signed by the employer and employee is a "contract of service" or a "contract for services" employers are required by law to manage employees' or individuals' personal data in accordance with the PDPA under both types of contracts.(44)

Jurisdictional applicability of the PDPA establishes who will be governed by this legislation. In a general sense, the jurisdictional application of the PDPA is like that of other laws. The two main criterion for the PDPA's applicability are the location of the data processing and whether Tanzanians are involved. Tanzanian employees are immediately covered by the PDPA if they are the data subjects or data controllers or processors, that is, employers. Where the data processing is located and who processes the data are the factors to consider for the jurisdictional application of the PDPA. Section 2 of the PDPA provides that the Act shall apply:

"to Mainland Tanzania as well as Tanzania Zanzibar save that in Tanzania Zanzibar this Act shall not apply to non-union matters."(45)

What about foreign entities that are present in Tanzania? In this context, the PDPA also extends its applicability to foreign corporations, institutions, and organizations operating in Tanzania, particularly those that utilize manual or computer-based processing systems within the country. Bearing how personal data is defined in

(42) The Personal Data Protection Act, [CAP 44, 2022].

(43)Section 96 of the Employment and Labour Relations Act (ELRA) to create and maintain one or more registers with details/records about each of his employees.

(44)C. Ogriseg, *GDPR and Personal data Protection in the Employment Context, in LLI*, Vol 3, No 2, (2017).; K. Hassan, *Personal data protection in employment: New legal challenges for Malaysia, op. cit.*, 699.

(45) The Personal Data Protection Act, [CAP 44, 2022].

section 3 of the PDPA, the PDPA deals with scenarios in which personal data is recorded in any format regardless of whether the data processing is automated or conducted manually.([46]) These formats include those involving computerised data processing, file systems, and the documenting of personal information. That is, the data can be entered manually into forms or filling systems, or it can be processed automatically by hardware, like a personal computer.

It is critical that some personal data directly connected to a given person be readily available for recording, holding, and/or retrieval using manual or computer means – that is, processing. The data must link to a specific person. But how does the PDPA's definition of personal data apply to indirectly connected data? "Indirectly related or connected" in this context refers to any circumstance in which the business particulars refer to an individual, such as in entity business concerns, in which case the data are said to pertain to that individual. As a result, information about him will be safeguarded by law. The personal data must be recognisable as belonging to a specific individual.([47])

Any individual who processes data, whether they are a natural or legal person, is subject to the PDPA as a data controller. The term "processing" is defined in Section 3 as:

"Analysis of personal data, whether by automated means, such as obtaining, recording, or holding the data or carrying out any analysis on personal data, including:

(a) organization, adaptation, or alteration of the personal data;

(b) retrieval or use of the data; or

(c) alignment, combination, blocking, erasure, or destruction of the data."

This definition includes analysis of personal data, whether by automated means, such as obtaining, recording, or holding the data or carrying out any analysis on personal data. For this reason, the term "processing" has a broad definition. Both the processing and the management of the data following processing are included in the processing of personal data, which can be done manually or by automated means.

In the employment context, unlike the GDPR – which is considered as the standard data protection law globally, the PDPA does not have any provision that specifically provides for protection of employees' personal data. As aforementioned, the PDPA is more of a multi-sectoral legislation, covering various actors, and aspects of personal data protection in Tanzania. Garnering inspiration from the working party opinion 2 of 2017 on *protection of personal data in the employment context* (Article 29 Working Party),([48]) it is important to analyse how the data protection conditions enshrined in the PDPA and its subsequent regulations outlines the employees' risks to personal rights posed by new technologies, balancing the employees' rights and the employers'

([46]) The Personal Data Protection Act, [CAP 44, 2022].

([47]) The Personal Data Protection Act, [CAP 44, 2022]; K. Hassan, *Personal data protection in employment: New legal challenges for Malaysia, op. cit.*, 699.

([48]) Article 29 Working Party, *Opinion on the Processing of Personal Data in the employment* (Brussels, 2014)

legitimate expectation to process personal data through human resource management.([49])

5.2 Data Processing in Employment

In the spirit of section 15 and 96 of the ELRA that provides for the particulars that must be recorded by employers with respect to their employees, it can be sufficient to note that in the employment context, sensitive data is the kind of data processed. For the purposes of data processing at workplaces, the PDPA and its regulations do not explicitly provide for the rules or exemptions from the prohibition on processing sensitive data in employment. Comparatively, the EU's implementation of the GDPR, which includes provisions on the processing of personal data in the context of employment and to provide for special regulations, procedures or guidance notes in this regard, offers best practices that can be applied.([50]) With regards to workers and their employers, it becomes clear that the only way forward towards protection of personal data processed in the workplace is by compliance with the data protection conditions and requirements in the PDPA.

Consent: The essential condition and prerequisite in processing of personal data in an employment or work context is the employee's consent. Before the employer or management can process or disclose any personal data about him, he or she must provide consent. The concept of "consent" under the PDPA remains ambiguous due to the absence of a clear definition within the legislation. This lack of definitional clarity represents a significant shortcoming of the PDPA. It is not clear whether "constructive consent" is acceptable, or does it only refer to "express consent." This difference raises consent to be a contentious and debatable issue in Tanzania. The High Court of Tanzania has in some cases regarding the right to privacy and protection of personal data acknowledged the requirement of consent before processing or disclosing personal data.([51]) For example, in the recent case of *Safari Automotive Limited v. Godwin Danda*,([52]) the High Court held the appellant liable to pay general damages for publishing a video clip of the respondent on social media platform without the Respondent's consent as the appellant's act was considered to interfere with personality and their right to privacy without justification. Although the judgement does not make any reference to the PDPA as it was not in force at the time of the institution of the case, the judgement

([49]) C. Ogriseg, *GDPR and Personal data Protection in the Employment Context, op. cit.*

([50])Article 88 of the GDPR, allows Member States to establish specific rules for processing employee data in the employment context, including best practices and guidance, to ensure the protection of rights and freedoms. See, Art. 88 GDPR – Processing personal data in the context of employment. Available at: https://gdpr-info.eu/art-88-gdpr/ (Accessed on 17th March 2025).

([51]) These cases include *Tito Magoti v. Attorney General,* (Misc. Civil Cause No. 18 of 2023) [TZHC 2024]; *Safari automotive Limited v. Godwin Danda,* (Civil appeal no. 978 of 2024) [2024] TZHC; *Deogras John Marando v. Managing Director, Tanzania Beijing Huayuan Security Guard Service Co. Ltd*, Civil Appeal No. 110 of 2018 [HCTZ, 2019]

([52]) *Safari automotive Limited v. Godwin Danda,* (Civil appeal no. 978 of 2024) [2024] TZHC

stands as a landmark decision on the requirement for 'consent' in personal data protection in Tanzania.([53])

On the other hand, it is contended that an employee has granted his consent if he is informed that his personal data is being processed or disclosed and he does not object to the same. Arguably, since the processed employee personal data are mostly 'sensitive in nature', the authors opine that explicit consent is necessary as required by the PDPA for sensitive personal data. For instance, in a recent Kenyan case of *Catherine Kainyu Murithi v. Becton Dickinson & Company (BD East Africa) & Safaricom PLC*,([54]) a former employee lodged a complaint against BD East Africa and Safaricom, alleging that her employer unlawfully shared her national ID with Safaricom, facilitating an unauthorized transfer of her mobile number without consent. The ODPC ruled in her favour, citing violations of Kenya's Data Protection Act, 2019, and issued strict compliance orders.([55])

But can consent only legitimise data processing in the employment context? Noting from Article 29 Working Party *Opinion 2/2017,* consent alone cannot legitimise processing of data in the context of employment because of the nature of an employment relationship. For instance, the Hellenic Data Protection Authority (DPA) in Greece imposed a 150,000 Euros fine to Pricewater House Coopers Business Solutions SA (Pwc Bs) investigated the lawfulness of the processing of personal data of its employees.([56]) The DPA found that PWC BS unlawfully processed employees' data, using an inappropriate legal basis – "consent", and in an unfair and non-transparent manner.([57]) The DPA also found that PWC BS failed to demonstrate compliance with Article 5(1) of the GDPR and violated the principle of accountability by transferring the burden of proof of compliance to the data subjects. The company was found to have violated the GDPR's provisions of Article 5(1)(a) and Article 5(2).([58]) The GDPR incorporates the long-held view of the European regulators that consent to processing in the context of a contractual employment relationship cannot be considered as freely given, due to the clear imbalance between the parties.

([53]) FB Attorneys, *High Court Pronounces Landmark Decision on Instagram Video,* 7th August 2024.

([54]) *Catherine Kainyu Murithi v. Becton Dickinson & Company (BD East Africa) & Safaricom PLC*, ODPC Complaint No. 1958 of 2024 (Kenya).

([55])The ODPC Complaint No. 1958 of 2024's ruling sheds light that personal data cannot be shared, transferred, or processed without explicit consent from the data subject. Employers must ensure that all employees understand and agree to how their data is used, especially post-employment. Employers must audit their data handling practices and employees must be aware of their data rights and speak up when violated.

([56]) European Data Protection Board (EDPB), Company fined 150,000 euros for infringements of the GDPR. Available at: https://rb.gy/wmq8g5

([57]) The DPA considered that PWC BS has processed the personal data of its employees in an unfair and non-transparent manner contrary to the provisions of Article 5(1)(a) indent (b) and (c) of the GDPR giving them the false impression that it was processing their data under the legal basis of consent pursuant to Article 6(1)(a) of the GDPR, while in reality it was processing their data under a different legal basis about which the employees had never been informed.

([58])Under the GDPR, consent must be actively and freely given to be a valid basis for data processing and so this historic approach is problematic.

Furthermore, given the usual dependence of the employment relationship, which never places workers in a position to freely offer, decline, or revoke consent, employees' assent may scarcely legitimise the processing of personal data.([59]) Because of the unequal negotiating power between the parties, an employee may be forced to consent, making reliance on consent as a legal basis for processing their data discouraged in the context of an employment relationship.([60])

In the alternative, as argued above in section **Errore. L'origine riferimento non è stata trovata.**, the available legal basis on processing personal data in the employment context may at a large extent be through performance of the "employment contract" – to meet the obligations under it such as processing of personal data for payment of renumerations, or for obtaining sick leave. The use of an employment contract could fit as a lawful basis for processing of employee's personal data since the employee shall have genuine free will and will be able to withdraw their consent without any detriment where the clause allows for the same.([61])

Legitimate Interest: The requirement under the ELRA for employers to keep and maintain employee records constitutes one of the legitimate bases for employers' processing of personal data. The processing of personal data in the workplace according to Article 29 of the Working Party must be legitimate and should be carried out in the least invasive way feasible and concentrate on the particular risk area. This would necessitate the employer as a data controller to imply proportionality and necessity of personal data during processing by limiting the amount of personal data collected to what is necessary for the intended purpose, applying available technologies for data avoidance and minimisation, and being able to demonstrate the relevance of the personal data during the processing.([62])

Transparency: Despite there being a legal basis, whether through consent or a legitimate interest, the transparency concept must be followed in all processing procedures. Workers must constantly communicate well and be properly informed. "Involving the data subject to choose how much of his personal data is handled by providing him with information." is what the WP29 suggests doing.([63]) Should the information or notice be in writing? The authors contend that written notification is not required though it is recommended for the sake of evidence as garnered from the *Safari automotive Limited v. Godwin Danda,*([64]) case.

On the other side of the coin, despite processing of personal data being required to be transparent, employee consent is required before any third party can access data

([59])Article 29 Working Party, *Opinion on the Processing of Personal Data in the employment* (Brussels, 2014)

([60])Business Daily, *Limits of employers on staff data privacy rights.* Business Daily (18th Sept. 2020).

([61])*Ibid,* note 53.

([62]) Regulation 28 of the Personal Data Protection (Personal Data Collection and Processing) Regulations, GN No. 449C of 2023

([63]) Article 29 Working Party, *Opinion on the Processing of Personal Data in the employment* (Brussels, 2014)

([64]) *Safari automotive Limited v. Godwin Danda,* (Civil appeal no. 978 of 2024) [2024] TZHC

that is not needed for its intended use. What matters is the disclosure's intended use. Unless an employee has granted consent for his data to be disclosed for purposes other than those for which it was originally intended, neither management nor the employer may disclose information for more than the intended purpose.

Security of personal data: During data processing, the management is responsible for making sure that no data are mistakenly accessed, lost, altered, destroyed, or abused. The security of employee data is guaranteed by this criterion. Since most management tasks are now completed electronically in the ICT era, data is vulnerable to viruses and cyberattacks. As a result, management needs to guarantee the best possible protection for employee data.([65]) Section 27 of the PDPA imposes stricter rules with regards to the security aspects in the processing of personal data. An employer is thus responsible for ensuring that adequate security measures are in place to protect the employees' data in their control. Practically, employees' personal files, in manual or electronic forms should be kept in securely locked cabinets and electronic databases or cloud storages. Furthermore, employers would be obliged to also ensure that, in a situations of outsourcing HR functions, a third party concerned takes reasonable steps to put in place security measures that protect personal data.([66])

Like a security guard at a bank, a data protection officer within an organisation, company or institution would be crucial for implementing security measures to protect sensitive personal data and ensuring compliance with data protection laws.([67])For instance, in a Tanzanian healthcare organization, the data protection officer oversees data protection policies, ensuring patient data is secure and processed in compliance with the PDPA. They also conduct risk assessments and liaise with regulatory authorities to prevent breaches.

5.3 Rights of employees as data subjects

Employees are among the data subjects recognized by the PDPA, bearing its multi-sectoral coverage and application. Part Six (VI) of the PDPA grants employees some rights that align with the previously discussed data protection principles. The employee has a right to their data, and the employer is obligated to respect both rights. The PDPA provides for the following rights for employees in respect of processing their personal data:

([65]) Section 27 of the Personal Data Protection Act, [CAP 44, 2022]; Article 29 Working Party, *Opinion on the Processing of Personal Data in the employment* (Brussels, 2014)

([66])Section 27 of the Personal Data Protection Act, [CAP 44, 2022] read together with Regulation 27 of the Personal Data Protection (Personal Data Collection and Processing) Regulations, GN No. 449C of 2023.

([67]) Section 27 (3) of the Personal Data Protection Act, [CAP 44, 2022].

(i) Employees' right to access their personal data (section 33 of the PDPA);

The possibility for the data subject to access and update their personal information must be provided. This approach to employment law is groundbreaking. Employees are typically not granted access to their personal files. Will the employer permit access to the office file even though it contains the employees' personal information? Would the employer also grant password access to an employee whose employee data are kept in electronic files? It would be fascinating to observe if this access right will suddenly grant employees access to their personal files and the data within under the PDPA.([68])

What "access" means and its scope under the PDPA is that the employee should be informed by the employer when their personal data is being processed by the employer themselves or on their behalf, to be provided with a description of the processed personal data and the recipients of the processed personal data.([69])However, the employer is not required to inform the employee where the personal data is involved in any investigation pursuant to the law, not accurate or prohibited by a court order.([70])

(ii) **Employees' right to have their personal data corrected or rectified (section 38 of the PDPA);**

Personal data must be true, complete, current, and not misleading. In other words, accurate. The information that the employer receives determines how accurate the data is. It is unlikely that the employee will experience harm or distress if the data is wrong when it is received. Nonetheless, it is the employer's responsibility to make sure that inaccurate data are promptly updated. Where the personal information is not updated or corrected, the employee has the right to apply to the PDPC requesting for the correction or rectification of their personal data. The PDPC may act by ordering the employer as a data controller to rectify or correct the inaccurate personal data.([71]) Upon rectification of the same, the employer will still be obliged to notify third parties that may had access or were disclosed with the inaccurate personal data of the rectification or correction of the personal data.

It is crucial that employees should be proactive in managing their personal data to ensure it remains accurate, complete, and current. This includes regularly reviewing their personal data that is maintained by their employer. It also includes checking for any errors or omissions in their records, such as incorrect addresses, names, or other

([68]) K. Hassan, *Personal data protection in employment: New legal challenges for Malaysia, op. cit.*, 699.
([69]) See, Section 33 of the Personal Data Protection Act, [CAP 44, 2022]
([70])Ibid, note 52.
([71])See, Section 38 (1) (3) of the Personal Data Protection Act, [CAP 44, 2022]

identifying information. If any discrepancies are found, employees have the right to submit a correction request to their employer.

In cases where the employer fails to update or correct the inaccurate data, employees can escalate the matter by applying to the PDPC for rectification. As aforementioned, the PDPC has the authority to order the employer to correct the data if it is found to be inaccurate. This process reinforces the importance of employees being vigilant about their personal data and understanding their rights under the PDPA.

(iii) Employees' right to prevent the collection and processing of data that would likely affect them;

This complies with the employer's ethical obligation. For instance, erroneous information will surely damage an employee's reputation and impact both their current and future careers, particularly if the information is harmful to them. In such situations, the employee has a right to require the employer through the procedures provided in the Personal Data Collection and Processing Regulations([72])to suspend or not to begin, processing of any personal data in respect of which the employee is a data subject, and such processing would cause substantial damage or affect him or another person.

(iv) Employees' right to prevent the processing of personal data for direct marketing purposes (section 35 of the PDPA);

Pursuant to section 35 of the PDPA, employees have the right to prevent the processing of personal data for direct marketing purposes. The provision thereby prohibits such processing unless the individual has given explicit consent. In practical terms, this implies that if an employer or any data controller wishes to use an employee's personal data for marketing purposes, they must first obtain clear permission or consent. If an employee withdraws consent, the employer as a data controller must cease processing immediately.

In the case of *Safari automotive Limited v. Godwin Danda,*([73])as aforementioned, the High Court ruled in favour of the respondent who had complained in the sub-ordinate court that the appellant had interfered with his personality and privacy by publishing a video of the respondent on their Instagram account for marketing purposes and promoting their services and products without his consent. The Court noted that, even though the appellant argued that the respondent had consented to the recording of the video, there was no explicit evidence tendered to prove that the respondent had consented for it to be posted on Instagram. The consent of the respondent for the video

([72]) Regulation 17 of the Personal Data (Personal Data Collection and Processing) Regulations, 2023 provides for the necessary procedures.

([73]) *Safari automotive Limited v. Godwin Danda,* (Civil appeal no. 978 of 2024) [2024] TZHC

to be recorded did not extend to posting the same on Instagram, which interfered with his family and employment. (74)

Comparatively, in Kenya, a common law jurisdiction like Tanzania, and a neighbouring East African country, the Kenyan Data Protection Commission (OPDC) in *Edith Andeso v. Olerai Schools Limited*,(75) dismissed the complaint upon determining that the complainant had knowledge of the purpose and context in which the photos taken and posted on the School's Facebook page were to be used and by her clear affirmative consent to the processing of her personal data by the school. The cases therefore emphasize on the necessity of consent in data processing, especially for marketing purposes. Similarly, in *Deogras Marando v. Managing Director, Tanzania Beijing Huyuan Security Guard Service Co. Ltd,* the Court reinforced the former employee's right to control their personal data, highlighting the legal obligation of data controllers to respect these rights.(76)

(v) Employees' right to notice of automated processing (section 36 of the PDPA);

Employees in any company, institution or organisation now have the right to not be subjected to automated systems if such decisions significantly impact them. This opens the doors for employees to request that the automated decisions be reviewed by a human. For instance, if an automated system determines employee promotions or terminations, employees may demand a reassessment by a human. But does the same apply to job applicants at the same organisation, company, or institution? Arguably as data subjects, yes. Even though the PDPA does not mention employees or job applicants perse, from the definition of a data subject in the PDPA,(77) and the principle of fairness and transparency, the right could extend to recruitment stages where in some jurisdictions, Artificial Intelligence is used for screening and shortlisting candidates. This right stands as a cornerstone to prevent potential biases and ensure that all data subjects, regardless or employee or job applicant status are subject to fairness in automated decision making.

For example, if an automated system determines employee promotions or terminations, employees may demand a reassessment by a human. However, this position is not absolute. It does not apply or hold any waters if the automated decision was necessary for entering into or performing a contract between an employer and the employee. Does this cure the wound or further adds salt to the wound? We argue that,

(74) *Safari automotive Limited v. Godwin Danda,* (Civil appeal no. 978 of 2024) [2024] TZHC at page, 5-8.

(75) *Edith Andeso v. Olerai Schools Limited,* (OPDC Complaint No. 725 of 2023).

(76) *Deogras John Marando v. Managing Director, Tanzania Beijing Huayuan Security Guard Service Co. Ltd*, Civil Appeal No. 110 of 2018 [HCTZ, 2019]

(77) A 'data subject' is defined as a subject of personal data processed under the Act. This can be anyone, including employees or job applicants.

except where the employee has consented to such application of automated decisions,([78])an employee's right to not be subjected to automated decisions could potentially be under scrutiny where an employment contract requires their immediate consent with regards to automated decision making that would be involved in the course of employment or during the application process.

Nevertheless, the employer would have to as soon as practicable, notify the employee that the decision was made based on an automated system. ([79])

(vi) Employees' right to erasure and destruction of personal data where it is no longer required;

The employer is required to consider how long the data is retained. Data should not be preserved for longer than is required. Given the length of an employment contract, it is expected that the employer will need to retain the employee's data for an extended period. In fact, section 96(2) of the ELRA requires an employer to keep an employee's record on file for five years following the termination of employee's employment contract. However, as stated in the PDPA, the employer is no longer permitted to retain the employee's personal data if the employee has retired or otherwise stopped his employment. In the ambit of the PDPA, an employee may choose to exercise this right by requesting the PDPC to order the employer as a data controller to erase or destroy the personal data. It is the PDPC that gives the directive to the employer for fulfilling this right, especially where the personal data processed was inaccurate. ([80])

This status quo thus begs the question: will the employer keep retaining the personal data after the end of employment period based on the ELRA, or can the employee jump in and request for erasure or blockage of their personal data based on the PDPA? We submit that, pursuant to the principle of interpretation, the PDPA would likely prevail due to its most recent enactment and specific focus on data protection. The ELRA does not specifically address the erasure of personal data after employment ends. The actual remedy thus falls within the ambit of the PDPA. As the PDPA grants data subjects rights such as access, rectification, and erasure of personal data, employers must comply with data protection requirements such as data minimization, purpose limitation and security measures unless specific exemptions apply, such as legal obligations for the protection of vital interests.

Comparatively, the EU's GDPR also allows individuals to request data erasure or restriction, known as the 'right to be forgotten', unless retention of personal data is necessary for compliance with legal obligations or other legitimate interests.([81]) Similar rights are present in other African jurisdictions with data protection laws, such as South

([78]) See, section 36 (3) (a) – (c) of the Personal Data Protection Act, [CAP 44, 2022]
([79]) See, section 36 (2) (a) (b) of the Personal Data Protection Act, [CAP 44, 2022]
([80]) See, section 36 (3) (a) – (c) of the Personal Data Protection Act, [CAP 44, 2022]
([81]) Recitals 65 and 66 of the GDPR; Article 17 of the GDPR

Africa's POPIA, which also emphasizes data subject rights to access, correct and erase personal data.([82]) In Kenya, the Office of the Data Protection Commissioner (ODPC) recently ruled in favour of Lee Mutunga in his complaint against Milestone Games Limited (SportPesa),([83]) determining that the betting company violated the complainant's right to erasure under Kenya's Data Protection Act by failing to delete his personal data despite numerous requests. The ODPC determined that SportPesa violated the data minimization principle by requiring unnecessary personal information for account deletion and obstructed the investigation by providing misleading information to the Data Commissioner and being uncooperative during a scheduled site visit on February 13, 2025. Consequently, the ODPC ordered SportPesa to pay Mutunga KES 350,000 (approximately USD3,500) as compensation for violating his right to erasure and causing distress, though this was significantly less than the KES 1,000,000 he had requested.([84])

(vii) Employees' right to compensation upon infringement of their privacy rights (section 37of the PDPA);

Pursuant to section 37 of the PDPA, data subjects are granted the right to compensation for damages resulting from violations of the PDPA. This right ensures that individuals can seek redress if their personal data is mishandled, leading to harm or loss.([85]) For instance, consider an employee whose sensitive personal data, such as health records, is improperly disclosed by their employer without consent, causing emotional distress or reputational damage. Subject to the right to compensation, the employee can claim compensation for these damages.

Just as a customer can seek compensation if a product causes harm due to a manufacturer's negligence, employees can claim damages if their data is mishandled, reflecting the PDPA's role in safeguarding personal data rights.

5.4 The Data Protection Officer

One of the most recent significant requests made by the PDPC is the requirement for a mandatory DPO at the workplace or within organizations, institutions, and companies in compliance with the PDPA and its regulations. This person would perform their duties autonomously and serve as a point of contact for employers, employees, and the relevant data protection authority. The DPO is a crucial component of any data protection law. Schaar does, however, emphasises that the DPO

([82]) The Personal Information and Protection Act (POPIA)

([83]) *Lee Mutunga v. Milestone Games Limited T/A SportPesa,* ODPC Complaint No. 1899 of 2024.

([84]) The determination highlights the serious consequences for companies that fail to respect data subjects' right to erasure and attempt to obstruct regulatory investigations, with both parties having thirty days to appeal the decision to Kenya's High Court.

([85]) The Personal Data Protection Act, [CAP 44, 2022]

must collaborate closely with employee representatives and have greater protection from employers' capricious behaviour. ([86])

In the EU, the DPOs at the workplace have been in demand and covered with dismissal protection, making a DPO not subject or bound to their employer's instructions, and without employees' representatives' participation or information.([87]) However, in the Tanzanian context, the PDPC explains through its website and training conducted to DPOs that a DPO must also handle employee personal data and act as a point of contact for any issues that arises. According to the PDPC, every organisation must have two DPOs. One of them can be an accounting officer, executive director, director general, or managing director of the company – who reviews all reports that the commission requests.([88]) As much as the requirement for a DPO at the workplace could make it easier for staff members to uphold the basic right to privacy, unlike in the EU, it is yet not stated if the DPO under the Tanzanian data protection legal framework is protected or covered with dismissal protection. Arguably, a dismissal of a DPO as an employee on account of fulfilling his statutory duty would amount to unfair termination or an employer may be challenged for unfair labour practice. Such dismissal would not meet the threshold of a fair and valid reason for the dismissal to be considered fair under the ELRA. This open caveat for a challenge on unfair labour practice by an employer could provide a certain level of protection to DPOs as employees.

Nevertheless, it potentially becomes tricky for an appointed DPO to be shielded from any form of employer's capricious tendencies. Perhaps covering employees from dismissal should be considered by the legislator or the PDPC with respect to appointed DPOs in an organisation.

6. 'Sensitive Personal Data' in connection with employment

Information about employees can be regarded as "sensitive personal data." Any personal information that includes details about a data subject's physical or mental health, political opinions, race, religious beliefs, or criminal history is referred to as "sensitive personal data."([89]) The management or employer keeps a record of this information in employment files as required under section 96 of the ELRA. The general principle mandates that the employer, as the data controller, must process sensitive personal data in compliance with PDPA.

([86]) P. Schaar, *Die geplante EU-Datenschutz-Grundverordnung, Auch beim Beschäftigtendatenschutz ist ein Nachbessern erforderlic*h, in *Computer und Arbeit*, 3, 2013.

([87]) P. Schaar, *"Die geplante EU-Datenschutz-Grundverordnung, op. cit.*

([88]) See, PDPC, Data Protection Officer. https://pdpc.mikutano.co.tz/en/protection/data-protection-officer/

([89]) Section 3 of the Personal Data Protection Act, [CAP 44, 2022]

As per the PDPA in processing of personal data, a data subject's 'explicit consent' is necessary before the data can be managed.([90]) The 'explicit consent' of the data subject is required before the data can be processed. There is no definition of 'consent' in the PDPA, but it is submitted that 'explicit consent' should mean written consent as provided in section 30 of the PDPA. However, attention should be paid to section 30 (1) of the PDPA which provides that the requirement for a written consent shall not apply where the processing is necessary for the purpose of compliance of any written laws. Does this infer that processing of sensitive personal data occurs automatically in the workplace, without consent? We opine that the employer as a data controller who processes sensitive personal data must satisfy the condition that the processing is necessary for the purposes of compliance with the ELRA in for instance, keeping and maintaining of employees' records.([91]) The requirements to get consent in relation to the processing of personal data is exempted for the purposes of performing an employment contract to which the employee is party. An employer would therefore have to evaluate and determine what information is necessary for the discharge of both the employer and the employees' duties and obligations to avoid any excessive data collection and processing.

It can further be inferred that, the PDPA permits the processing of sensitive personal data for management objectives in the workplace. In that, employers may deal with the employees' sensitive personal information without obtaining their express consent. Even though employers are permitted to manage sensitive personal data about their workers, but they are not supposed to treat employees unfairly based on any information gleaned from this data, including genetic information, disease, physical impairment, or religious beliefs. If there was a drug-use clause in the employment contract, the employer might pursue legal action against the employee where they have contravened with the clause.([92])

7. Conclusion

Tanzania's Constitution has enshrined the right to privacy, first as a freedom and a human right for each individual. Currently, an employee can exercise control over their own personal identity or data processing in accordance with the PDPA. A unique identity that each person develops via their own diachronic identification process. Delineating our individual identities, we travel a route paved with decisions—sometimes clear-cut and deliberate, other times negotiated and subject to revision.

Throughout life, a variety of facts or elements that can constitute a person's identity frequently coexist. The choice of which identity to prioritise in the workplace

([90]) M. Bakar, Y. Mohd, *Data privacy and data protection,* In Petaling Jaya: Sweet and Maxwell Asia, 2002.

([91]) Section 30 (5) (a) of the Personal Data Protection Act, [CAP 44, 2022]

([92])K. Hassan, *Personal data protection in employment: New legal challenges for Malaysia, op. cit.*

should belong to every one of us freely. That kind of choice about standards that pertain to social collective microcosms is made possible by freedom. Data protection acknowledges a control on the accuracy of our "personal hologram," which is periodically defined by the personal information we provide that is gathered and connected by third parties.

In the Tanzanian context, the discussion in this article demonstrates that management, or the employer, now has an additional responsibility to guarantee the appropriate handling of employees' personal data because of the new legislation. The PDPA requires management, as the data controller or processor, to protect employee data in accordance with the Act. It will also be a positive move when data protection for employees is acknowledged as a distinct type of data protection in Tanzania. Employee privacy will be enhanced by a specific guidance note from the PDPC on employee personal data protection and, in many cases, by companies and organisations appointing a DPO in compliance with the law.

References

Albrecht J., *Inofficial Consolidated Version after LIBE Committee Vote Provided by the Rapporteur* (published 22nd of October 2013, accessed July 12, 2024, http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE. pdf)

Article 29 – Data Protection Working Party, *Opinion on the Processing of Personal Data in the Employment Context, Executive Summary*, published 2001, accessed July 18, 2024, http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/files/2001/wp48sum_en.pdf

Article 29 – Data Protection Working Party, *Working document on the Surveillance of Electronic Communications in the Workplace*, published 2002, accessed July 113, 2024, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf

M. Bakar - Y. Mohd, *Data privacy and data protection*, Petaling Jaya: Sweet and Maxwell Asia, 2002

Boshe P., *Data Privacy Reforms in Tanzania*, in *African Data Privacy Laws*, Springer, 2016.

Boshe P., *Interceptions of communications and the right to privacy: Commentary on Zitto kabwe's political saga*, in *Open University Law Journal*, Vol. 4, No. 2:1-5.

Braverman H., *Labor and Monopoly Capital; The Degradation of Work in the Twentieth Century,* NYU Press, 1998.

Busch K., Hermann C., Hinrichs K. und Thorsten S., *Eurokrise, Austeritätspolitik und das Europäische Sozialmodell, Wie die Krisenpolitik in Südeuropa die soziale Dimension der EU bedroht*, Friedrich-Ebert-Stiftung, November 2012, accessed August 4 2024, http://library.fes.de/pdf-files/id/ipa/09444.pdf

Business Daily, *Limits of employers on staff data privacy rights.* Business Daily (18th Sept. 2020).

Clyde & Co, *Tanzania: The Personal Data Protection Act of 2022.* (16th February 2023).

Delbar C. et al., *New technology and respect for privacy at the workplace*, in *European Industrial Relations Observatory,* 2003.

Ebert I., I. Wildhaber & J. Adams-Prassl, *Big Data in the Workplace: Privacy Due Diligence as a Human Rights-Based Approach to Employee Privacy Protection* (2021) in *Big Data & Society* 2021, 8, 1, https://doi.org/10.1177/20539517211013051

Electronic and Postal Communications (Consumer Protection) Regulations, GN No. 61 of 2018

European Data Protection Board (EDPB), Company fined 150,000 euros for infringements of the GDPR. Available at: https://rb.gy/wmq8g5

FB Attorneys, *High Court Pronounces Landmark Decision on Instagram Video,* 7th August 2024.

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law,* Law, Governance and Technology Series, Springer, 2015, DOI https://doi.org/10.1007/978-94-017-9385-8__6

Habinsky J. & H. Boone, *Monitoring and protecting employee privacy*, XpertHR Employment Law Manual, 2022.

Hassan K., *Personal data protection in employment: New legal challenges for Malaysia,* in *Computer Law & Security Review*, Volume 28, Issue 6, 2012, https://doi.org/10.1016/j.clsr.2012.07.006.

Hendrickx, F., *Protection of workers' personal data in the European Union, Two Studies.* University of Leuven/Tilburg, 2002, accessed February 4, 2014, http://collection.europarchive.org/dnb/20070702132253/.

Hirsh E., & G. Olson, *Starting from Marginalized Lives: A Conversation with Sandra Harding*, in *JAC, Journal of Rhetoric, Culture, & Politics*, 1995, accessed August 4 2024, http://www.jaconlinejournal.com/archives/vol15.2/hirsch-starting.pdf

International Labour Organization, "Protection of Workers' Personal Data," Geneva 1997, accessed 2nd of February 2014 http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

Knorr-Cetina, K., *Manufacture of Knowledge*, Oxford, 1981.

Makulilo A., *African Data Privacy Laws*, Springer, 2016.

Mitrou L. M. Karyda, *Employees' privacy vs. employers' security, Can they be balanced?* Elsevire Ltd., 2005.

Mitrou, L, Maria Karyda, *Employees' privacy vs. employers' security, Can they be balanced?* Elsevire Ltd. 2005, accessed February 4, 2014, http://www.icsd.aegean.gr/website_files/metaptyxiako/82038633.pdf

Molè M. – Mangan D., *'Just More Surveillance': The ECtHR and Workplace Monitoring*, in *European Labour Law Journal*, 2023, 14, 694

Molè M., *The Internet of Things and Artificial Intelligence as Workplace Supervisors: Explaining and Understanding the New Surveillance to Employees Beyond Art. 8 ECHR,* in *Italian Labour Law e-Journal*, 2022, 15, 87.

Mujtaba B., *Digital Literacy on Privacy Rights Policies in the American Workplace*, in *Multidimensional and Strategic Outlook in Digital Business Transformation. Contributions to Management Science*. Springer, Cham 2023. https://doi.org/10.1007/978-3-031-23432-3_10

Ogriseg C., *GDPR and Personal data Protection in the Employment Context,* in *LLI*, 2017, Vol 3, No 2.

Olsen C., *To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR,* in *International Data Privacy Law*, 2020, Vol. 10. No. 3.

Personal Data Protection (Personal Data Collection and Processing) Regulations, GN No. 449C 2023

Personal Data Protection Act, CAP 44 2022

Rosemblat A. - T. Kneese - D. Boyd, *Future of Labor: Workplace Surveillance*, in *Data & Research Institute*, 2014.

Schaar P., *Die geplante EU-Datenschutz-Grundverordnung, Auch beim Beschäftigtendatenschutz ist ein Nachbessern erforderlic*h, in *Computer und Arbeit* , 2013, 3.

PM. Schwartz - KN. Peifer, *Transatlantic data privacy* (November 7, 2017), in *The Georgetown Law Journal*, 2017, 106-115, UC Berkeley Public Law Research Paper. Available at SSRN: https://ssrn.com/abstract=3066971.

Swell G., *Nice Work? Rethinking Managerial Control in an Era of Knowledge work,* Organization 2005, 12, 685.

Ubena J., *Privacy - a forgotten right in Tanzania.* Tanzania Lawyer, I/2JTLS 2012, 72-114

Wahlgren P., *Information and Communications Technology Legal issues: Data protection and Privacy*, in *Scandinavian studies in law*, 2010.