



## Safeguarding Digital Labour: Data Protection for Platform Workers

By Hilda Mwakatumbula<sup>1</sup>, Lilian Sylvester<sup>1</sup>, Goodiel Moshi<sup>2</sup> & Daniel Arubayi<sup>3</sup>  
REPOA<sup>1</sup>, University of Dodoma<sup>2</sup> & Oxford University<sup>3</sup>

### Key Messages

- The digital revolution, coupled with the rise of the gig economy has transformed the way work is understood and performed globally.
- The gig work—temporary and flexible jobs offered by online platforms—has become increasingly prominent in Tanzania as it is in other parts of the world.
- Gig platforms in Tanzania offer opportunities but also raise data protection concerns due to the extensive collection of personal data from drivers and customers.
- As more Tanzanians venture into gig work, data protection becomes paramount.

### Gig Economy in Tanzania

In recent years, Tanzania has experienced a surge in gig work. Gig work refers to the use of mobile apps or website marketplaces to connect individuals providing services with customers. On the one hand, this rising trend can be attributed to increased internet penetration, smartphone usage, and urbanization. For instance, as of March 2023, the number of internet users in Tanzania surpassed 33 million, with the country witnessing an average internet subscription growth rate of 17 percent annually over the past five years. This remarkable growth can be attributed to several government initiatives aimed at improving digital infrastructure, increased competition among mobile operators, and support for local innovators to create localized content.

On the other hand, a study by the World Bank revealed that more than 80 percent of individuals engaged in gig work are motivated by prospects of earning extra income, better pay, and enjoying flexible working hours<sup>i</sup>. As a result, many who are unemployed or underemployed now prefer working on platforms such as ride-hailing and delivery services. These platforms present enhanced economic empowerment opportunities, enabling individuals to earn income flexibly. To function effectively, these platforms collect vast amounts of data from both consumers and service providers, including personal information, work histories, location data, and payment details. This policy brief reviews data protection issues in the context of the

gig economy. It is based on the review of data protection policies and framework, and a study conducted in Tanzania by REPOA in partnership with FAIRWORK from the University of Oxford between June and July 2023.

At the time of this writing, many gig platforms in Tanzania seems to operate without regulatory oversight in accordance with data protection principles and standards. This leaves room for potential abuse and exploitation of workers' and users' data.

### Data Protection

As with many digital operations, gig platforms are susceptible to data breaches, interception and misuse. For gig workers, a breach could lead to financial losses, identity theft, or even personal security threats, especially for those who rely on these platforms as their primary source of livelihood. For instance, in October 2016, Uber experienced a significant data breach that affected 57 million customers and drivers. The data exposed included names, email addresses, and phone numbers of customers, while over 600,000 U.S. driver's license numbers were compromised<sup>ii</sup>. In another incidence, in September 2019, DoorDash (the delivery App) confirmed a data breach affecting approximately 4.9 million customers, delivery workers, and merchants. The breach exposed data such as names, email addresses, delivery addresses, and hashed (encrypted) passwords. In some cases, the last four digits of payment cards and bank account numbers were accessed by unauthorized parties.

Also, Gig platforms often use algorithms to match workers with jobs. Without proper oversight, there's potential for these algorithms to make biased decisions or violate users' privacy, especially if they're making determinations based on sensitive data.

Furthermore, the global nature of the digital economy means that a significant percentage of platforms in Tanzania might have origins outside the country or might operate cross-border. This introduces complexities in data governance, as different countries have different standards and regulations. Without a clear data protection framework in Tanzania, there's a risk that these platforms could lead to more lenient data standards, potentially compromising Tanzanian users' data. Clear guidelines ensure that regardless of the platform's origin, they are obligated to adhere to Tanzania's data protection principles.

## Continental & Regional Data Protection Frameworks

Several initiatives have been undertaken in the African continent to establish a harmonized data governance framework. These efforts aim to assist countries in easily adapting to the ever-changing data mechanisms. The Malabo Convention, an African Union convention on Cybersecurity and Personal Data Protection, came into force on 8th June 2023<sup>iii</sup>. It is the only other enforceable continental data protection treaty outside the European Union's General Data Protection Regulation (GDPR). The Convention lays down six principles for processing personal data: consent and legitimacy of personal data processing; lawfulness and fairness of personal data processing; purpose, relevance, and storage of processed personal data; accuracy of personal data; transparency of personal data processing; and confidentiality and security of personal data processing. Besides these principles, the Convention also emphasizes the structure and powers of National Data Protection Authorities, data subject rights, and guidelines on international data flows and localization. The Malabo Convention aligns with many principles found in the GDPR and Europe's Convention 108 related to personal data protection.

Despite the forward-thinking facets of the Malabo Convention, significant developments have occurred since its inception on 27 June 2014, including a substantial shift towards cloud services, platformization, and big data. In 2022, the African Union introduced a continental data policy framework, drawing upon other initiatives like the African Common Free Trade Agreement (AfCFTA)<sup>iv</sup>, Smart Africa – Digital ID<sup>v</sup>, and the Policy and Regulation Initiative for Digital Africa (PRIDA) - Data Protection and Data Location track. This framework adopts a more expansive approach, addressing both personal and non-personal data protection issues. It is guided by principles such as

cooperation, integration, fairness and inclusiveness, trust, safety and accountability, sovereignty, comprehensive and forward-looking perspectives, and integrity and justice. These continental data protection efforts shape how nations, including Tanzania, address personal data protection.

## Legislative Framework for Tanzania's Data Protection Framework

As the digital world evolves, nations are tasked with protecting both their citizens and their economic interests. For Tanzania, this includes addressing the specific needs of its growing digital economy. An essential step towards achieving this is implementing a comprehensive legislative framework tailored to the real needs of digital workspaces.

The Personal Data Protection Act No. 11 of 2022, enacted in Tanzania to safeguard individuals' right to privacy and data security<sup>vi</sup> applies to both public and private entities handling personal data. The Act sets specific requirements for lawful and transparent data collection and processing, ensuring accuracy, security, and limited data transfer outside Tanzania.

Businesses are directly impacted, as they must secure and manage personal data, including staff, customers, and account holders, using encryption and other protective measures. The Act establishes the Personal Data Protection Commission to oversee compliance, register data collectors and processors, and address data protection complaints.

As per the Act, data can only be disclosed with consent, when required by law, for the intended purpose, or for public interest. Data subjects have rights such as access, rectification, objection to automated decision-making, and compensation.

The Act emphasizes limiting data collection, managing third-party risks, and appointing Personal Data Protection Personnel/Officers within organizations. Penalties for data breaches are further outlined, including fines and imprisonment for individuals or corporate bodies found guilty of unauthorized data disclosure or destruction.

To build trust, organizations are mandated to inform consumers about data practices, allow access and correction of personal data, and protect it with adequate security measures. However, there are concerns, such as ambiguity in provisions related to commercial advertising and the lack of clear procedures for handling data breaches, which may require further clarification in the future.

In 2023, post the enactment of the Act, two significant regulations were introduced. First, the Personal Data Protection (Complaints Settlement Procedures) Regulations, detailing the complaint resolution process

for breaches of personal data protection in Tanzania. Second, the Personal Data Collection and Processing Regulations, sets guidelines for registering data controllers and processors, upholding the rights of data subjects, and transferring personal data outside the nation.

## Why is data protection awareness important for gig workers

The study revealed that most gig workers are unaware of the data protection policies on their platforms. Additionally, over half of the thirteen platforms examined could not provide evidence of having such policies in place, thereby increasing the risk of data breaches. Therefore, it's crucial for gig workers to have a sound understanding and awareness of data protection legislations because of:

	<p><b>Access to personal data</b></p> <ul style="list-style-type: none"> <li>Gig platforms collect vast amounts of personal data. Drivers, for instance, might have access to a passenger's name, phone number, and address. This information can be misused if not properly secured.</li> </ul>
	<p><b>Data rights and ownership</b></p> <p>Gig workers may not be clear on who owns the data they generate while working. For instance, does a ride-share driver have any rights to the route data, or does it solely belong to the platform?</p>
	<p><b>Cybersecurity risks</b></p> <p>Gig workers often use personal devices for work, which may not have the same security measures as company-provided devices. This makes them more vulnerable to cyber-attacks or data breaches.</p>
	<p><b>Data retention and deletion</b></p> <p>Gig workers might not know how long their data is retained on these platforms or how to request its deletion. They may also be unaware of what happens to their data once they stop using the platform.</p>
	<p><b>Cross-border data transfers</b></p> <ul style="list-style-type: none"> <li>Many gig platforms operate globally. This means data can be transferred across borders, potentially to countries with laxer data protection standards, posing the danger of data breach.</li> </ul>
	<p><b>Regulatory ambiguity</b></p> <ul style="list-style-type: none"> <li>Gig workers often fall into gray areas in terms of employment classification. They're not always considered employees, which can lead to uncertainties regarding their rights under data protection laws.</li> </ul>
	<p><b>Consent issues</b></p> <ul style="list-style-type: none"> <li>While gig platforms typically have terms of service that users must agree to, workers might not fully understand the extent to which their data is being used, shared, or sold.</li> </ul>

## Recommendations

Given Tanzania's implementation of the Data Protection Act and two associated regulations, the following recommendations are essential to safeguard a secure and resilient gig economy ecosystem:

**First, it is vital to empower gig workers to be conversant with data protection regulations and data privacy policies.** For many gig workers in Tanzania, the immediate concern is often daily income rather than the nebulous concept of data protection. However, these concerns are deeply intertwined. The misuse of data can lead to lost job opportunities or unfair treatment on these platforms. For instance, a platform could unfairly restrict a worker's access based on biased algorithms or inaccurate data. Thus, empowering gig workers is crucial. Gig workers must be educated about the importance of data protection, their rights, and methods to protect their data. This can be facilitated by non-governmental organizations, workers' unions, or even the platforms themselves.

**Second, platforms should adhere to the Data Protection Act and be accountable to ensure the**

**safety of its users by developing and enforcing data privacy policies.** Digital platforms operating in Tanzania have a legal responsibility to protect user data as stipulated by the Act of 2022. Further, they can adopt to global data protection standards, benchmarking themselves with best practice. Essential to this is a clear data usage policy, and transparency in data practices, including how breaches are addressed. These are pivotal in building and maintaining users' trust. Thus, Tanzanian platforms should prioritize data protection, considering the changing legal and regulatory landscape in the country pertaining to personal data protection and privacy.

**Third, raising awareness about Data Protection Act and reviewing the legal and regulation framework to incorporate data protection regulations for gig workers.** Tanzania's burgeoning gig economy, heavily reliant on technology, necessitates tailored data protection regulations for gig workers. Given that a significant portion of digital platforms in Tanzania operate across borders or have foreign origins, it's crucial to address potential data governance complexities to ensure users' data is not compromised and are adequately legally

protected. Without comprehensive data protection regulations specific to the gig economy, the Tanzanian government can neither safeguard the data of its citizens, both workers and customers, nor bolster the credibility of digital platforms operating within its borders. Such regulations would position Tanzania as a leader in digital transformation and data protection in Africa.

**Fourth, incorporating feedback is crucial for platforms to improve safety on digital platforms.** Platforms should actively involve gig workers in the decision-making process, especially concerning how their data is used. This fosters a sense of ownership and allows platforms to better understand the concerns of their user base.

## Conclusion

The rise of the gig economy in Tanzania presents both opportunities and challenges. While it has the potential to uplift many from unemployment and underemployment, it also exposes them to new risks in the digital age. Protecting gig workers is not just about ensuring they get paid but also about safeguarding their data and, by extension, their dignity, identity, and security. As Tanzania continues to grow and evolve in the digital space, raising awareness of newly enacted Data Protection Act and its subsequent regulations will be key to ensuring that digital growth benefits everyone equitably. Specifically, policy makers and regulators need to consider the unique challenges posed by the gig economy and update data protection regulations accordingly.

## A collaboration between:



Berlin Social Science Center

## Funders:

This policy brief arises from research funded by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), commissioned by the German Federal Ministry for Economic Cooperation and Development (BMZ).



Bundesministerium  
für Wirtschaft  
und Klimaschutz



### REPOA Resource Centre

Our Resource Centre provides a good environment for literature research, quicker, easier access and use of knowledge and information. It has full internet connection for online library to support Master's & PhD candidates, researchers and academicians with free access to latest journals, books, reports, webcasts, etc.

### Opening Hours

Tuesday to Thursday from 10:00am to 1:00pm, 2:00pm to 05:00pm.

Friday 10:00am - 01:00pm

The online library opens 24 hours.



### REPOA HQs

157 Migombani/REPOA streets, Regent Estate, PO Box 33223,  
Dar es Salaam, Tanzania.

Tel: +255 (22) 2700083 Cell: +255 78 455 5655

Website: <https://www.repoa.or.tz>

Email: [repoa@repoa.or.tz](mailto:repoa@repoa.or.tz)

### Branch Office

2<sup>nd</sup> Floor Killimo Kwanza Building  
41105 Makole East, Kisasa,  
Dodoma, Tanzania

### @REPOA 2024

Findings and opinions expressed are those of the author(s) and do not necessarily reflect the views or policies of REPOA and any of her partners.

<sup>i</sup> <https://www.worldbank.org/en/topic/jobsanddevelopment/publication/online-gig-work-enabled-by-digital-platforms>

<sup>ii</sup> <https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data>

<sup>iii</sup> <https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/>

<sup>iv</sup> <https://www.eac.int/about-eac>

<sup>v</sup> <https://smartafrica.org/wp-content/uploads/2020/12/BLEUPRINT-SMART-AFRICA-ALLIANCE-%E2%80%93-DIGITAL-IDENTITY-LayoutY.pdf>

<sup>vi</sup> <https://oagmis.agctz.go.tz/portal/acts/237>