

Gender & Policy

Assessment of the Data
Protection and Privacy Act,
2019 compliance with the AU
Data Protection Framework 2022

REPORT-2023



APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS



WOMEN OF UGANDA NETWORK

TABLE OF

Content

1.0 INTRODUCTION	03
2.0 THE ANALYSIS OF THE DATA PROTECTION AND PRIVACY ACT 2019	06
3.0 INTERPRETATION OF THE OF THE DATA PROTECTION AND PRIVACY ACT 2019	07
4.0 PRINCIPLES OF DATA PROTECTION AND PRIVACY	08
5.0 FUNCTIONS OF THE DATA PROTECTION OFFICE	09
6.0 THE DATA GOVERNANCE MANDATE OF STAKEHOLDERS/ OPPORTUNITIES AND RECOMMENDATIONS FOR LOCALIZATION OF THE AFRICAN UNION DATA PROTECTION FRAMEWORK 2022.	10
7.0 CONSENT TO COLLECT OR PROCESS PERSONAL DATA	12
8.0 PROTECTION OF PRIVACY	13
9.0 COMPLAINTS ABOUT BREACHES AND NON-COMPLIANCE	13
10.0 GENERAL RECOMMENDATIONS TO ENHANCE THE LOCALISATION OF AFRICAN UNION DATA PROTECTION FRAME WORK 2022 AND THE DATA PROTECTION AND PRIVACY ACT 2019	14
11.0 Conclusion	16

1.0 Introduction

Gender equality and women empowerment is one of the major objectives of the African Union and in particular making all African women and girls to be more active users and influencers of the technological space and gender enabling E- solutions.

1. Since the official birthday of the internet in 1983 and the invention of cloud computing and social networking platforms in the early 1995, there is a terrific and massive growth in data processing and use by individuals, private sector and state and non-state actors.

2. For example, people generate data every time they go online, leaving behind information to systems with little transparency. The development of the internet was accredited to two great men Vinton Cerf and Bob Kahn and not a single woman led to this development implying that women's perspectives and needs may have not been part of this

invention and more so making it challenging to protect the rights of women.

3. Since gender bias in privacy started in the 19th century as a male hegemony and privileges, women continues to face privacy challenges in the modern times because availability of privacy and perceived value vary with cultures, economy, status, age and gender.

4. Privacy is a fundamental human right therefore no one should interfere with the privacy of someone's privacy, family, home or correspondence, nor to attacks upon his/her honour and reputation and the law should protect against any such interference or attacks.

5. Even with the existence of the legal frameworks on data protection and rights, many consumers including policy makers lack knowledge on how personal data are harvested for business purpose and they are unaware about existence of their rights.



1 African Union (2018): African Union strategy for Gender Equality and Women's empowerment

2 Price Water Coopers (2018): Technology's role in data protection, the missing link in GDPR transformation; <https://www.pwc.com/gx/en/issues/risk-regulation/technologys-role-in-data-protection-the-missing-link-in-gdpr-transformation.pdf>

3 Jonathan Hogeback (Britannica): Who Invented the Internet; <https://www.britannica.com/story/who-invented-the-internet>

4 Allen, Anita L. and Mack, Erin, "How Privacy Got Its Gender" (1991). Faculty Scholarship at Penn Carey Law. 1309; https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2309&context=faculty_scholarship

5 Article 12, Universal Declaration of Human Rights; <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

Similarly, application of data of data to improve living standards of the population in Africa is hindered by the small number of digitized datasets and accuracy concerns over collected data and the accessibility of this data collected by the government is limited.

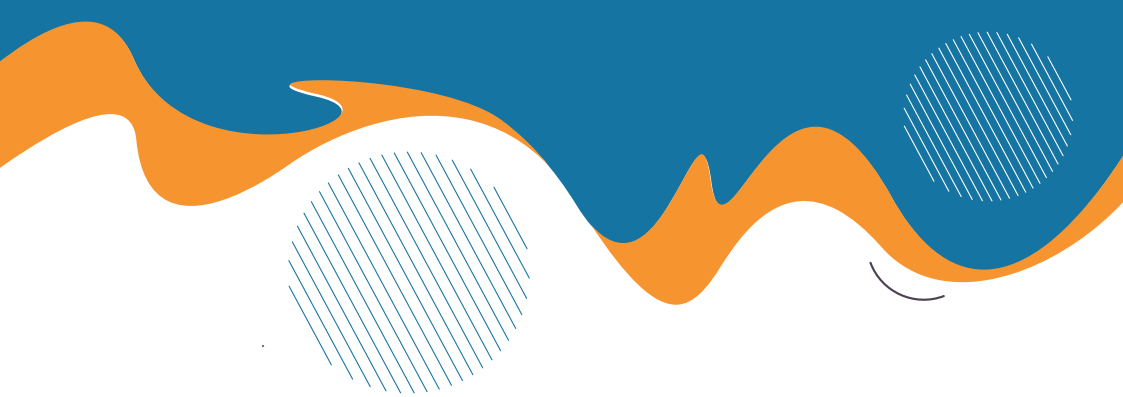
In 2015, the European Union developed the GDPR as a basis for fundamental change in how data controllers and data processors must handle personal data based on the premise that global peer-to-peer interactions occur at equal degrees of power, understanding of mechanisms & bureaucracies involved. The missing link from the GDPR is the appreciation of the concerns related to gender and sexuality and what is needed to address these issues. In Africa, it is estimated that 32 out of the 55 countries have enacted or embraced some form of regulations to protect personal data and some of them include; the Convention on Cyber Security and Personal Data Protection 2014.⁶In 2022, the African Union adopted the Data Protection and Privacy Framework to create an environment where all data is consolidated with harmonized governance systems that allows free and secure flow of data across the continent while safeguarding human rights and upholding security and above all for allowing equitable access and sharing of benefits from the data. In Uganda, article 27 of the 1995 Constitution provides for the protection of person's privacy correspondence, communication or other property which is further detailed under the Data Protection and Privacy Act 2019 with its 2021 regulations.

The Data Protection and Privacy Act 2019 provides for the protection of privacy of individual and personal data by regulating the collection and processing of personal data and to provide for the rights of the persons whose personal information is collected and the obligations of data collectors, data processors and data controllers, to regulate the use or disclosure of personal information and any other related matters.⁷ Policy makers and law enforcers should implement this act bearing in mind that this act focuses on the protection of individual and personal data which is the core element of data protection regulation but does not provide detailed regulations regarding non-personal data.



⁶ African Union Data Protection Framework 2022.

⁷ Data Protection and Privacy Act 2019



According to the African Union Data Protection Framework, there is need for all African member states to adopt AUDP framework 2022 for effective regulations of personal or non-personal data.⁸ Data regulations should not only target mitigation of the risks and harms to individuals but rather ensure the people of Africa including persons with disabilities and the marginalized women and girls, lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI) people exercise their rights freely/safely and use available data to spur innovation, productivity and access relevant opportunities. There is also need for a free flow of data across borders to achieve equitable distribution of benefits across the countries or regions.

Despite the existence of the African Union Data Protection and Privacy Framework 2022 and the National Data Protection and Privacy Act 2019, there are many people in Uganda who do not know about the existence of these legal frameworks and what relates to personal data or their rights. From a gender perspective, there is a possible link between control over own data and willingness to exchange data for benefits, highlighting a potential mediating relationship that could be worthwhile pursuing by the government of Uganda to promote gender equality. Factors such as gender, ethnicity, culture, race, age, social origin, wealth, economic self-sufficiency, education and legal and political frameworks are all affected by digital technologies and privacy.

The right to privacy is particularly important to protect the privacy of people facing inequality, discrimination or marginalization on the basis of their gender, sexual orientation, gender identity, sex characteristics or expression such as women, persons with disabilities and lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI) people.⁹

Once the African Union Data Protection Framework is ratified by all the member states, each member states shall be required to allow free flow of data without any legal barrier, be responsive to the voices of those marginalised by technological developments, ensure safety and security as well as providing accountability to data subjects.

More still, member states will be required to self-manage their data, ensure just and lawful collection, processing and usage in addition to having in place functional data infrastructure managed by the people with adequate capacity coupled with a harmonized legislation and regulation that take into consideration advancement in technology.

With the suggested data governance framework at national level, Ministry of Information and National Guidance through its agencies such as National Information Technology Authority, Uganda Communication Commissions, Data Protection and Privacy Office, Uganda Bureau of Statistics, National Information Registration Authority, Judiciary, Ministry of Foreign and Internal Affairs, Ministry of Trade, Telecommunication Companies are some of the key players that need to spear head the implementation of this African dream.

Women of Uganda Network (WOUGNET) with support from Association for Progressive Communications (APC) between November and December 2023 conducted an analysis of the current Data Protection and Privacy Act 2019 from the Gender and policy perspective of the AUDPF 2022 and these are some of the gaps and recommendations based on the literature review of the available online resources and best practices.



8 African Union (2022). Data Protection and Privacy Framework

9 United Nations (2019:) Human Rights Council Fortieth Session Report of the Special Rapporteur on the right to privacy.



2.0 The Analysis of the Data Protection and Privacy Act 2019

Article 33 of the 1995 National Constitution of the Republic of Uganda provides for the rights of women under sections 1-6 where women are supposed to be accorded full and equal dignity as men in terms of providing necessary opportunities and equal protection while considering their unique status/functions in society and all cultures, customs or traditions against these rights are prohibited. The missing link in the data protection and privacy Act is that women are treated as equal to men yet women's online participation is affected by lack of agency and control over data, consent in unequal power dynamic contexts, loss of privacy, discrimination, online gender-based violence targeting women and bias that is compounded when age, class and gender intersect.¹⁰ For example, women are more concerned with their privacy and they have less control over their personal data, compared to men. More still, women are more likely than men to exercise rights granted through GDPR or other regulations and take measures to control their privacy and personal data.¹¹

This is a confirmation that all laws and legislations being passed must consider women issues in all their diversity that is to say; women with disabilities and the marginalized women and girls including lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI) people which is not the case with the data protection and privacy Act 2019. To address this challenge, we propose the Data Protection and Privacy Office should introduce a separate section(s) that provide protection for women's specific challenges related to consent in unequal power dynamics and all forms of gender-based violence or technology facilitated violence.



10 KICTANET(2023): Gender Perspective on Data Protection



3.0 Interpretation of the of the Data Protection and Privacy Act 2019

Consent refers to any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

In the current state, this interpretation does not protect the rights of women whose privacy are violated through nonconsensual distribution of intimate images commonly known as revenge porn, cyber harassment and cyberstalking because their private data would have been collected freely and willingly but they might have not consented to processing and use of such data by third parties who in this case are the perpetrators. There is no law in Uganda that specifically protects women against non-consensual distribution of intimate images apart from the anti-pornography Act, 2014 which in itself is problematic because it criminalizes pornography. Section 2 of the Data Protection Act 2019, is also silent about this issue hence making it troublesome for survivors to successfully report cases related to cyber-attacks as a privacy breach since consent must be either processed electronically or manually.

Similarly, the Data Protection and Privacy Act 2019 in its current state clearly defines individual and personal data in line with African Union Data Protection Framework as being any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

This is a great opportunity for the data governance stakeholders in Uganda to explore possibility of not only focusing on the protection of collection, processing and usage of personal data but rather seek for avenues to use existing data to empower and provide equal services and benefits to all citizens including the women with disabilities and the marginalized women and girls as well as lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI) people.

Data processing by individuals, private sector, state and non-state actors must follow the principles of legitimacy, openness (including incident reporting, an important

correlation to cybersecurity and cybercrime imperatives) and data specificity or purpose which is not stipulated by the Act yet most challenges African governments are grappling with relates to cybersecurity and cybercrime due to rapid technological advancement.



4.0 Principles of data protection and privacy

The Act intends to guide the collection, processing and usage of data within the territorial boundaries and it is important that the new amendment should reflect the vision of the African Union that puts emphasis on ensuring mutual corporation in data exchange among member states, allowing data to flow in a secured and human rights manner, establishing trust and accountability as well as developing national data infrastructure and capacity. While prioritizing some of these suggestions, rights or the women unique nature and status in the society must as well be put into consideration to ensure equal benefits from data and its enablers. In order to fully incorporate the principles of the AUDPF 2022, we are proposing the Data Protection and Privacy Office should introduce the following principles in the Data Protection and Privacy Act 2019;

- i. Fairness and inclusiveness: Redress inequalities by being responsive to the voices of those marginalised by technological developments.
- ii. Trust, safety and accountability: Promote trustworthy data environments that are safe and secure, accountable to data subjects and ethical and secure design.
- iii. Comprehensive and forward-looking: Encourage investment and innovation through development of infrastructure, human capacity and harmonisation of regulations and legislation.
- iv. Integrity and justice: Data collection, processing and usage must be just and lawful- not used to discriminate or infringe on peoples' rights. By ensuring data justice, rights of women girls as well as lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI) people will be protected.

5.0 Functions of the Data Protection Office

According to the African Union Data Protection Framework, immense benefits are realized from data when there is an enabling regulatory and policy framework in place that allow obtaining useful data, enhanced human, institutional and technical capacities to create value from data. Similarly, there must be free flow of data across institutions or boundaries and the state must show legitimacy and public trust to manage data. In addition, the government must establish data infrastructure as part of the asset for the country and all data system must put into consideration the adaptive digital economy. The Data protection and Privacy Office should ensure that information and communication technology does not constitute a threat to public freedoms and private life of citizens by strengthening the implementation of institutional framework and enhancing adaptation to the digital revolution. Similarly, the data protection and privacy office must build the capacity of all data regulators bearing in mind protection of peoples' personal data in the digital ecosystem including governance of AI, IoT and Blockchain tech and digital platforms. The office should also establish mechanism and collaborate with regional and global governance processes to ensure a consultative and evidence-based data regulation and in instances where the regulations in branches of laws such as; data protection law, competition law, cyber security law, electronic communications and transactions law, intellectual property law overlap and conflict with one another, they must harmonise them to ensure compliance.

This function requires regular reviews and consultation with key stakeholders to identify the gaps and seek mutual redress for rebalancing the legal ecosystem.

In addition to performing its obligations as stipulated in section 5 of the Act, the Data



6.0 The Data governance mandate of stakeholders/opportunities and recommendations for localization of the African Union Data Protection Framework 2022.

Protection office must strengthen its collaboration and partnerships with member states, government ministries and departments and private firms to achieve the African dream as stipulated in the Data Protection and Privacy Framework 2022.

Data governance involves the exercise of authority and control over the management of data with the goal of increasing the value of data and minimizing the data-related cost and risk. Therefore, in this section, we provide details of key stakeholders in Uganda and propose recommendations as per the African Union Data Protection Framework 2022.

Figure 1: Showing the Current mandate of stakeholders/opportunities and recommendations for localization of the African Union Data Protection Framework 2022

No	Name of the stakeholder	Current mandate	Recommended functions
1	Ministry of ICT and National Guidance	The current mandate is to provide strategic and technical leadership, overall coordination, support and advocacy on all matters of policy, laws, regulations and strategy for the ICT sector	<p>Review the ICT sector policies to enhance data value with focus on competition, trade and taxation policies in the digital ecosystem.</p> <p>Empowering the Data Protection and Privacy Office in relation to infrastructure, alignment of policies and data protection, cybersecurity and institutional data governance.</p> <p>Collaborate with stakeholders at international, regional and national levels for improved data governance.</p>

No	Name of the stakeholder	Current mandate	Recommended functions
2	National Information Technology Authority Uganda (NITA-U)	The current mandate is to coordinate, promote and monitor Information Technology (IT) developments in Uganda within the context of National Social and Economic development.	<p>Establishment of data infrastructure for increased access to affordable and reliable broadband data and internet by all including persons with disabilities, marginalized women and girls as well as lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI) people.</p> <p>Establish data infrastructure that allows free exchange of data. This can include cloud services that allows easy management of big data, regulation of e-trade through digital ID.</p>
3	Judiciary	The current mandate of the judiciary is to administer justice, interpret the constitution and laws of Uganda, promote rule of law, safeguard the constitution and protect human rights	Collaborate with the DPPO to create legitimate and trust worthy data system through safeguarding human rights, regulations in a transparent and consultative process with gender diverse teams and providing accountability for use all of personal data.
4	Parliament of Uganda	Parliament's current function is to pass laws for the good governance of the country, provide legislative sanctions and to scrutinize government policy administration.	<p>Introduce bills initiated by private members and urge relevant committees to initiate and spur legislation from the executive on the AUDPF. Women in all their diversity that is to say; women with disabilities and the marginalized women and girls including lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI) people must be part of the consultation.</p> <p>Build the capacity of MPs in data governance using regional and continental parliamentary groups like the Africa Parliamentary Network on Internet Governance (APNIG).</p>

No	Name of the stakeholder	Current mandate	Recommended functions
5	Uganda Bureau of Statistics (UBOS)	The Uganda Bureau of Statistics mandate is to ensure collection, analysis and publication of integrated, relevant, reliable and timely statistical data and information in Uganda	<p>Building the digital and data capabilities of public servants at all levels on basic understanding of how data can be used to enhance service delivery and policy implementation and as well promote the use of high-quality data.</p> <p>Data collection, processing and usage must prioritize the needs, rights and interest of women in all their diversity that is to say; women with disabilities and the marginalized women and girls including lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI) people.</p> <p>Build capacity of public servants and adoption of best practices on data and AI governance in the context of African data use cases.</p>

7.0 Consent to collect or process personal data

Section 7 of the Data Protection and Privacy Act requires data collectors to seek for consent from data subject before collecting or processing any personal data and this is one of the key enablers for the African Union Data Protection Framework.

Exception to consent should not be recognise in a situation of protection of privacy of women whose privacy are violated through nonconsensual distribution of intimate images commonly known as revenge porn, cyber harassment and cyberstalking because their private data would have been given freely and willingly but they might have not consented to processing and use of such data by third parties who in this case are the perpetrators.

8.0 Protection of privacy

Privacy requires trust in the entire political system and the risk of any collected or processed data is born by the data subjects. A gender inclusive and multistakeholders approach should be adopted in law formulation to foster accountability in access and use of public data.

In collection or processing of personal data, the DPPO should add a section that safe guard citizens from new threats and unwanted risks brought about by the technological disruptions because with many people in Uganda still being digitally illiterate, digital consent may not be achieved.

A new section should be included to show how the government is ensuring data justice by ensuring equal visibility, representation and equality with digital data. Data justice should also address the challenge related to data availability, accessibility, usability, and integrity that impact equitable inclusion.

9.0 Complaints about breaches and non-compliance

Article 31 does not show the procedure which the data protection authority should undertake in case of breach and non-compliance and we are proposing a new article be introduced encompassing the following procedure;

The national data protection and privacy office should decide on the following measures

1. Issuing of warning to any data processor who fails to comply with any article of this the Data protection and privacy Act 2019.
2. An official warning to stop such breaches within a set time frame

Where the data processor fails to comply with the official warning addressed to him/her, the national data protection office should implement the following sanctions;

1. Temporary withdrawal of the permit granted
2. Permanent withdrawal of the permit granted
3. Reasonable and equivalent monetary fines

In case of emergencies, where the processing or use of personal data results into violation of fundamental rights and freedoms.

1. Discontinue data processing
2. Block some of the personal data collected
3. Permanent or temporary prohibition of data processing relayed to the Act

10.0 General recommendations to enhance the localisation of African Union Data Protection Framework 2022 and the Data Protection and Privacy Act 2019.

- i. The government of Uganda should ratify the African Union Data Protection Framework 2022 to act as a guiding legal framework to regulate collection, processing and use of personal data.
- ii. Parliament of Uganda should allocate adequate funding to strengthen capacity of the Data Protection Office to enable effective implementation of the Data Protection and Privacy Act 2019 and the 2021 regulations.
- iii. Parliament of Uganda should review the Data Protection and Privacy Act, Right to Interception of Citizens Communication, Right to Access of Information and the Communication, procedures and practices to ensure effective fulfilment of set obligations without compromising rights and privacy of data subjects. The review will enable harmonization of the legal frameworks and compliance with the International norms such as the AUDPF and GDPR.
- iv. In jurisdictions where members of parliament also serve in the executive, they should use their unique position and power to push the cabinet to initiate implementation of the recommendations of the AUDPF.



- v. Ministry of ICT and National Guidance together with its agencies such as Uganda Communication Commissions (UCC) should pay equal attention to surveillance practices by individuals, the private sector and state actors to ensure full rights to privacy and full control of personal data and information online.
- vi. The National Data Protection and Privacy Authority should consider organising a national annual forum involving all stakeholders in pursuit of multistakeholders implementation of the best practices.
- vii. National Data Protection and Privacy Authority should initiate a research study to understand the major challenges limiting cross-border data transfers among Uganda's partners countries.
- viii. The Government of Uganda through Ministry of ICT and National Guidance should hold sensitization and raising campaigns to ensure data collectors and processors oblige by the AUDF and DPPA set procedures and standards.
- ix. The government of Uganda through Ministry of ICT and National Guidance should ensure that all employees are aware of the AUDPF and the DPPA, 2019 requirements and their responsibilities by providing regular training and updates.
- x. The private firm and civil society organisations including the government should increase investment in a multistakeholders data governance systems and tools that can automate many of the tasks associated with data discovery, classification, and lineage; consent management; and compliance reporting.
- xi. The government of Uganda through Uganda Bureau of statistics (UBOS) and its related agencies and ministries should use the data collected over the years to achieve equal distribution of benefits and address risks that are related to human rights and security including protection of women's privacy in case of nonconsensual distribution of intimate images commonly known as revenge porn, cyber harassment and cyberstalking.
- xii. Mainstreaming existing frameworks such the Feminist Principles of the Internet developed by Association for Progressive Communications (APC) and partners to ensure more women and queer persons – in all our diversities are empowered to fully enjoy our rights, engage in pleasure and play, and dismantle patriarchy. For example, principles 13, 14 and 15 will promote gender inclusion and reduce unconscious bias or discrimination in laws/regulations on data based on sexual lifestyles, sexual orientation & gendered practices within patriarchal contexts.

for Science and Technology (UNCST) should utilize its expertise in gender to advise the government to enhance the implementation of the Data protection regulations including the African Union Data Protection Framework 2022 and the Data Protection and Privacy Act 2019. Regular capacity building should be provided to the staff as well.

xiv. Ministry of Gender Labour and National Development should use existing data on the conditions of women in all their diversity in Uganda for evidence-based policy making and this will lead to more effective and efficient public services and policies, which will benefit all the people of Uganda.

Collaboration with PDPO for regular capacity building to women in all their diversity in data protection to sensitize the public about their rights.

xv. The wider civil society organisations and the media should deliberately organise data literacy initiatives to build capacity of their employees and communities on data issues to develop policy and technical knowledge in these areas.

11.0 Conclusion

Localisation of the African Union Data Protection Framework 2022 and effective implementation will play a great role in enabling Uganda as a country to harness the full benefits of data driven economy. With the existence of the Data Protection and Privacy Authority and amendment of the Data Protection and Privacy Act 2019 in line with the above proposals to serve as a law for the data protection within the wider territorial scope with harsh penalties for non-compliance and breach or violations centered around a human rights agenda in the digital ecosystem will increase the value of data. Implementing some of the policy proposals above will enable Uganda to mitigate some of the weaknesses and threats identified by the African Union and create an enabling environment for the data that is gender inclusive and equitable.

