African Multistakeholder GDPR Response Action Plan

This action plan is the outcome of a multistakeholder practicum held at the African School on Internet Governance (AfriSIG) in Zanzibar, Tanzania, October 2018.

Outline

I. About this document
II. Preamble
III. Recommendations
IV. Next Steps

I. About this document

Whereas the AU formed a multistakeholder commission to review possible actions that may be taken in response to the adoption by the EU of the GDPR, the commission has reviewed both the current situation in Africa and the possible effects of the GDPR on the African continent and submits this initial report to the AU on the situation and on a possible action plan. This document does not represent a comprehensive solution to the effects of the GDPR but indicates a way forward for Africa in light of the GDPR.

II. Preamble

Whereas the African Union Convention on Cybersecurity and Personal Data Protection was adopted back in 2014, very few countries are signatories and only two have ratified the convention raising a concern around its acceptability and adequacy.

We also acknowledge the regional (SADC and ECOWAS) and individual country efforts to develop data protection and privacy laws, however gaps are still identified in terms of inclusion and restricting how data are acquired, gathered and used. We strongly feel there is a need to enhance people's privacy and give them greater control over their personal information. Reaffirming the commitments of member's states to freedom and people's rights in declarations, conventions and other mechanisms we request coordinated efforts through the AU to harmonise data protection and privacy laws in accordance to global standards of human rights.

Members of this multistakeholder commision submit that we recognise and support ambitions to have common ground on a way forward on GDPR compliance across the board in Africa. Africa has a different, nascent innovations ecosystem to that of Europe; therefore we should be cognisant of the need to have regulations that do not stunt the emergence of new business innovations by imposing policies that do not support small businesses.

In the wake of rapid advancements in Information and Communications Technology (ICT), the need for individual privacy and data protection has gained more relevance and importance not only in the African Union (AU) and European Union (EU) but also all over the world. Indeed, EU's General Data Protection Regulation (GDPR) has set global precedent on data protection and privacy. The AU through the African Union Convention on Cybersecurity and Personal Data Protection (AUC) seeks to enforce a related regulation for the AU.

We, the members of this commission acknowledge the adoption of the AU Convention on Cybersecurity and Personal Data Protection that provides an opportunity for African states to ensure the security and protection of their citizen's enjoyment of online democratic space and that prevents multinational corporates from abusing the data and information provided by citizens in the course of their online activity.

We are concerned that data protection and privacy laws either being proposed or being implemented in some AU member states restrict freedoms and civil liberties and are not compliant with the GDPR Sec proposal.

III. Recommendations

Therefore, we recommend that:

1. The AUC consider updating the AU Convention so as to harmonise data privacy laws and legislation among the member states with the European Union GDPR.

2. The African Union Commission (AUC) organise a multistakeholder high level round table discussion on the challenges that Member States are facing to sign and ratify the AU Convention on Cybersecurity and Personal Data Protection. The outcome of this round table should be an agreed timeline for amendments, signing and ratification of the Convention.

3. Member States review the AU Convention on Cybersecurity and Personal Data Protection and amend Article 2 which prohibits online gambling as a form of electronic business in member states.

4. The AUC, as agreed should consider engaging a task force to develop a Model AU Personal Data Protection law that provides essential equivalence to the GDPR and that reflects the aims and aspirations of Africans which the Member States would adopt and domesticate.

IV. Next Steps:

5. The development of this model law could:

   a. Utilise the AUC PDP Guidelines developed in 2018 in partnership with ISOC and others. These guidelines provide very clear recommendations and model of PDP law for member states that reflects the unique realities of Africa. They also reflect the aims and aspirations of member states.

   b. Recommend that data controllers and processors hold personal data for a specified period of time.

   c. Recommend a specific period for data breach disclosures. Appropriate fines for failure to comply .

d. We recommend that the model law continues to encourage the connections between the private sector (both small and established multinational corporations) and African states by balancing local contexts with international standards.

e. The model law should not discourage relationships between African states and African private sector in favour of relationships with MNCs.

f. Further, general ease of business and cost implications should be taken note of in order to ensure the model law doesn't make it hard for Africa's private sector to operate extraterritorially.

g. We submit that until all AU member states have adequate levels of data and privacy protection as envision in the GDPR, and that the private sector be allowed to transfer data between states which have adequate protection.

6. We recommend that additional privacy laws should apply to sensitive personal data, informed consent must be required and judicial oversight respected

7. We recommend that the AUC request national data protection authorities to publish concise reports on issues and incidents pertinent to data protection and privacy in member states.

8. We recommend dedication of financial resources by the Secretariat of the AU for appropriate capacity building around data protection in member states.

9. The AU Convention on Cybersecurity and Personal Data Protection be revised to harmonise it with the EU GDPR.

10. There should be transparency and participation in the process of drafting national cybersecurity and data protection laws.

11. The convention recognises online gender-based violence as real violence.

12. The convention should provide clear definitions of terms such as public interest, national interest, fake news, etc.

13. We recommend that AU member states enforce special protection for collection, processing, dissemination, portability, localisation and sovereignty of personal data of and on minors.

14. We recommend that the AU require states to ensure that educational institutions as well as libraries and archives, comply with personal data

privacy laws through carrying out risk management and compliance on personal data collected during research including anonymised data.

15. We recommend that capacity building and infrastructure for national state memory institutions should be improved for efficient and effective retrieval, storage, preservation and overall management of data records and information.