**AFRALO / AfrICANN joint meeting**

**Abu Dhabi, Wednesday 1st November 2017**

**---------------------------------------------------**

**Statement**

**----------------**

We, African ICANN Community members participating in the ICANN 60 International Public meeting in Abu Dhabi and attending the joint AFRALO / AfrICANN meeting on Wednesday 1st November 2017, discussed the general data protection regulation (Regulation (EU) 2016/679) (GDPR).

We acknowledge the fact that the regulations have elicited a lot of interest from many stakeholders within the ICANN community and the ICANN organization due to their Possible implications, especially on Whois. We also note the fact that the regulations are of big interest for Africa. This is due to the fact that significant content and domain registrations of the region are hosted off the continent with a significant number of them within the EU and we interested to understand the negative and positive implication of the GDPR once implemented.

In addition one should consider that many African countries also have BPOs and other data housing locations or co-locations which will have economic impact at length. Many of those businesses as much as registrars and registries including the RIR Afrinic will be impacted heavily on the enforcement side. As some of the countries in Africa like for example south Africa has added a similar enforcement as the GDPR. Mauritius for example will be fast tracking and adopting the GDPR by early January for example.

Many African countries lack data protection or requisite privacy legislation. The few that have utilize a diverse set of standards that are not harmonized despite the cross border nature of data exchange brought about by increased use of the Internet.

While some countries have sufficient data protection laws, a majority lack GDPR compliant Data Protection.

The following heat map shows more or less those countries who are aligned and those not and so on:



Source: <https://www.dlapiperdataprotection.com/index.html>

As a note the grey areas marks quite a few number of countries in Africa that has some or no proper privacy laws and may need to adopt some level of adoption.

The GDPR comes into force on 25th May 2018. We encourage African countries that are major trading partners of the European Union to consider adopting relevant measures needed to ensure compliance. More importantly, we encourage Registries and Registrars who are serving non-EU regions like Africa to ensure implementation does not have damaging implication on their non-EU customers. This will ensure that cross border transactions with the EU are not affected. There are both financial and non-financial implications of ensuring compliance under this comprehensive regulation.

A special note is that Organisations which breach provisions of the GDPR which are most important for data protection, could be fined up to €20 million or 4% of its global annual turnover for the preceding financial year, whichever is greater. For any other breach, a fine of up to €10 million or 2% of global turnover or the preceding financial year can be imposed, whichever is greater.

We urge all stakeholders to:

* examine how the regulations will affect their organizations
* implement policies that comply with the GDPR
* raise awareness on the purpose of the GDPR to mitigate any risks that may result from non compliance
* use GDPR to their advantage.
* There is also an easier way to approach the whole problem which is approach the government and inform and perhaps adopt the GDPR as a way forward with changes to your defined area or country.
* Also to get certified within the EU space on GDPR
* The other way may also be to have ISOC within different countries to really get citizens or individuals to understand their privacy rights.
* Also start moving or getting one person to understand the different implications of the GDPR and organisations small or large to understand that if they deal with EU as a general practice need to consider and have a DPO (Data Protection Officer) who understand what the role implicates.

Meanwhile, we believe that ICANN should investigate if there are compliance issues under the registry agreement (RA) and the registrar Accreditation Agreement (RAA) because of the GDPR and work with contracted parties to understand these issues and take the necessary actions to solve them. We also encourage the ICANN Board to conduct an awareness campaign to educate the community on the implications of the GDPR as it concerns the technical identifiers.

ALAC through the RALOs may actually sensitise as well their constituencies and make them more aware of the different enforcement implications.

As a note the GDPR is mainly Dutch and Belgian laws that have been integrated into one and the only difference is that the EU have worked and tailored it to reflect the whole EU space. The also the change has been that the GDPR was here but the main change has been the enforcement part which now becomes very important.

To turn things around the DNS is where all resolution takes place. One interesting option to consider is that be it ICANN or anyone as well as RIR are heavily impacted and a potential solution is to probably use just a NIC Handle and hide the whole datasets and make them available through law enforcement agencies. But a special note here is that for America it is a money making business that ISPs and others can rip additional benefits from. Also the important point to consider is that there are back to back extradition and suing agreements between the EU and US.

A personal suggestion to think and perhaps even get rid of the problem all together for African countries and ICANN is to perhaps use NIC handles and hide the whole persona data at length and that the only people to perhaps consider to release information would be when law enforcement requests details of the Nic handles under law enforcement authorities with a proper legal papers.

As far as the right to be forgotten or deleted from the database, this could be solved within the agreements between registries and registrants by adding a line or two that suggests that these will be used in case of abuses or other infractions they may have happened in past but is now coming from a law enforcement perspective.

As a last note some of the major changes have been:

* Compensation is now expressly available for non-material damages
* The conditions for consent have been strengthened, organisations will be required to ensure that a request for consent is intelligible and provided in an easily accessible form, with the purpose for data processing attached to the relevant consent form
* The burden of proof in at least some circumstances will be borne by the defending controller or processor
* Privacy will become a legal requirement as the GDPR calls for the inclusion of data protection mechanisms and security structures from the onset of the designing of data processing systems, rather than in addition to
* Controllers and processors without an establishment in the EU may also be liable in cases where they process the personal data of subjects which are resident in the EU

It is however important to note that the impact will be heavy and EU has estimated the number of countries would be 190 countries at least.

Lastly we believe the GDPR issue is of particular interest to the ICANN Ecosystem because of the fact that eCommerce and access to information online is entirely dependent on the DNS Ecosystem that ICANN is a key player.

Thank you!