
DNS and Universal Acceptance Privacy Compliance

By Winny Koech.





Know me a little

- I am an attorney with a keen interest in Data Privacy and policy
- Currently a Compliance Director at a non-profit in Texas.
- Originally from Kenya, East Africa.
- My friend shared Nextgen application with me because she thought it well fit within a topic we had just discussed.
- I like to play Tennis, ride horses and travel.
- I hope to join ICANN's UA working group.
- I hope to gain a deeper insight into the internet governance and data privacy and hopefully one day work for ICANN on compliance.

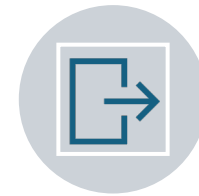
Some key areas of compliance that ICANN should/prioritizes.



DNS Security and
Stability



Data Protection and
Privacy



Contractual
Compliance



Internet
Governance
Principles



Legal and
Regulatory
Compliance



Community and
Stakeholder
Engagement



Universal Acceptance

Universal Acceptance (UA) is about how to appropriately support internationalized identifiers (IDNs and EAI), as well as new and long top-level domains (TLDs).

Compliance with Universal Acceptance (UA) is crucial for ensuring that all internet users, regardless of their language, region, or background, can fully participate in the online world.

How can UA be compliant with data privacy laws worldwide and what are some of the challenges it may face?

General statistics on Universal Acceptance-Focus on Swahili Language.

- 1) Domain Names: - Internationalized Domain Names (IDNs) in the Swahili language, which would allow domain names to be registered and used in Swahili script, have the potential to make online content more accessible to Swahili speakers. Efforts to promote the use of Swahili IDNs have been part of broader initiatives to support multilingualism on the internet.
- 2) Email Address Internationalization (EAI): - EAI support for Swahili email addresses, which would enable individuals to use Swahili characters in their email addresses, has the potential to enhance communication and accessibility for Swahili speakers. However, the full implementation of EAI for Swahili is still be a work in progress.
- 3) Awareness and Education: - Efforts to raise awareness about the importance of UA for the Swahili language and other African languages have been ongoing. These efforts aim to highlight the significance of enabling full support for Swahili domain names and email addresses across internet platforms and applications.
- 4) Technical Implementation: - The implementation of UA for the Swahili language may require technical adjustments and updates to ensure that systems and applications can fully recognize and process Swahili domain names and email addresses. This technical work may be ongoing within the internet and technology industry.
- 5) Regional Considerations: - Given the regional significance of the Swahili language in East Africa, there may be a growing focus on promoting UA for Swahili and other African languages to enhance digital inclusion and accessibility for users across the region.

UA Compliance with data privacy laws worldwide

Challenges and solutions

1.Data Minimization and Purpose Limitation:

Challenge: The challenge lies in implementing systems and processes that can accurately handle and process internationalized identifiers while ensuring that only essential personal data is collected and used, in line with data privacy laws across different jurisdictions.

UA must adhere to data privacy principles such as data minimization and purpose limitation. This means that only necessary personal data should be collected, and it should only be used for the specific purposes for which it was collected. When supporting internationalized identifiers, UA must ensure that personal data associated with IDNs and EAI is collected and processed in compliance with these principles.

2. Consent and User Control:

Challenges: Implementing user consent mechanisms that are effective and understandable for users across diverse linguistic and cultural backgrounds can be challenging. Additionally, ensuring that users have meaningful control over their personal data in the context of internationalized identifiers presents technical and user experience challenges.

UA needs to respect user consent and provide mechanisms for users to control the processing of their personal data. This includes obtaining clear and informed consent for the processing of personal data associated with internationalized identifiers and TLDs.

3. Cross-Border Data Transfers:

Challenges: Managing cross-border data transfers for internationalized identifiers and TLDs may require navigating complex legal and regulatory landscapes, including ensuring that appropriate data transfer mechanisms, such as standard contractual clauses or binding corporate rules, are in place.

UA must manage cross-border data transfers in compliance with data protection regulations that restrict the transfer of personal data outside of specific jurisdictions.

4. Data Security and Encryption:

Challenges: Implementing strong data security measures that are effective across different languages and scripts can be technically complex. Additionally, ensuring that encryption methods are compatible with internationalized identifiers and TLDs presents challenges related to interoperability and standardization.

UA must implement robust data security measures, including encryption, to protect personal data associated with internationalized identifiers and TLDs.

What are some of the laws that may restrict the application of UA

General Data Protection Regulation (GDPR): The GDPR, which applies to the processing of personal data of individuals in the European Union, imposes strict requirements on the collection, processing, and transfer of personal data.

California Consumer Privacy Act (CCPA): The CCPA, applicable to businesses operating in California, imposes obligations related to the collection and handling of personal information of California residents



3) Data Protection Laws in Other Jurisdictions: Various countries and regions have enacted their own data protection laws that may impact the application of UA. For example, the Personal Information Protection Law (PIPL) in China and the Personal Data Protection Act (PDPA) in Singapore impose requirements on the processing of personal data, which may affect how UA is implemented in these jurisdictions.



4) Internet Corporation for Assigned Names and Numbers (ICANN) Policies: ICANN's policies and contractual obligations with domain registries and registrars may also impact the application of UA.

5)National Internet Governance Laws: Some countries have specific regulations governing internet services and online activities, which may include requirements related to domain name registration, email communication, and data privacy. These laws can impact the application of UA, particularly in terms of how personal data associated with internationalized identifiers and TLDs is handled.



6)Cross-Border Data Transfer Regulations: Laws and regulations governing cross-border data transfers, such as the EU-US Privacy Shield and standard contractual clauses, can impact the international application of UA, especially when personal data associated with internationalized identifiers and TLDs is transferred across borders.

In Summary, for UA to be compliant, it should;

Data Minimization and Purpose Limitation

User Consent and Transparency

Data Security and Privacy by Design

Compliance with ICANN Policies

Cross-Border Data Transfer Compliance

Legal and Regulatory Monitoring

Collaboration with Legal and Privacy Experts

- By participating in the IDN work at ICANN, I aim to contribute by implementing measures to help organizations involved in UA, comply with data privacy laws and regulations. This will also involve supporting the accessibility and usability of internationalized identifiers and new TLDs in a way that respects user privacy and data protection.

Thank You,
Winny Koech.