ETHIOPIA'S NEW PERSONAL DATA PROTECTION LAW: A STEP TOWARDS SAFEGUARDING INDIVIDUAL PRIVACY

Background

The House of Peoples' Representatives approved the Personal Data Protection Proclamation No 1321/2016 ("PDP Proclamation" or "Proclamation") on April 4, 2024. This landmark law signifies a commitment to protect the privacy of Ethiopian citizens.

The Proclamation establishes a comprehensive framework for regulating the processing of personal data which has been lacking in Ethiopia. Prior to this, the few rules governing personal data protection were found scattered in different legislations. The preamble of the proclamation clearly articulates the law's objectives, which are safeguarding individual privacy and nurturing a secure digital economy.

The Proclamation further strengthens clarity and consistency through a comprehensive definitions section. Key terms like "personal data," "biometric data" (encompassing fingerprints and facial recognition), "sensitive personal data," and "generic data" are clearly defined. This ensures data subjects and data controllers/processors have a clear understanding of data classifications, what data is protected, and how it can be used. By specifying what data is protected and how it can be used, the law empowers data subjects and guides data controllers/processors in responsible data handling practices.

The Scope of Application

The Proclamation applies to all situations where personal information is handled, encompassing both automated processing and manual processing of data within a filing system. The scope extends to data controllers and processors established in Ethiopia, regardless of the data's location. Additionally, it covers entities not based in Ethiopia but utilize an equipment within the country for data processing (excluding mere transit) and have a designated Ethiopian representative. Notably, the proclamation applies to both private and public institutions across federal and regional governments, including city administrations, that possess the authority to process personal data.

However, certain exceptions exist. This Proclamation does not govern personal data processing for purely personal or household activities, the exchange of information between government agencies on a need-to-know basis, data processing exempted under a separate chapter of the Proclamation[1], or data originating outside Ethiopia that simply transits through the country.

Enhanced Individual Rights

The new proclamation empowers individuals by granting them control over their personal data. Accordingly, data subjects now have the right to access, rectify, erase, and restrict how data

[1] These are: (A) The protection of national security, defence, or public security; (b) historical, statistical, and scientific research; (c) an objective of public interest, including an economic or financial interest of the State; (d) the protection of judicial independence and judicial proceedings.

controllers process their personal data. Additionally, they can object to the use of their data for targeted marketing or automated decision-making.

This new proclamation assigns responsibilities to organizations that handle personal data, known as data controllers. These companies must register with the Ethiopian Communication Authority ("ECA") before processing any data. The Ethiopian Communication Authority is designated as the regulatory body that is responsible for enforcing the proclamation and ensuring compliance. Moreover, the Proclamation mandates data controllers to obtain informed consent from individuals before processing their information. They must also implement robust security measures to protect the data and report any breaches that occur. The new proclamation also regulates cross-border data transfer, allowing them only if they comply with relevant data protection regulations and appropriate safeguards are in place in the receiving third party jurisdiction. Accordingly, the following are the safeguards/conditions for cross-border data transfer:

- The data controller/processor has given proof to the ECA on the existence of appropriate level of protection in that third party jurisdiction.
- The data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer such as the absence of appropriate level of protection.
- The transfer is necessary; or
- The transfer is made from a register which, according to law, is intended to provide information to the public.

The Proclamation explicitly states that data controllers can only store personal information for a "***reasonable time necessary***" to achieve the intended purpose. Additionally, it clarifies the conditions under which data can be stored indefinitely, such as with explicit consent or for historical research purposes.

Furthermore, the law emphasizes transparency by requiring the designated authority to report on the implementation of the proclamation. This will ensure that the public is kept informed about the effectiveness of the legislation.

The proclamation establishes a dedicated supervisory body/Authority, ECA, to oversee the implementation and enforcement of these regulations. This supervisory body will play a crucial role in ensuring that both individuals and organizations comply with the new data protection standards.

Penalties for Violations

To ensure responsible data handling and deter violations, the law outlines penalties for non-compliance. These range from fines of 60,000 to 100,000 Birr for certain offenses, with the possibility of imprisonment for more serious breaches. This reinforces the importance of organizations taking data privacy seriously.

Securing Ethiopia's Digital Future: A Path Forward

Thus, The Personal Data Protection Proclamation marks a significant stride for Ethiopia. This legislation balances individual privacy and data security by granting clear rights to citizens and imposing strong obligations on data controllers. This approach paves the way for a secure and vigorous digital future for the country.