Ethiopia's New Data Protection Law: Enhancing Privacy and Security in the Digital Age

Background

Ethiopia's legislative landscape experienced a significant development with the recent approval of the Personal Data Protection Proclamation No. 1324/2024 **(PDPP)** by the House of Peoples' Representatives. This legal alert highlights the key elements of the approved PDPP and its impacts on business organizations.

Whilst it is true that the data-driven digital world has brought highly beneficial uses, it also carries very significant risks for potential breach of citizen's rights unless sufficient legal protections are put in place. Cognizant of these challenges, many countries have adopted comprehensive data protection laws that establish the required safeguarding measures and ensure protection of applicable legal standards.

Ethiopia did not have a comprehensive data protection law. The data protection rules were scattered in various legislations. The primary legislation that lays the foundation for data protection rules is the Constitution of the Federal Democratic Republic of Ethiopia. The Constitution recognizes the right to privacy and inviolability of the correspondences of individuals. The Ethiopian Civil Code also provides certain privacy rights none of which specifically addresses data protection. Both laws offer overarching protections for the right to privacy. Additionally, certain specific legislations in various domains, such as the Computer Crimes Proclamation No. 958/2016, Freedom of Mass Media and Access to Information Proclamation No. 590/2008, Financial Consumers Protection Directive FCP-01-2020, and Telecommunications Consumer Rights Directive No. 3-2020, provide rules on data protection within their respective scopes.

As technology evolves and the use of personal information by third parties increases, the right to privacy should be expanded to include the types of data to be collected from citizens, the data collection process, data processing requirements, data transfer procedures, and data erasure obligations. This requires a comprehensive personal data protection law. The establishment of the national digital identification system introduced as part of the implementation of the recent Ethiopia Digital Identification Proclamation also necessitates a robust data protection system to safeguard personal data and foster trust in data owners. Aligning Ethiopian standards with international best practices is also one of the main objectives of having a comprehensive law dealing with the protection of personal data. The European General Data Protection Regulation **(GDPR)** had provided a standard for over a hundred jurisdictions across the globe to use it as a resource to regulate the sector. Ethiopia is no exception in this respect.

Scope of application of the PDPP

Similar to most modern legal frameworks, the scope of the 'personal data' definition adopts the concept of identifiability of an individual. The PDPP defines personal data broadly, encompassing various identifiers and information that can identify individuals. Sensitive personal data includes particularly delicate information, such as health records or religious beliefs. Data subjects are natural persons whose data is processed and are the primary beneficiaries of data protection frameworks. The benefits of data protection frameworks are extended to deceased person up to 10 years.

The Proclamation applies to all entities established in Ethiopia (public or private) or that have representative in Ethiopia and processing personal data within Ethiopia's borders. The law limits the extra-territorial implementation of the rules by excluding the application of the Proclamation to companies processing the personal data of data subjects outside Ethiopia with no equipment and presence in Ethiopia.

Data controllers determine how and for what purposes data is processed. Data processors are entities which process data on behalf of controllers. Data processors must comply with the controller's instructions and any other obligations imposed on processors by the data protection framework.

Data protection principles

The data protection principles outlined in the PDPP establish a framework for the lawful, fair, and transparent processing of personal data. The PDPP requires the personal data to be collected only for specific, legitimate purposes, to be relevant, adequate, and not excessive in relation to these purposes, and be kept accurate and up to date where necessary. Additionally, the PDPP stipulates that data should only be retained for as long as necessary, with measures in place to uphold its integrity, confidentiality, and security. Moreover, the law establishes the necessity of respecting data sovereignty throughout the entire processing procedure.

Major obligations of companies as data controller and processor

1. **Registration:** Registration with the Ethiopian Communications Authority is mandatory for companies operating as either data controllers or data processors prior to commencing personal data processing activities.
2. **Consent:** The organization must be able to demonstrate that the data subject has consented to the processing of their personal data. Consent must be freely given, specific, and informed.
3. **Lawful Processing:** Ensuring that personal data is processed lawfully, fairly, and transparently, in accordance with applicable data protection laws and regulations.
4. **Data Minimization:** Collecting and processing only the minimum amount of personal data necessary for the specified purposes and avoiding excessive or irrelevant data collection.
5. **Purpose Limitation:** Specifying the purposes for which personal data is collected and processed and ensuring that it is not further processed in a manner incompatible with those purposes.
6. **Accuracy and Data Quality:** Maintaining accurate and up-to-date personal data and taking reasonable steps to rectify or erase inaccurate or incomplete data.

6. **Data Security:** Implementing appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage.

7. **Accountability and Record Keeping:** Demonstrating compliance with data protection laws by keeping records of processing activities, conducting data protection impact assessments where necessary, and appointing a data protection officer in certain cases.

8. **Data Breach Notification:** Notifying the relevant supervisory authority and affected data subjects without undue delay in the event of a personal data breach unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

9. **Cross-Border Data Transfers:** Ensuring that any transfers of personal data to third countries or international organizations comply with applicable data protection laws and regulations and providing appropriate safeguards for such transfers.

10. **Data Protection Officers (DPOs):** Organizations that engage in large-scale processing of personal data, or that process certain types of sensitive data, are required to appoint a Data Protection Officer (DPO) to oversee compliance with the data protection laws.

11. **Data Protection Impact Assessments (DPIAs):** Organizations must conduct DPIAs where data processing is likely to result in high risk to the rights and freedoms of individuals.

12. **Cooperation with Supervisory Authorities:** Cooperating with supervisory authorities, such as responding to requests for information and investigations, and complying with orders or corrective measures issued by supervisory authorities.

Rights of Data Subject

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights on automated decision-making and profiling

Cross border transfers

Ethiopia's data sovereignty measures require personal data collected locally to be stored within the country. A data controller or processor is allowed to transfer personal data to a third-party jurisdiction under the following defined circumstances:

(a) if they provide evidence to the Authority demonstrating an appropriate level of data protection in the receiving jurisdiction, and the Authority confirms this determination;

(b) if the data subject has given explicit consent after being informed of potential risks, such as inadequate protection in the recipient country;

(c) if the transfer is necessary based on the conditions provided under the Proclamation; or

(d) the transfer is made from a register which, according to law, is intended to provide information to the public.

The practical application of these conditions will have to be worked out in detail through the issuance of directives in each area.

Key next actions for businesses

The actions to comply with Ethiopia's personal data protection law can be taken following a phased approach:

Phase 1 (Preparation Phase): given that the Proclamation has not yet entered into force until its publication, businesses can take preparatory actions, awareness creation and policy formulation measures at this phase.

- **Preparatory actions:** Companies will need to identify what types of personal data they collect and process, the compliance obligations of the company in connection with the personal data, and penalties that are applicable to their organization in case of breach. In this process, companies can develop a strategy in terms of creating a structure within the organization, selection of the systems that will best suit their operation and safeguard the rights of data subjects, and implementation.
- **Developing policy and guidelines:** At this stage, companies can develop their internal data privacy and protection policy and guidelines to regulate how the company will process personal data and the specific measures to be taken during implementation.
- **Awareness creation:** It is also important to create awareness to the team in an organization regarding the purpose and scope of the law, obligations of the company, and the systems that will be adopted and installed for data processing management.

Phase 2 (Implementation Phase): actions will be taken once the law has been made effective and the Communications Authority starts playing its roles under the PDPP.

- **Registration:** the Proclamation obligates the data controller or the data processor to be registered with the Authority to process personal data.

- **Appointment of DPO:** A data controller or data processor shall designate or appoint a data protection officer if the conditions provided under the Proclamation are met.
- **Technical and organizational measures:** The Proclamation adopts the data protection by design and default approach. Companies shall implement appropriate technical and organizational measures designed to comply with the rules of the Proclamation both at the time of the determination of the means for processing and at the time of the processing data.

Phase 3 (Compliance Phase): these are measures to ensure sustainable compliance during the implementation phase.

- **Monitoring the operation:** Regular assessment and auditing of the privacy operation and the applicable systems, rectifying problems, and improving the technology, and procedures are crucial to keep compliant with the legal and regulatory requirements.
- **Breach notification:** The law mandates data controllers to inform the Authority within 72 hours of detecting a personal data breach. As a result, companies must establish efficient mechanisms to swiftly detect and resolve such breaches.
- **Collaboration with regulatory authorities**: The PDPP emphasizes collaboration with regulatory authorities, akin to GDPR's emphasis on cooperation with supervisory authorities. Businesses must be prepared to make records available to the regulatory authority upon request, facilitating regulatory oversight and alignment with the law's cooperative regulatory approach.

Key remaining actions

- **Entry into force of the law:** The Proclamation needs to be published in Negarit Gazette to be effective.
- **Creating a strong regulatory system with the relevant resources, and technical capacity:** The Authority is the key institution to ensure effective and sustainable implementation of the Proclamation. It has the overall responsibility starting from creating public awareness including guiding companies to comply with the rules, conducting audits on compliance with personal data laws, addressing complaints from data subjects, and issuing administrative penalties when companies are not complying with the law. Strengthening the capacity of the regulator should be a starting point to cultivate a culture of responsible and compliant data management, safeguard individuals' privacy rights, and bolster trust in the digital economy. The fact that the designated regulatory authority is Ethiopian Communications Authority, (not a separate independent data protection entity) may pose its own practical challenge as the Communications Authority is already entrusted with an extensive mandate of regulating the communication services sector.
- **Public awareness:** Launching public awareness campaigns is essential to educate citizens about their rights under the PDPP, empower them to manage their personal data, and highlight the significance of data protection in today's digital landscape.
- **Capacity building:** To facilitate proper enforcement of the law, the government may need to initially develop a flexible implementation framework that considers the varied needs and capacities of businesses. This might entail a phased implementation approach, offering technical support to small and medium-sized enterprises, and providing incentives for proactive data protection measures.

MTA | ALN
MESFIN TAFESSE & ASSOCIATES
መሠፍን ታፈሰ እና ጓደኞ የሕግ ቢሮ

Website: https://www.mtalawoffice.com/

Phone No.: +251 11 6 672341

Address: Nisir Building, 2nd Floor, Office No. 002, Off Bole Road, General Seare Mekonnen Avenue

P.O.Box: 8867, Addis Ababa, Ethiopia