AMAN & PARTNERS

LEGAL UPDATE

ISSUE 13

BRIEF OVERVIEW OF THE NEW PERSONAL DATA PROTECTION PROCLAMATION

JUNE 2024

BOWMANS
ALLIANCE FIRM

AMAN & PARTNERS

BRIEF OVERVIEW

THE NEW PERSONAL DATA PROTECTION PROCLAMATION

Ethiopia did not have a unified and comprehensive legal framework governing data protection although there have been scattered rules that directly or indirectly regulate personal data. With a view to formulating a consolidated and comprehensive law, the government has recently adopted Personal Data Protection Proclamation No. 1321/2024 ("the Proclamation"). Prior to the adoption of the Proclamation, the Telecommunications Consumer Rights and Protection Directive, the Financial Consumer Protection Directive, the Computer Crime Proclamation, and the Criminal Code were some of the legislations that incorporated some rules on personal data protection.

This legal update provides an overview of the Proclamation focusing on collection, processing, and transfer of personal data.

SETTING THE SCENE

People tend to share their personal data in different ways i.e. while using the internet, interacting with people, or getting access to any kind of service or product and other similar interactions. In many cases individuals accessing websites are required to consent to privacy terms, which provide that personal data will be collected, processed and used for various purposes. Most users are not patient and interested in reading the privacy terms and often just click on the 'I Agree' checkboxes. By so doing, they consent to give access to their personal data.

Entities/persons collecting personal data may use such data for various purposes, including to understand the needs and preferences of their customers. This will allow such entities to launch targeted marketing strategies or sell such data to other interested companies. As such, entities/persons that collect and process personal data generate revenues directly or indirectly. Further, when personal data fall into the wrong hands, such data can be used for identity theft, discriminatory practices, or even physical harm.

SCOPE OF APPLICATION

The Proclamation applies to; (a) data controller or data processor established in Ethiopia; or (b) a data controller or processor not established in Ethiopia but uses equipment in Ethiopia for processing data otherwise than for the purpose of transit through Ethiopia and has a representative established in Ethiopia.

A data controller is defined under the Proclamation as a person which has decision making power in determining the purposes and means of processing personal data. A data processor, on the other hand, is a person engaged by the data controller to do the data processing on behalf of the data controller. The Proclamation applies to any person having establishment in Ethiopia (including, but not limited to, any employer, event organizer, banks or other financial institutions, schools, ride-hailing service providers, or any other company) collecting and/or processing personal data. The Proclamation also applies to entities not incorporated in Ethiopia but use equipment located/based in Ethiopia and operate through representatives.

The requirement to have a representative in Ethiopia may raise concerns about the representative's form of presence. The Proclamation does not specify whether the representative should be established as a business organization, a commercial representative, a branch or other form of entity.

Moreover, the provisions of the Proclamation do not apply on activities of data processing for the purposes of; (a) protection of national security, defense or public security; (b) historical, statistical and scientific research; (c) an objective of general public interest, including an economic or financial interest of the state; (d) the protection of judicial independence and judicial proceedings; or (e) the protection of a data subject or the rights and freedoms of others.

Further, the scope of the Proclamation is limited. Giant companies that collect and/or process personal data on daily basis like Facebook, YouTube, and other related social media platform providers are apparently excluded from the scope of the Proclamation.

Regulatory Authority

The Ethiopian Communications Authority ("ECA or the Authority") is mandated under the Proclamation to monitor and ensure compliance of data controllers and processors with the provisions of the Proclamation.

The Proclamation empowers the Authority to register data controllers and/or processors if they are to engage in data processing. The Authority shall issue a registration certificate that is valid for two years. The Authority is mandated to issue a directive outlining details on requirements for registration. The Authority retains the power to cancel the registration where it finds that the information given to it by the applicant is false or misleading or the holder of the registration certificate fails to comply with any requirement provided under the Proclamation.

The Authority is also required under the Proclamation to record details of a data protection officer ("DPO") to be appointed by data controllers and processors. A DPO shall be appointed by a data controller or data processor whose core activities require large-scale processing of sensitive data, and large-scale systematic monitoring of a publicly accessible area. Nonetheless, what constitutes 'large-scale' is not defined under the Proclamation. In addition to data controllers or processors, public bodies, except courts acting in their judicial capacity, are also required to appoint DPO.

A DPO is mandated under the Proclamation, among others, to advise the data controller or data processor and their employees on data processing requirements and facilitate capacity building of staff involved in data processing operations. It is also required to cooperate with the Authority on matters relating to data protection.

Data Collection & Processing

Data collectors and processors are required to collect and process personal data in compliance with the Proclamation and other relevant laws. The collection and processing of data shall not be done in ways that are unduly detrimental, unexpected or misleading to the data subject. Data controllers should collect personal data for explicit, specific and lawful purposes only. The purpose for which personal data is obtained needs to be specified to the data subject by the data controller prior to processing.

Data controllers are required to collect and process personal data that is adequate, relevant, and limited to what is necessary for the purposes for which data is processed. Further, personal data obtained by the data controller or processor is required to be accurate and not misleading.

Besides, data controllers or processors are required to collect the minimum amount of data they require for their intended processing operation and ensure that personal data are processed in a manner that ensures the appropriate level of security and confidentiality. They are also required to ensure that data collected locally are stored on a server or data center located in Ethiopia.

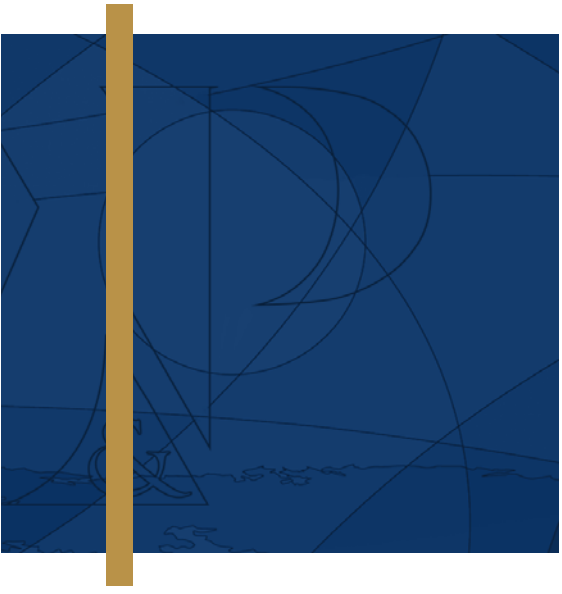
Cross Border Transfer of Data

In principle, personal data collected or obtained locally are required to be stored on a server or data center located in Ethiopia. However, data controller or data processor may transfer personal data to a third-party jurisdiction upon; (a) providing a proof to the Authority on the existence of appropriate level of protection in that third party jurisdiction; (b) the data subject has given explicit consent to the proposed transfer; (c) the transfer is necessary: for the performance of a contract between the data subject and the data controller/processor; for the conclusion or performance of a contract concluded in the interest of the data subject; or for important reasons of public interest; or (d) the transfer is made from a register which, according to law, is intended to provide information to the public.

Remedies and Sanctions

Data subjects are granted the right to submit a complaint in writing to the Authority to have remedy for violation of rights and appeal the Authority's decisions to the Federal High Court within sixty days of the date the decision was rendered if they are not satisfied with the decision of the Authority.

The Authority may impose on data controller or processor a fine up to 4% of its total worldwide turnover of the preceding financial year where an offence has been committed; (a) by an institution; (b) in relation to sensitive data; or (c) in relation to personal data of a child. Moreover, a data controller or processor shall be subject to penalties, including criminal sanctions upon violation of the provisions of the Proclamation.



Concluding Remarks

Businesses or individuals need to be aware that the Proclamation applies to any person collecting and/or processing personal data. As such, all persons collecting and or processing data (including any employer, event organizers collecting personal data, financial institutions, ride hailing service providers, among others) are required to implement personal data protection measures in accordance with the rules prescribed under the Proclamation. The Proclamation does not provide transitional period for compliance and as such compliance is required since the coming into force of the Proclamation.

The enactment of a new Proclamation with a view to governing the collection, processing and transfer of personal data is a step in the right direction. However, the exclusion of multinational technology companies that are likely major personal data collectors and/or processors from the scope of the Proclamation is concerning viewed from the perspective of protecting individuals from unauthorized access, improper and unfair use of data.