Personal Data Protection under the Ethiopian Regime: Legal Update.

1. Introduction

Ethiopia followed sector-specific approach in protecting personal date until the promulgation of Proclamation No. 1324/2024 (hereinafter 'the proclamation). The sector-specific approach was not exhaustive and specific laws were limited to few sectors like the banking sector, telecom sector and computer network. There were also broader rules enshrined under the FDRE constitution and the civil code. However, those rules are inadequate and do not lay down comprehensive rules. With the promulgation of the proclamation Ethiopia switched to EU-model comprehensive data protection law. This legal update highlights key features of the Proclamation.

2. Justification for the proclamation

Protection of personal data under the proclamation, as enshrined in the preamble, is grounded on eclectic considerations relating to rights-based and utilitarian considerations. The rights-based rational is grounded on Art. 26 of the FDRE constitution which stipulates that everyone has the right to privacy. Sub article (3) of the constitution clearly requires public officials to respect and protect the right to privacy. In this digital World, while governments can violate this right by collecting and processing personal data by exercising surveillance on private individuals, it is also important that government takes measure to prevent or redress violations carried out by non-government bodies. This is further supported by Art. 12 of the UDHR and Art. 17 of the ICCPR which prohibit arbitrary or unlawful interference with one's privacy. The legislation is also a response to increased vulnerability of the privacy right and the right to personal data to abuse in this era of digital technology. Under Art. 26 (3) of the FDRE constitution the enjoyment of the right to privacy can only be restricted only in compelling circumstances and in accordance with specific laws whose purposes shall be the safeguarding of national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others.

Secondly, the preamble of the new proclamation underscore the role of protection of personal data in promoting digital economy. In the age of digital economy individual data is collected and processed by governmental and non-governmental actors in multiple

MEHRTEAB & GETU ADVOCATES LLP
Suite No. 805, 8th Floor, Dembel City Center,
Africa Avenue, Addis Ababa, P.O. Box 33449, Ethiopia.

context in the course of participation in trade, provision of financial and payment service, health service, transport service, and employment, etc. This goes in tune with the recent economic reforms in Ethiopia including partial liberalization of the telecom sector, impending opening up on the banking sectors to the foreign investors, launching of new payment systems, and commencement of online payment systems, launching of the National ID service, etc. Hence, the law aims to stipulate rights and obligations of participants in digital transactions in respect of personal data. In particular, the proclamation aims to define major roles, rights and obligations of data controllers, processors, and others involved in handling personal data. In addition, the proclamation seeks to stipulate the rights of owners of personal data, and data regulators, and lay down principles for data processing.

The growing interest on the part of domestic and foreign investors to set up data centres in Ethiopia is also considered as additional motivation to legislate to regulate rights and obligations of participants in the sector.

3. Some Concepts

a) **Consent** means any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by (a) a written statement; (b) verbal affirmations; or (c) any clear affirmative action by which he signifies his agreement to personal data relating to him being processed;

b) **Data** means information that is being processed by means of equipment operating automatically in response to instructions given for that purpose, recorded for processing or as part of a filing system, or forms part of any other accessible public record;

c) **Data controller** means any person who, alone or jointly with others, has decision-making power with respect to data processing;

d) **Data processor** means any person other than an employee of the data controller who processes the data on behalf of the data controller;

e) **Data subject** means an individual who is the subject of personal data;

f) **Personal data** means any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

g) **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

h) **Processing** means an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

i) **Sensitive personal data** means data on a natural person's: racial or ethnic origins; genetic or biometric data; physical or mental health or condition; sexual life; political opinions; membership of a trade union; religious beliefs or other beliefs of a similar nature; the commission or alleged commission of an offence; any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in the proceedings; communications data, including content and metadata; or any other personal data as the authority may determine to be sensitive personal data.

4. Scope of Application

This federal legislation is designed to apply to data processing in private and public institutions at the federal and regional levels including Addis Ababa and Dire Dawa cities. Therefore, the Proclamation applies only data relating to natural/physical persons and does not apply to data belonging to legal persons. As such data controller and data processor are subject to the Proclamation, concerning any personal data, if: it is established in Ethiopia and the data are processed in the context of that establishment including government organs, or if it uses equipment in Ethiopia for processing the data even it has no establishment in Ethiopia. However, the Proclamation does not apply to the processing of personal data: by an individual in the course of purely personal or household activity; which involves the exchange of information between government agencies where such exchange is required on a need-to-know basis; exempted under the Proclamation; and which originates outside of Ethiopia and merely transits through this country.

5. Regulatory organ

The Ethiopian Communication Authority (hereinafter "**the Authority")** oversees personal data protection. The Authority has several powers including: a) ensuring enforcement of the Proclamation, b) ensuring that personal data processed by data controllers and data processors are done according to the data

protection principles; c) monitoring the use of personal data and sensitive personal data; d) keeping and maintaining the Register of data controllers and data processors; e) investigating following legally established investigation procedures and principles complaints made to it, and require information which is relevant for its investigation which will enable it to take administrative measure; f) getting injunction order for the expeditious preservation of personal data, including traffic data, where it has reasonable ground to believe that the data are vulnerable to lose or modification.

6. Principles of Data Processing

To ensure the protection of personal data, the data controller and data processor has several obligations and duties. This includes:

a) **Lawful processing**: data controller or data processor shall ensure that personal data is processed for lawful purposes, which is demonstrated by the existence of the consent of data subject; or the processing is necessary for: a) the performance of a contract with data subject, b) compliance with the obligation to which the personal data controller is subject, c) protecting vitally important interests of the data subject, including life and health, responding to a national emergency, d) complying of public order and safety, f) fulfilling functions of public authority, and g) the purposes of the legitimate interests pursued by the personal data controller or by a third party to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection of personal data. However, sensitive personal data can only be processed on the grounds and conditions provided under the Proclamation.

b) **Consent for processing**: The consent for data processing shall be: given prior to the commencement of the processing; be free, informed, specific, clear and require an active action from the data subject. The requirement that consent has to be free is not defined but it seems to refer to grounds that vitiate consent under contract law, i.e., mistake, fraud, and duress. The requirement of informed consent seems to require the identity of data processor and the purpose for which the data is processed to be indicated. The burden of proof of consent lies on the data processors

c) **Proportionality of Processing**: data processing shall be proportionate in relation to the legitimate purpose pursued.

d) **Prior authorization and consultation**: data controller or data processor shall obtain authorization from the Authority prior to processing personal data to ensure compliance of the intended processing with this

Proclamation and in particular to mitigate the risks involved for the data subjects where a data controller or data processor cannot provide for the appropriate safeguards concerning the transfer of personal data to a third party jurisdiction.

e) **Record of processing operation**: every data controller or data processor shall maintain a record of all processing operations under his/her/its responsibility.

f) **Fairness and Transparency**: the data controller or data processor shall take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child; processing shall not be done in a way that is unduly detrimental, unexpected or misleading to the data subject; or processing shall respect the right to be informed and be done in a manner which is clear, open and honest.

g) **Purpose Limitation**: data collector shall ensure that personal data is obtained only for one or more explicit, specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes. The purpose for which personal data are obtained shall be specified (a) in a notice given by the data controller to the data subject; or (b) in a notification given to the Authority. The data controller shall not make the provision of any goods or services or the quality thereof, the performance of any contract, or the enjoyment of any legal right or claim, conditional on consent to processing of any personal data not necessary for that purpose.

h) **Accuracy and timeliness**: data controller shall ensure that personal data is accurate and, where necessary, kept up-to-date. The data controller shall implement mechanisms to ensure that the time limits established for the rectification, erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data are observed.

i) **Storage limitation**: data controller has the duty not to keep personal data processed for any purpose or purposes for longer than is necessary for that purpose or those purposes unless the retention of the record is required or authorized by this Proclamation or other laws, or reasonably necessary for a lawful purpose related to a function or activity.

j) **Integrity and confidentiality**: The data controller shall take reasonable steps to ensure the reliability of any employees of his who have access to the personal data. When data processor processes personal data on behalf data controller, data controller shall choose a data processor who provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out;

and take reasonable steps to ensure compliance with those measures.

k) **Personal data security**: data controller and data processor shall take appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data. Prior security checks shall be taken before the beginning of the processing or transfer.

l) **Cross-border Data Transfer**: data controller or data processor may not transfer personal data to a third-party jurisdiction that undergoes processing unless it is subject to the Proclamation and the third-party jurisdiction to which the data is to be transferred ensures appropriate levels of protection.

m) **Personal data sovereignty**: any data controller or data process shall ensure that any personal data collected or received in Ethiopia is processed in a server or data centre located in Ethiopia.

n) **Data Protection Impact Assessment**: where processing operations are likely to result in a high risk to the rights and freedoms of data subjects by their nature, scope, context and purposes, every data controller or data processor shall, before the processing, assess the impact of the envisaged processing operations on the protection of personal data.

7. Rights of Data Subject

Subject to the conditions provided under the Proclamation, data subject has the following rights:

a) **Right to be informed**: data controller shall inform the data subject when it collects personal data from the data subject or other sources.

b) **Right of post-mortem protection**: personal data protection survives even after the death of the data subject for 10 years.

c) **Right of access**: data subject shall have, with some exceptions, a right to obtain, on request, at reasonable intervals, free of charge, and without excessive delay

d) **Right to rectification**: when data subject believes that the personal data is inaccurate, incomplete, misleading, not-up-to-date, or is otherwise being processed contrary to the provisions of the Proclamation, s/he shall have, on request, free of charge and without excessive delay, the right to request the data controller to correct the data.

e) **Right to erase**: data subject shall have, on request, free of charge and without excessive delay, the right to erasure of processing of personal data.

f) **Right to restrict processing**: data subject shall have the right to request the restriction of processing of personal data.

g) **Right to object**: The data subject shall have the right to object in writing at any time to the processing of personal data concerning him unless the controller demonstrates compelling legitimate grounds for the

processing which override the data subject's interests, rights and freedoms or for the establishment, exercise or defense of a legal claim.

h) **Right not to subject to automated processing**: data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or significantly affects him.

i) **Right to withdraw consent**: data subject may withdraw his consent at any time and information with regard to withdrawal of consent shall be given prior to giving his consent.

j) **Right to Data Portability**: data subject has the right to receive personal data concerning him, which the data subject has provided to a data controller or data processor, in a structured, commonly used and machine-readable format.

8. **Obligation of Data Controller and Data Processor**

a) **Registration**: To process personal data, the data collector and data processor shall be registered with the Authority. The authority is authorized to set in a directive requirements for registration. Those who meet the requirements will be issued certificate of registration valid for two years and renewable every two years. The law provides grounds for cancellation of registration.

b) **Notification of personal data breach**: In the event of personal data breach, the law requires the data controller to, within 72 hours after having become aware of it, notify the personal data breach to the Authority. The notification shall: a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; c) describe the likely consequences of the personal data breach; and d) describe the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. The data processor is also required to notify the data controller without undue delay after becoming aware of a personal data breach. In addition, the controller is required, subject to exceptional circumstances in the law this duty does not apply, to communicate the personal data breach to the data subject within 72 hours after having become aware of it.

9. **Dispute settlement**

Anyone who has a complaint against a decision rendered by a data controller or data processor shall

have the right to make an administrative complaint to the Authority within twenty-one days of such decision. The Authority after hearing the complaint shall render its decision in writing within twenty-one days. The authority is empowered to issue directives on the administrative procedure to handle complaints.

10. Non-compliance

a) Failure to notify personal data breach; implement technical and organizational measures when a breach is committed; and processing data in violation of the Proclamation is punishable with simple imprisonment from one to three years or a fine from thirty thousand Birr to fifty thousand Birr or both.

b) Failure to erase personal data; respect the right to object processing; restrict processing; and respect the right against automated decisions is punishable with serious imprisonment for a period starting from three years to five years or a fine from fifty thousand Birr to one hundred thousand Birr or both.

c) Re-identifying personal data which has been de-identified; processing re-identified personal data; selling or offering to sell personal data; or transferring personal data outside. Ethiopia in violation of the Proclamation is punishable with serious imprisonment from five years to ten years or fine from one hundred thousand to three hundred thousand Birr or both.

However, if the above offence is committed by a legal entity; has caused any damage and as a result, became a serious offence; has been committed concerning sensitive personal data; or has been committed in relation to the personal data of a child; it is punishable with a fine up to four per cent of its total worldwide turnover of the preceding financial year.

MEHRTEAB & GETU ADVOCATES LLP
Suite No. 805, 8th Floor, Dembel City Center,
Africa Avenue, Addis Ababa, P.O. Box 33449, Ethiopia.