Jurisdiction	Ethiopia
Date	28 March 2022
Law Firm	Mesfin Tafesse & Associates Law Office
Title, Name	Principal Attorney
Contact Information	Mesfin Tafesse E: mtafesse@mtalawoffice.com

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the private sector at the present or in the near future?

No.

Ethiopia has a draft personal data protection law. This law has not yet been entered into force. Under the current legal framework, the other data protection rules and provisions in the private sector are found scattered in different legislations. There is no general law governing the personal information.[1]

ii. Does your country have a general law concerning protection of personal information in the public sector at the present or in the near future?

No.

As provided under the response to Question (i), there are data protection rules in the public sector which have been incorporated in various legislations enacted on specific sectors. There is no general law governing the personal information.

iii. Does your country have laws concerning protection of personal information which apply in individual (specific) sectors at the present or in the near future? (If yes, please describe outline.)

Yes. The telecom sector, the financial sector and the health sector have

[1] We understand the general law concerning the protection of personal information is referring to laws that are not sector specific but regulate personal information in general.

specific laws protecting personal information.

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I. (Please add a reply column as necessary,)

The title of the law ：**Constitution of the Federal Democratic Republic of Ethiopia**

① The definition of "Personal Information"	N/A
② The scope in which the law applies	All persons natural and legal
③ The territorial scope	Within the territory of Ethiopia
④ Remark	This law contains a provision which provides a general guarantee of the right to privacy. It states that everyone has the right to privacy and the right not to be subjected to searches of their home, person, property, or seizure of any property under their personal possession. It further provides that everyone has the right to inviolability of their notes and correspondence including postal letters, and communications made by means of telephone, telecommunications, and electronic devices.

The title of the law ：**The Civil Code of Ethiopia**

① The definition of "Personal Information"	N/A
② The scope in which the law applies	All natural and legal persons
③ The territorial scope	Within the territory of Ethiopia
④ Remark	There is no definition of personal information. The Civil Code provides protection of individuals and their domiciles.

The title of the law ：**Telecom Fraud Proclamation No. 761/2012**

⑤ The definition of "Personal Information"	N/A
⑥ The scope in which the law applies	All natural and legal persons
⑦ The territorial scope	Within the territory of Ethiopia
⑧ Remark	There is no definition of personal information. This Proclamation protects data of telecom service subscribers from illegal interception, access,

	alteration, destruction, or damage.

The title of the law ：**Computer Crimes Proclamation No. 958/2016**

⑨ The definition of “Personal Information”	N/A
⑩ The scope in which the law applies	All natural and legal persons
⑪ The territorial scope	Within the territory of Ethiopia
⑫ Remark	There is no definition of personal information. This Proclamation protects all types of data on computer systems from unauthorized and illegal access, interception, and damage. It also protects computer systems from unlawful interference and has provisions dealing with identity theft, computer related forgery and fraud.

The title of the law ：**Freedom of Mass Media and Access to Information Proclamation No. 590/2008**

⑬ The definition of “Personal Information”	• Information related to the medical, educational, or academic, employment, professional or criminal history, financial transactions individuals have been involved, • Information related to the ethnic, national or social origin, age, pregnancy, marital status, color, sexual orientation, physical or mental health, well-being, disability, religion, belief, conscience, culture, language, or birth of the individual, • Information relating to any identifying number, symbol, or other particular assigned to the individual, the address, fingerprints, or blood type of the individual, • The personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award, or a prize to be made to another individual, • The views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual but excluding the name of the other individual where it appears with the views or opinions of the other individual, • The views or opinions of another individual about the individual, or, • The name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual

	• Confidential commercial information of third parties including trade secrets, financial, commercial, scientific, or technical information, and information supplied by third party in confidence and the disclosure would put the third-party at a disadvantage. • Information about a person who passed away before 20 years.
⑭ The scope in which the law applies	All natural and legal persons
⑮ The territorial scope	Within the territory of Ethiopia

The title of the law ：**Federal Income Tax Proclamation No. 979/2016**

⑯ The definition of "Personal Information"	N/A
⑰ The scope in which the law applies	All natural and legal persons that provide information to the federal government's tax collecting authority.
⑱ The territorial scope	Within the territory of Ethiopia
⑲ Remark	The data protected by this law is any information tax officers obtain in their professional capacity from taxpayers.

The title of the law ：**Electronic Signature Proclamation No. 1072/2018**

⑳ The definition of "Personal Information"	N/A
21 The scope in which the law applies	All natural and legal persons exchanging messages through electronic means
22 The territorial scope	Within the territory of Ethiopia
23 Remark	Personal Information is not defined. Digital certificate providers are obligated to keep personal information that is provided to them confidential.

The title of the law ：**Financial Consumer Protection Directive No. FCP/01/2020**

24 The definition of "Personal Information"	N/A
25 The scope in which the law applies	All
26 The territorial scope	Within the territory of Ethiopia
27 Remark	The word 'data' is defined as any information about an identified or reasonably identifiable financial consumer or security provider. Financial consumer is defined as current or prospective customer of a financial service provider. Financial service providers are expected to keep all their customer's data confidential and secure.

	Financial service providers are required to put in place policies and procedures that ensure confidentiality and security of financial consumers' data. The policy must include protection of data, collection, use, and disclosure of data, types of data collected, and third parties' disclosure procedures. Copies of these policies must be available on the bank's websites and on-demand from customers.

The title of the law ：**National Bank Circular No. FIS/01/2014**

28	The definition of "Personal Information"	N/A
29	The scope in which the law applies	Finance service providers
30	The territorial scope	Within the territory of Ethiopia
31	Remark	This circular obliges financial service providers engaged in agent and mobile banking to retain data centers and related infrastructure in the premises of financial institutions that they have acquired, leased or have special agreements with for the same purposes. It restricts Technology Service Providers from accessing any customer data unless they are authorized by the financial institution for specific period and purposes related to support and maintenance.

The title of the law ：**Draft Personal Data Protection Proclamation**

32	The definition of "Personal Information"	"Personal Data" means any information relating to an identified or identifiable natural person who can be identified: • From those data, or • From those data and other information, which is in the possession of, or is likely to come into the possession of, data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual "Sensitive Personal Data" is defined as a person's: • Racial or ethnic origins, • Genetic data 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, • 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, or • Any other personal data as the Ethiopian Personal Data Protection Commission may determine to be sensitive personal data.
33 The scope in which the law applies	All natural and legal persons
34 The territorial scope	Within the territory of Ethiopia
35 Remark	This is a draft law which has not yet entered into force. It has only been included for information purpose that the enactment of the data protection law is in progress. It is anticipated that it will inter into force in near future.

The title of the law：**Food, Medicine and Healthcare Administration Control Council of Ministers Regulation No. 299/2013**

36 The definition of "Personal Information"	N/A
37 The scope in which the law applies	All natural and legal persons
38 The territorial scope	Within the territory of Ethiopia
39 Remark	This regulation obligates health professionals from disclosing information regarding a patient. Information regarding patients may be released for research purposes without identifying an individual patient directly and indirectly.

ii. If there are any special instructions about the laws, please describe them.

N/A

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

(b) Data Quality Principle

(c) Purpose Specification Principle

(d) Use Limitation Principle

(e) Security Safeguards Principle

(f) Openness Principle

(g) Individual Participation Principle

(h) Accountability Principle

As noted above, Ethiopia does not have a comprehensive private data protection law. Many of the laws related to data are found scattered across various laws. Some of the laws containing provisions related to personal data do contain some of the OECD Privacy principles.

Computer Crimes Proclamation

The Computer Crimes Proclamation indicates that data obtained during searches that is irrelevant to the investigation should be deleted immediately based on the decision of the Attorney General (Ministry of Justice.)[2] This provision, though not in a clear manner, seems to incorporate the Collection Limitation, Use Limitation and Purpose Specification principles.

Anti-Terror Laws

The Prevention and Suppression of Terrorism Crimes Proclamation states that the police have a duty to keep confidential any evidence obtained by them that has a nature of secrecy.[3] This provision includes elements of Use Limitation and Security Safeguards Principles in that the police have a duty to keep the data confidential and use it for the purposes of their investigation alone. There are also provisions

[2] Article 25(5) of Computer Crimes Proclamation 958/2016.

[3] Article 34 (3) of Prevention and Suppression of Terrorism Crimes Proclamation No. 1176/2020.

incorporating the Accountability Principle under the Proclamation.[4] Moreover, elements of Collection Limitation, Use Limitation and Purpose Specification Limitation principles exist in relation to the employment of special investigative techniques including surveillance and interception of data by police during terrorism investigations. Police are obligated to obtain a warrant justifying the need for the data they collect, and to keep all information they obtain confidential. They are also obligated to destroy data and information they receive when it is not relevant to their investigation. Persons (natural or judicial) have the duty to provide data and information that may assist police in prevention of terror attacks or during investigations.[5] However, data that is defamatory to the suspects rights to privacy may only be obtained through court order. The police also have the duty to keep information they receive confidential thereby including the Use Limitation principle.

Registration of Vital Events and National Identification Card

Registration of Vital Events and National Identity Card Proclamation states in general that the organ entrusted to keep registers of civil status shall be responsible for their safeguarding[6] which includes elements of Security Safeguards principle. It reiterates this principle under another provision.[7] Moreover, it includes Data Quality Principle by providing that "any vital event shall be registered with the necessary detail information that can be used for legal, administrative and statistical purposes".[8] The law further includes detailed provisions on the type of data that is to be entered into the registrars with regards to birth, marriage, divorce, and death. The law also includes Individual Participation Principle in relation to corrections of personal data entered.[9] There are procedures outlined for the correction of data entered into the registrar. Regarding national Identity Cards, the law obligates the card holder to notify changes in the particulars of the identity card subscribing to Data Quality Principle in the keeping up-to-date aspect. Purposes of why the data relating to ID cards and vital events collected by the authorities may be disclosed

[4] Article 41 of Prevention and Suppression of Terrorism Crimes Proclamation No. 1176/2020.

[5] Article 43 of Prevention and Suppression of Terrorism Crimes Proclamation No. 1176/2020.

[6] Article 15 of Registration of Vital Events and National Identity Card Proclamation No. 760/2012.

[7] Article 65 of Registration of Vital Events and National Identity Card Proclamation No. 760/2012.

[8] Article 17 of Registration of Vital Events and National Identity Card Proclamation No. 760/2012.

[9] Article 49 of Registration of Vital Events and National Identity Card Proclamation No. 760/2012.

are listed down on the law[10] and this confirms with the Purpose Specification Principle. Moreover, this provision also includes the Individual Participation principle in that unless the consent of a data subject is obtained, data may not be disclosed to any other person other than those mandated by law. The law further states that information will not be disclosed to others even with the consent of the data subject where such information is likely to prejudice public interest. Lastly, the law holds anyone who damages, destroys, suppresses, or unlawfully accesses data collected in relation to registration of vital events and ID card issuance.

Freedom of Media and Access to Information

The Freedom of Media and Access to Information Proclamation has detailed sections about how data that is in possession of public bodies must be disclosed to third parties. These include asking for the consent of the data subject.[11] Moreover, the Proclamation has detailed steps on how individuals request for information and under what circumstances. These requests include request for confirmation of whether the data controller has data relating to the individual who made the request as well as requests for deletion of data. These provisions reflect the Use Limitation and Individual Participation principles.

Financial Data

Financial Service Providers are obligated to put in place procedures that ensure the confidentiality and security of the data of their consumers. The service providers are obligated to inform and disclose their policies regarding protection, collection, use and disclosure, types of data collected and third parties to whom they may disclose data to their customers.[12]

The laws also state that data must be collected using lawful and fair means and must be for legitimate purposes that are necessary for the service provider's

[10] Article 64 of Registration of Vital Events and National Identity Card Proclamation No. 760/2012.

[11] Article 19 of Freedom of the Mass Media and Access to Information Proclamation No. 590/2008.

[12] Article 5.4 of Financial Consumer Protection Directive No. FCP/01/2020.

activities.[13] The same principles also apply when it comes to the use of such data.[14] The law also obligates service providers to ensure that third parties that they disclose data to keeps the data confidential and secure. These laws conform to the Security Safeguards principle.[15]

There are detailed provisions stating procedures for customers to access and correct their data as well that is consistent with the Individual Participation Principle.[16]

Draft Personal Data Protection Proclamation[17]

The Draft Personal Data Protection Proclamation (**Draft Proclamation**) includes a comprehensive list of principles that contain the OECD principles in detail. It further includes other data principles that are not included in the OECD principles.

The first principle in the Draft Proclamation is the **principle of lawfulness**.[18] Data must be processed lawfully and puts conditions that must be fulfilled to process personal data.

The principle of fairness and transparency:[19] This principle dictates that data must be processed in a fair and transparent manner where the data subject is aware of how their personal data is processed in an easy and intelligible manner.

The principle of purpose limitation:[20] It states that personal data must be obtained only for one or more explicitly stated and lawful purposes.

---

[13] Article 5.4.6 of Financial Consumer Protection Directive No. FCP/01/2020.

[14] Article 5.4.7 of Financial Consumer Protection Directive No. FCP/01/2020.

[15] Article 5.4.8 of Financial Consumer Protection Directive No. FCP/01/2020.

[16] Article 5.4.9 of Financial Consumer Protection Directive No. FCP/01/2020.

[17] This law has not yet entered into force.

[18] Article 16 of Draft Personal Data Protection Proclamation.

[19] Article 21 of Draft Personal Data Protection Proclamation.

[20] Article 22 of Draft Personal Data Protection Proclamation.

The principle of data minimization:[21] This principle works in tandem with the purpose limitation principle and dictates that personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

The principle of accuracy:[22] This principle states that personal data must be accurate and kept up to date. It further includes the principle of storage limitation.[23] This principle states that personal data must not be kept for longer than is necessary for the purpose it was collected.

The principle of integrity and confidentiality:[24] This principle is focused on making sure that the confidentiality of personal data is kept even in situations where the data controller transfers the data to third-party processers.

The principle of security:[25] This requires for the appropriate technical and organizational measures to be in place to protect unauthorized access and accidental loss, destruction, or damage to personal data.

The principle of data transfer:[26] This puts the foundation for the data localization provisions that are included in the Draft Proclamation.

The principles of accountability[27] **and the principle of rights of data subjects**[28] are also incorporated in the Draft Proclamation. The accountability principle states that data controllers and processers are responsible for complying with all obligations set out in the Draft Proclamation and the rights of data subjects principle states that personal data must be processed in accordance with the rights of data subjects under the Draft Proclamation including the right to be informed, right of

[21] Article 23 of Draft Personal Data Protection Proclamation.

[22] Article 24 of Draft Personal Data Protection Proclamation.

[23] Article 25 of Draft Personal Data Protection Proclamation.

[24] Article 26 of Draft Personal Data Protection Proclamation.

[25] Article 27 of Draft Personal Data Protection Proclamation.

[26] Article 28 of Draft Personal Data Protection Proclamation.

[27] Article 33 of Draft Personal Data Protection Proclamation.

[28] Article 34 of Draft Personal Data Protection Proclamation.

access, right to rectification, and right to request for erasure.

By way of conclusion, though the Draft Proclamation does not directly include the OECD principles as they are, it covers and reflects all of them in the list of principles provided above.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

(a) Collection Limitation Principle

(b) Data Quality Principle

(c) Purpose Specification Principle

(d) Use Limitation Principle

(e) Security Safeguards Principle

(f) Openness Principle

(g) Individual Participation Principle

(h) Accountability Principle

There is no law that excludes the application of the OECD principles. However, these principles may not be applicable for all legislations (may not be incorporated in all legislations) that have data protection provisions. Some of the laws may also provide exceptions to these general principles.

The National Security and Intelligence sector: This law establishes the National Intelligence and Security Service which has the power to collect data for intelligence and investigation purposes. This law states that any person has an obligation to cooperate when requested in providing intelligence or evidence that is necessary for the work of the National Intelligence and Security Service. Some of the principles such as individual participation principle and openness principle do not apply to this sector.

The Registration of Vital Events and National Identity Card Proclamation: This law states that government regulators who register vital events and ID card information must store it properly so that it may be used for different purposes.[29] Moreover, informal sharing of data is allowed under the Freedom of Mass Media and Access to Information Proclamation.[30] This is contrary to the Purpose Limitation principle.

Computer Crimes Proclamation: This Proclamation indicates that service providers must retain data traffic for two years and must keep it confidential, without providing an obligation to disclose this to the data subject. This may go against the openness principle as well as the individual participation principle.

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as comprehensive government access to personal data or Data Localization? If yes, please describe them.

Yes

Government Access: Revised Federal Ethics and Anti-Corruption Commission Establishment Proclamation No. 1236/2021, Revised Anti-Corruption Special Procedure and Rules of Evidence Proclamation No. 434/2005, Revised Anti-Corruption Special Procedure and Rules of Evidence (Amendment) Proclamation No. 882/2015, Federal Attorney General Establishment Proclamation No. 943/2016 and a Proclamation to Provide for the Definition of the Powers and Duties of the Executive Organs give power to the Ministry of Justice (former Attorney General Office) to access certain types of data without a court warrant.

Commissioner of Ethics and Anti-Corruption Commission has the power to obtain information about bank accounts of persons or organizations which are under suspicion

[29] Article 63 of Registration of Vital Events and National Identity Card Proclamation No. 760/2012.

[30] Article 12(3) of Freedom of the Mass Media and Access to Information Proclamation No. 590/2008.

and investigation for corruption crimes.[31] The organ empowered to prosecute corruption offences has the power to intercept communications between persons and to use camera, sound recorder and other electronic devices without warrant from courts.

Any person has the duty to cooperate when requested in providing intelligence or evidence that is necessary for the work of the National Intelligence and Security Service regardless of a court warrant.[32]

Ministry of Justice is authorized to give permission to investigatory organs to conduct interception and surveillance without a court warrant where urgency requires and there are reasonable grounds to conclude that a computer crime that can damage critical infrastructure is or about to be committed.

Police have the power to conduct surprise searches to prevent terrorism offences with the permission of the Commissioner General of the Federal Police, or anyone designated by him without the need of a court warrant. The Police may also utilize special investigation techniques during investigation of terrorism like interception and surveillance on exchange of information through any devices as well as using camera and audio or video recording devices.

Financial Intelligence Center has the power to obtain information it deems useful for investigation of money laundering and related crimes. It may also request information from police departments, authorities regulating financial and designated non-financial institutions, and any other government organs.

Information collected in relation to registration of vital events or issuance of a national identity card may be disclosed to other organs of government without a court warrant for the following purposes:

- National Intelligence and Security Services,
- Crime prevention and investigation,
- Tax collection,
- Administrative and social services,
- Implementation of risk management systems of financial institutions, and

[31] Article 9(2)(i) of Revised Federal Ethics and Anti-Corruption Commission Proclamation No. 1236/2021.

[32] Article 27 of National Intelligence and Security Service Re-establishment Proclamation No. 804/2013.

- Other purposes authorized by law.

The Document Authentication and Registration Authority that is in charge of registering and authenticating various types of documents may disclose data to government entities empowered by law (police, Ministry of Justice, or other government entities with the power to request information without a court warrant.

Data Localization: The Draft Data Protection Proclamation incorporates detailed regulations about transfer of data. However, this Proclamation has not yet entered into force. Except for the Financial Consumer Protection Directive, the other sector specific laws regulating the data protection regulate data retention obligation in general, not the possibility of cross border transfer.

The Financial Consumer Protection Directive regulates cross border data transfer. Financial data retained by financial service providers mobile and agent banking service cannot be transferred outside the banks data centers and servers. This is provided under a circular that was issued by the National Bank of Ethiopia in 2014 (Circular No. FIS/01/2014). Article 2.4 of the Circular states that “data center and related infrastructures which are used for the provision of mobile and agent banking service shall be kept in the premises of financial institutions that they have acquired, leased or have entered special agreements for the same purpose.”

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

There is no Data Protection Authority in Ethiopia. There is a Data Protection Commission that is included in the Draft Personal Data Protection Proclamation. As noted in our previous responses, this law has not yet entered into force.