Position Paper on the Draft

PERSONAL DATA PROTECTION PROCLAMATION OF ETHIOPIA

Center for the Advancement of Rights and Democracy

August 2022

---

1 CARD acknowledges Mesenbet Assefa (Ph.D.), ADAPT’s Data Protection Fellow, for the preparing this Position Paper.
Introduction

Recent liberalization of the telecom service providers, the mushrooming of tech start-ups that collect huge data from their customers, the rising introduction of online payment systems, and the launch of a National ID Service that collects biometrics information of citizens make the necessity of placing personal data protection laws and policies urgent in Ethiopia. Despite the implications that these realities have on everyday online citizens, there is little to no awareness of the need for personal data protection for those citizens. All the while, there is little progress toward the adoption of a comprehensive personal data protection legal framework.

This position paper aims to outline the key issues to be considered in the draft Personal Data Protection (PDP) Proclamation of Ethiopia. The draft Proclamation of PDP was first introduced in 2020 and updated in 2021 under the auspices of the Ministry of Science and Technology (MiNT). Although the current status of the draft is not clear due to the absence of transparency and public consultations, the fact that the subject of personal data protection is becoming a key legal issue in many jurisdictions may very well push policymakers to support the quick adoption of the draft proclamation.

As the issue of data protection touches upon an important constitutional right to privacy and the fundamental rights of individuals, citizens and civil society organizations must have the insight and tools to monitor the drafting process and provide inputs in the process. The purpose of this position paper is also to serve as an advocacy tool that can support the adoption of the draft PDP by providing feedback and comment on provisions and concepts that could have significant repercussions on the rights of individuals.

The draft PDP proclamation is regarded as a relatively strong data protection law that integrates most of the principles governing the regulation and processing of personal data. Most of the provisions of the draft PDP proclamation were taken from the European General Data Protection Regulation (GDPR) and this position paper also gratefully provides more contextualized and up-to-the-standard recommendations for revisions based on lessons from the GDPR.

At CARD, we believe that the draft law and its subsequent PDP Commission, that will be established on the adoption of the draft, should ensure complete independence of the regulatory commission and provides guaranteed capacity in terms of protecting the personal data of citizens. Therefore, the major consideration that we recommend to the drafters of this legal framework and the legislative body is to make sure that the independence of the Personal Data Protection Commission is complete. In our belief, the Commission’s independence can be assured if:

1. The selection and appointment of Commissioners are based on merit and the process is transparent,
2. The financial and budget sources of the Commission are not having any conflict of interest,
3. The mandate of the Commission is by no way undermined by the interference executive body, and
4. The power and authority of the Commission are clearly defined to impose appropriate regulatory measures.

---

2 The draft personal data protection proclamation this position paper refers unless specified otherwise, has been the version availed at the Ethiopian National ID website as of August 9, 2022.
Preamble, Definitions, and Meanings

Firstly, the preamble should include the importance of data protection beyond personal data and national security contexts, and highlight the importance of maintaining data security, integrity, and safety where most online citizens of Ethiopia have poor digital literacy.

Secondly, the preamble should provide more explicitly that the right to privacy is a constitutionally enshrined fundamental human right and of individuals and situate data protection and privacy into broader Ethiopian socio-political contexts. For example, GDPR has 173 recitals that underlie and justify the substantive and procedural rights contained in the regulation.

Thirdly, it is advisable for the preamble to also provide stress to the importance of establishing an independent and efficient regulatory body in the face of massive and commercialized personal data processing trends with the advancement of technological capacities and fast cross-bordering information flow.

Regarding the stipulated definition of person, the updated version of the draft, in art 2(17), excludes legal persons who were defined as data subjects under art 2(18) of the 2020 draft version but are removed under the revised draft of 2021. A comparative lesson from the 2013 South African Protection of Personal Information Act (PoPIA) which defines a person as either a natural or legal person extends personal data protection to legal persons as well. We suggest this provision should be re-drafted as “personal data” shall mean “any information relating to an identified or identifiable natural person, and where it is applicable, an identifiable existing legal person who can be identified”.

Art 2(5), the article that defines the meaning of consent, does not include revocation of consent, which should be clearly articulated. Some countries further strengthen this definition by cross-refering or mentioning their civil law on the formation of contracts to regulate consent. This can be used as complimentary protection of the consent given and the right of the data subject to withdraw its consent.

Art 2 (7), the definition of “data controller” is better captured in the GDPR law which defines it as “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”.

Art 2(10), the definition of “direct marketing” should include not just individuals but also “or group of individuals” to reflect the principle that direct marketing may also target an individual based on her/his group profile.

Art 2 (12), the definition of “encryption” can be better described as “encryption shall mean the reversible process of transforming electronic data into a form that is unintelligible to anyone but the intended reader or recipient.” Reversibility is important, as is the principle that encryption does not stop an adversary from accessing the data in question, but does prevent them from being able to understand it. The suggested wording would also make the definition consistently applicable to both data in motion (communications traffic) and data at rest (stored files/emails).

Art 2(26), the definition of “sensitive personal data” does not include membership in a political party that is sensitive in different contexts and should be referenced explicitly.
Independence of the PDP Commission

The independence of data protection regulatory bodies is considered indispensable to ensure the protection of the data privacy of individuals. The draft data protection proclamation proposes the establishment of an independent PDP Commission of Ethiopia but there is limited indication or guidance on how the Commission will effectively ensure its independence in discharging its responsibilities.

The most important provision related to this is Art 4/2 which provides that the Commission is “accountable to the House of Peoples’ Representatives”, which is the supreme political body and law-making organ of the state. The other provision that touches on the independence of the Commission is Art 8 which provides that “the budget of the Commission shall be allocated by the House; and, whenever necessary, may receive financial support from local, foreign and international institutions”. However, for a complete independence finance and budget sources must be cautiously defined. The proclamation must explicitly restrict financial support from data collectors or any other commercial body that might have conflict of interest with the regulatory mandate of the Commission.

Furthermore, ensuring the institutional independence of the Commission requires structural mechanisms that are added to the existing provisions in the draft PDP proclamation. The most important aspect of ensuring the independence of the Commission is also the appointment of independent Commissioners who are not politically affiliated to lead the Commission. The revised draft PDP proclamation has provided criteria on how an independent committee of five members would recruit candidates for commissioners. In addition, the independence of the commissioners and their recruits need to have an explicit reference, in the draft, to restrict the nomination of political party members to be commissioners. In some legislations adopted recently such as the Ethiopian media proclamation 1238/2021, the law provides the selection of board members that regulate the media sector in Ethiopia in art 11/6 that a board member cannot be “a member or employee of a political party”. The draft PDP proclamation indeed provides generic guidance that the commissioners should be independent and impartial. But given the experience of lack of independence of most rights-based institutions in Ethiopia, a more robust and explicit provision on the composition of the commissioners will be more desirable. More concerning, Art 63 (3)(4) awards the prime minister the authority of certifying specific data controllers to be exempted from the regulation under the drafted proclamation to process personal data. It is our concern that this would centralize too much power in a single office and one that is external to the Commission and therefore risks undermining its ability to demonstrate its independence. As a form of remedy, we recommend this privilege of authorizing the exemption should be reserved for the House of Peoples Representatives to whom the Commission is accountable.

The independence of regulatory bodies can be ensured not merely by the establishment of supervisory bodies but also by guaranteeing their independence through an organizational structure that demonstrates independence. Legislative frameworks such as the EU’s GDPR stipulate that supervisory authorities must have “complete independence”. As an authority that has the mandate to regulate the extremely sensitive personal data of citizens which in turn impacts their right to privacy as guaranteed by the constitution, the independence and impartiality of the Commission are critical to gaining trust and legitimacy from the public and necessary to carry out its watchdog function of ensuring the right to privacy of individuals. Moreover, the staffing process for the data protection Commission should also be independent
and impartial in the discharge of their duties. It should also be emphasized the importance of ensuring the security of tenure of the commissioners and protection from any unlawful removal from office of the Commissioners and staff of the Commission.

**Mandate and Power of the Commission**

Regulatory authorities must have the mandate and power to discharge their responsibilities of ensuring the right to privacy and the personal data of persons. The draft Ethiopian PDP proclamation endows several powers to the PDP Commission to discharge its responsibilities. Some of the key mandates and powers of the Commission outlined in Art 5 of the draft DPD proclamation are quite broad. However, upon closer inspection one also notices that some issues should have been better articulated in providing a wide range of powers to the Commission. The Handbook on the GDPR recommends that the power of supervisory bodies should be stipulated in a way that provides them more power and responsibilities to ensure that they have adequate power to exercise their authority. In this regard, the EU experience shows that it is desirable that “the powers of the supervisory authority... be interpreted broadly to ensure full effectiveness of data protection for data subjects”. For example, it is not clear from the draft PDP proclamation whether the Commission has the power to provide effective remedies including compensation for the damage sustained by data breach of data subjects in addition to other measures such as sanctions and penalties that include taking away licenses from data controllers.

A parallel clause in the GDPR, Art 82, provides a clear stipulation that individuals have the right to receive compensation for data breaches sustained by data controllers. While criminal responsibility such as the imposition of fines is common in many jurisdictions, whether the Commission will have the power to provide compensation to individuals whose data privacy has been breached is something that needs to be clarified. The GDPR Art 82 provides that individuals have not just the right to lodge complaints but also to get effective remedies including compensation for the violations. Art 82(1) of the GDPR provides that “any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.” Within the framework of international human rights law, it should be noted that states should provide effective remedies for violations of human rights. In many of the general comments and the case law of the supervisory bodies, this has been interpreted in particular to allow individuals the right to get compensation for the violation of their rights. Accordingly, the data protection Commission should also be granted the power to provide compensation for any damage sustained by human rights violations of individuals. Similarly, in the context of a breach of data privacy individuals should also have the right to claim compensation for damage sustained by a data breach and the data protection proclamation should provide a clear mandate for the Commission to award such compensation. The compensation should include both material and non-material damages.

It is encouraging that Art 71 of the revised draft of the PDP proclamation has adopted the provision of GDPR in art 83(f) that reads “the supervisory authorities shall have the power to impose administrative fines for the infringement of the regulation up to 20,000,000 euros or in the case of an undertaking, 4% of the total worldwide annual turnover, whichever is high.” However, the draft PDP proclamation fails to provide a specific figure of fines to be levied at the national level of Ethiopia as an alternative. Even if it could be argued that the percentage figure would be ideal for data breaches at the national level in Ethiopia too, it remains important that clear guidance for regulators is considered. In the context of Ethiopia, it will also be good if there
is some indicative figure about fines imposed on data controllers. In fixing the amount of fines and compensation for data breaches supervisory authorities such as the Commission should consider the nature, gravity, and duration of the infringement, the categories of personal data affected, and whether it had an intentional or negligent character.

Art 5(17) provides that the Commission “delegate whenever necessary any power conferred on it by this Proclamation to any public entity of the Federal or State Government;” this does not seem to be a desirable provision particularly as the power to investigate and oversee the implementation of personal data is the sole responsibility of the Commission itself and the level of independence this Commission have might not be equivalent to the delegated office.

Moreover, while the draft PDP proclamation provides a right of appeal to the Federal High Court, it does not indicate explicitly the right of data subjects to seek judicial remedy in that they are aggrieved by the decision of the Commission. If one looks at the parallel provision of the GDPR Art 78 it provides that data subjects should have a right to an effective judicial remedy against a supervisory authority, if their rights are not adequately protected and they’re aggrieved by its decision.

**Conditions of Consent**

The process of giving consent should not be implied. It should be an expressed consent given in the form of an opt-in, a declaration, or an active motion so that there is no misunderstanding that the data subject has consented to the processing or storage of his/her personal data.

Moreover, consent should also include “coupling prohibition” or “prohibition of coupling or tying” which means that consent given at one time and context should not be allowed for processing the personal data of a data subject that what was originally stated.

There must be a clear mechanism for a data subject to enable him to withdraw his consent at any time. Moreover, withdrawal must also be as easy as giving consent and there should not be additional burdens.

Art 19 of the Draft PDP proclamation on “processing of personal data of a child” has provided specific safeguarding to children’s data storage and processing. In addition, the subsection can benefit from the UN CRC Committee in its General Comment No 25 (2021) paragraph 72 which provides that “[States parties] should also provide information to children, parents, and caregivers on such matters, in child-friendly language and accessible formats.”

There should be a separate consent requirement for children below the age of 16, in which case the legal guardian should have also the consent. While states may opt for a lower age limit to consent below the age of 16, it should not generally be less than 13 years of age.

The GDPR provides provisions (art 8) that can be used as a benchmark as follows:

“[Where consent is given] to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

Art 16 does not indicate the conditions under which consent should be given. In line with the GDPR, it is better to provide it as follows:
“If the data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.”

The provision dealing with the rights of data subjects after they withdraw or revoke consent is not clearly provided. It is also questionable how a data controller can have the right to use personal data after consent is withdrawn.

**Art 16(6)** provides that "where the data subject withdraws consent for the processing of any personal data necessary for the performance of a contract to which he is a party, reasonable legal consequences for the effects of such withdrawal shall be borne by him. The withdrawal of consent by the data subject shall not affect the lawfulness of processing based on consent before its withdrawal." A parallel clause in Art 7(3) of the GDPR captures it better and Art 16(6) of the draft PDP may be better amended as follows "the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent."

**Art 18(3)** provides that the processing of sensitive personal data in some exceptions does not apply to race and ethnicity. However, this does not seem to take into consideration policy coherence with other laws and practices in Ethiopia where often disclosure of ethnicity is required.

While **Art 17** on the Processing of Sensitive Personal Data in principle bans the processing of personal data, the conditions in which sensitive personal data is processed are poorly articulated in the draft proclamation. The GDPR indicates a more robust articulation of the conditions in which personal data may be processed. For example, Art 9(2)(b) of the GDPR provides that “processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject”. While the draft proclamation **Art 17(2)(c)** which parallels this clause provides that "the processing is necessary to achieve the lawful and non-commercial objectives of public organizations", is not clear what the implications of Art 17(3) is. **Art 17(3)** provides that: "sensitive personal data in respect of race or ethnic origin shall not be processed unless the processing is: (a) for ensuring justice and equality with regard to race or ethnic origin; and (b) carried out with appropriate safeguards for the rights and freedoms of the data subject." It is not clear why this particular form of sensitive data cannot be processed and also raises the question of the everyday practice of disclosing these things in the Ethiopian public and political life.

**Art 19**, in line with **Art 16(5)** should provide an explicit obligation on the data controller to ensure that they have complied with the requirements of **Art 19(1)** in ensuring the rights and best interests of children. There should be a clear caption in the section that deals with the rights of data subjects. The GDPR provides under the heading “rights of the data subject” the different categories of rights and protection of data subjects. This draft law of PDP does not have a similar
structure and as such can be confusing (See Art 20). While Articles 33-43 refer to the rights of data subjects, it is not clear what Articles 20-32 refer to.

Art 38(3) which provides the exception for the rights of erasure does not provide an exception “for exercising the right of freedom of expression and information” (Art 17(3)(a) of GDPR). This is a significant omission that needs to be reconsidered to prevent the narrowing of constitutional rights.

The draft PDP proclamation does not provide specific rules on data processors. Art 28 of the GDPR provides the relationship between data controllers and processors and the legal responsibilities to processors.

Art 30 which provides for cross-border transfer needs to have a more robust and careful articulation of the conditions for the cross-border transfer, as this may hold significant implications for the rights of data subjects. The GDPR Art 45(2) provides additional safeguards including clauses that ensure that “(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security, and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which is complied with in that country or international organization, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred’. This ensures the existence and effective functioning of one or more independent supervisory authorities, the duty to publish states which have been considered unsafe to transfer data, and more.

**Data Protection Officer (DPO)**

Apart from the mandatory appointment of DPO by big companies that process larger data, the law can provide a means where other smaller companies can appoint DPO on a part-time basis (French Data Protection Law). The idea of a DPO doesn’t necessarily be for all data controllers, but for those companies where the core processing is commercialized and where a data controller is holding sensitive personal data which is vital to the data subject.

To ease the burden of appointing a data protection officer for every company, it is also common in some states to allow for a group of data controllers to appoint a data protection officer collectively. Moreover, in terms of the modality of the appointment of a data protection officer, data controllers can appoint either an internal employee or an external data protection officer.

The major responsibility of the DPO should be providing expert professional knowledge in data protection law and IT security, ensuring compliance with data protection laws, monitoring processes, creating awareness and training of employees, and collaborating with supervisory authorities such as the Personal Data Protection Commission. The appointment of a data protection officer should also be notified to the regulatory authority in an information note that includes the name and contact information.

Art 24(5) and Art 24(6) may introduce a conflict with the “Principle of Purpose Limitation”, in that an unscrupulous data controller might claim to be retaining personal data even after the legitimate purpose of collection has expired.
Art 29, on “condition for cross-border transfer”, has the potential to introduce a severe operational bottleneck, even though we understand the need to establish the authority of the Commission to make effective decisions. If the Commission has to research and issue dozens of adequate findings immediately, the timing and resourcing of this process will need careful management unless a legal way can be found to introduce an appropriate level of flexibility without compromising effectiveness and accountability.

Art 30, on “safeguard prior to cross-border transfer”, is potentially problematic in that it implies resources and capabilities, not within the Commission’s power to deliver (for instance, the necessary resilient and secure infrastructure to host particular categories of data stored or processed in a server or data center located in Ethiopia). We recommend a cautious and careful approach to exercise this mandate, perhaps based on a broader process of stakeholder engagement by the Commission with government and critical national infrastructure (CNI) stakeholders.

Art 36 (l)(d), on the “exception of the right of access”, the Commission should beware of constraints on transparency under the umbrella of “commercial confidentiality” and issue guidance about the criteria that might justify such a refusal to disclose.

Art 43 has replaced Art 44 of the preceding draft of PDP; however, it has omitted previous sub-provisions that established the rights of lawful heirs or guardians to make decisions on behalf of the data subject. It is advisable to see proposals for the data subject’s rights to pass to their lawful heir from other experiences given in legislations in Hungary, Spain, Estonia, Slovakia, and Denmark, among others. It may be useful for the drafters to explore whether current practice elsewhere is to apply a time limit to the exercise of those rights, as a right that persists too long may create disproportionate problems.

Art 45, on the registration of data controller and processor, makes registration mandatory. This article seems likely to create a significant bureaucratic burden both for the Commission and for the organizations in question – particularly small and medium enterprises, with a knock-on effect on innovation.

It would be better for the Commission to be able to audit data controllers and data processors for compliance with data protection law without necessarily requiring registration in a data protection register (for instance, assuming that regulated entities will be registered in a register of companies, charities, etc.). The Commission, instead, can provide a necessary guideline for other registrars and regulatory bodies to follow in light of registering data collecting and processing entities.

Art 54 doesn’t make it clear what the consequences are for a data controller if data breaches happened due to negligence and/or in cases where a data breach is not notified to the Commission and thereby to the data subject.

Art 56 provides that the Commission has the power to conduct checks on the implementation of security measures such as encryption and anonymization. This is encouraged, but it is important to note its effectiveness will depend on the resources and expertise available to it, and the capability to keep abreast of best practices, current risk/threat models, and so forth. Therefore, staffing and resourcing the Commission with the right facilities and technical capabilities that adapt to the fast changes in the digital age is equally important to provide in the sub-articles.
Art 59, on "prior authorization", imposes quite a high procedural burden on the Commission, data controllers, and data processors. Again, if data processors are acting exclusively under the control and authority of data controllers, it may be superfluous to have them explicitly seek authorization at this point, rather than making the data controller responsible as the principal party here.

We suggest an approach based on assuming compliance, with the Commission conducting checks and audits, publicizing compliance (or failures), and good practice. In our view, Art 65 and 66 establish sufficient powers to make prior registration unnecessary.

Art 63 (4), it is our concern that exemption to be certified by the prime minister would centralize too much power in a single office that is external to the Commission and therefore risks undermining its ability to demonstrate its independence.

International Cooperation & Compensation

The draft law fails to provide a section to draw cooperative mechanisms to establish international means of enforcing the legislation as well as protection of personal data controlled or processed in servers or data centers located in foreign countries. Art 50 of the GDPR, according to lessons to Ethiopia’s draft, establishes that “in relation to third countries and international organizations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance, and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries

The draft law also fails to provide safeguards with specific situations of processing that require additional regulation and guidance in the area of freedom of expression and access to information. For example, Art 85 (1) of GDPR stresses the need to “reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression".
Conclusion

It is long overdue that Ethiopia introduced a draft personal data protection proclamation. This position paper is developed by the Center for the Advancement of Rights and Democracy (CARD) with the support received from Internews’ Advocating for Data Accountability, Protection, and Transparency (ADAPT) project. The position paper provided recommendations and suggestions on key elements for the draft PDP proclamation concerning the independence of the Personal Data Protection Commission that the law will establish, its structure, mandate, and authority as well as clearing definitions and meanings of concepts, the need to establish international cooperation framework to deal with cross border data issues in addition to ensuring well-intended and careful exemption of data restrictions for educational purpose, to protect freedom of expression and journalistic missions, and other necessary functions.