Proclamation No. 1284/2023

Ethiopian Digital Identification Proclamation

WHEREAS, the establishment of a reliable Digital Identification System in Ethiopia ensures the Resident’s right to be identified, enhances the ability to exercise other rights, improves trust between service providers and residents, creates a nationwide enabling environment to ensure transparency, accountability and efficiency;
WHEREAS, establishing a technologically developed, cross sectorial foundational Digital Identification System, helps to plan national development effectively, create economic transformation, ensure good governance, reduce wastage of resources, eliminate redundancy and ensure inclusiveness when policies are designed and development plans are executed;

WHEREAS, establishing a nationwide Digital Identification System is important to institute a reliable, accessible and secured system, and to promote the country's social, political and economic development and predictability, to ensure the overall peace and security of Residents and reinforcing the justice system;

WHEREAS, it is necessary to establish a legal basis for the use of Digital Identification in a comprehensive, consistent and reliable method by establishing a Digital Identification System for the registration of Residents of the country and by retaining the information of the Registrants; properly define the trust framework and legalize the relationship between the various stakeholders of the Digital Identification System, including the Registrant, Registrar, Relying Party, Authentication Service Provider and the Digital Identification Institution;

NOW, THEREFORE, in accordance with Article 55(1) of the Constitution of the Federal Democratic Republic of Ethiopia, it is hereby proclaimed as follows.
SECTION ONE
General Provisions

1. Short Title
This Proclamation may be cited as “Ethiopian Digital Identification Proclamation No. 1284/2023.”

2. Definition
Unless the context requires otherwise in this Proclamation:
1/ “Foundational Identification” means a legal identifier that enables Resident to access services by making use of his unique identity;
2/ “Digital Identification System” means an organized and reliable Foundational Identification system that provides a Unique Number to each Resident by collecting Demographic and Biometric Data in a central database;
3/ “Digital Identification” means a Foundational Identification with a Unique Number that is issued to a resident that is registered on the Digital Identification System;
4/ “Minor Digital Identification” is a type of temporary Digital Identification issued without collecting Biometric Data to a minor as defined per the guidelines of the Institution;
5/ “Biometric Data” means physical attributes that can be computed off of a natural person such as fingerprints, iris and facial photo used for unique calculation of a person’s identity;
6. "Demographic Data" means the non-biometric personal attributes of a resident entered into the Digital Identification System after a successful registration of Biometric and Demographic Data and the unique Digital Identification of the Resident;

7. "Unique Number" means a special and non-repeating number issued to a resident who registered with the Digital Identification System and obtained a unique Digital Identification of the Resident;

8. "Alias Number" is a special, non-repeating number issued to a resident as described in Article 174 of the Civil Code providing the requirement of residence permit from relevant authorities.

9. "Institution" means a Governmental Digital Identification entity that will implement the Digital Identification System and execute this Proclamation or it may be an office established within a relevant Government body;

10. "Resident" means a natural person living in Ethiopia, fulfilling the requirement of residence place provided in Article 174 and 175 of the Civil Code.
11/ “Registrant” means a resident person who receives a Digital Identification after providing his Demographic and Biometric data;

12/ “Registrar” means the Digital Identification Institution or a person entrusted by the Institution to collect the individuals’ data;

13/ “Registration” means the process of enrolling a Registrant, through a unique deduplication process of personal data sent by the Registrar to the Digital Identification System;

14/ “Relying Party” means a person that authenticates an individual’s identity, with the knowledge and consent of the Digital Identification Institution and the individual;

15/ “Authentication” means the process of verifying and authenticating, whether online or offline, the identity of an individual against the registered information in the Digital Identification System central database;

16/ “Authentication Service Provider” means a person that responds to a request for authentication of Digital Identification Data at the inquiry of a Relying Party;

17/ “Personal Data” means Biometric Data collected with the Digital Identification System and Demographic Data indicated under Article 9 of this Proclamation;
18/ "Sensitive Personal Data" means data on a natural person:
   a) racial or ethnic origins,
   b) genetic data,
   c) physical or mental health or condition,
   d) political opinion,
   e) religious beliefs or other beliefs of a similar nature,
   f) the commission or alleged commission of an offense,
   g) any proceedings for an offense committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in the proceedings,
   h) any other personal data as the Institution or other authorized entities may determine to be sensitive personal data.

19/ "Digital Identification Credential" means a physical or Digital documentary evidence containing Personal Data and either the Unique Identification Number or Alias Number;

20/ "Region" means a Region established in accordance with Article 47 of the Constitution of the Federal Democratic Republic of Ethiopia and for the purpose of this Proclamation, it includes Addis Ababa City Administration and Dire Dawa City Administration;
21/ “Government” means the Government of the Federal Democratic Republic of Ethiopia; and for the purpose of this Proclamation, it includes Regional Administrations;
22/ “Person” means any natural or Juridical person;
23/ In this Proclamation, any phrase expressed with a masculine gender includes the feminine gender.

3. Scope of Application
This Proclamation shall be applicable on any person in Ethiopia

4. Objectives
The Digital Identification System shall have the following Objectives:

1/ To contribute to the protection of human rights and the improvement of good governance by ensuring that residents’ right to be easily identified when they move from place to place in the country;
2/ To establish a Digital Identification System that allows easy identification of individuals who want to receive services, to build trust between service providers and service recipients, and prevent illegal activities;
3/ To address duplication of efforts in the preparation of national policies, strategies, plans and in undertaking development activities; thereby reducing resource wastage and enhancing inclusiveness;
4/ To collect demographic and biometric data of residents by establishing a system that is consistent at the national level, which is not limited by sector or regional states and to serve as a source of identification system for other governmental and non-governmental entities; to ensure the transition of service-oriented identifications to a Digital Identification System.

5. Establishing Institution

The Council of Ministers may establish by Regulation an Institution to implement the powers and responsibilities of the Digital Identification System stipulated in this Proclamation or it may be established within a relevant Government body as the case may be.

SECTION TWO

Digital Identification System Principles,

Enrollment and Service Provision

6. Principles

Digital Identification System shall abide by the following principles:

1/ Inclusiveness;

2/ Infallibly;

3/ Data minimization;

4/ Interoperability;

5/ Transparency and accountability;

6/ Technology lead.
7. The Right to get Digital Identification
Any resident who registered for Digital Identification by giving his biometric and demographic data shall have the right to get Digital Identification.

8. Registration System
1/ When any Resident applies for registration, the Institution shall ensure that the applicant has not given Digital Identification before;

2/ The Institution or Registrar entity shall verify and register the personal data of the Registrant using identification documents and other documents acceptable by the Institution or witnesses. The details shall be decided by Directive to be issued by the Institution.

9. Registration System of Personal Data
1/ Personal Data pushed to the Digital Identification System shall consist of Demographic and Biometric Data of each Registrant;

2/ Without prejudice to Sub Article (1) of this Article, Digital Identification System shall consist of the following Demographic Data:

a) First Name, Father’s Name, Grandfather’s Name or when the Registrant does not have such legal name, the Institution may collect the name of the Registrant which is known by the local community;
a) Nationality;

b) Date of birth, month and year;

c) Gender;

d) Domicile Address.

3/ Without prejudice Sub-Article (2) of this Article, with the exception of sensitive Personal Data, additional personal data may be collected including, but not limited to:

a) Mother's name;

b) Phone number;

c) Email address;

d) Postal Address.

4) Pursuant to Article 8 of this Proclamation; if the Registrant fails to submit the required proof of identity, he may present an individual witness who:

a) has a Unique Number, or

b) is registered in the Digital Identification System.

5) Registration of Biometric Data

a) without prejudice to Sub Article (1) of this Article, if it is confirmed by the Registrar that the Registrant can not give Biometric Data because of physical injury or due to a reason beyond capacity, Digital Identification may be provided by registering facial photograph;
10 Circumstances of Issuance of Digital Identification for Minors

(a) The Registrar may register a minor for whom an application has been made, if the applicant has fulfilled the conditions set out in Sub-Article (4) of this Article.

(b) Where a minor has been registered under this Article, the Digital Identification issued to the minor shall be valid for a period not exceeding 10 years from the date of issue.

(c) The Registrar may perform the following actions:

(i) Modify or delete the data held in the Digital Identification of a minor, if it is necessary to correct any error or to prevent fraud.

(ii) Cancel the Digital Identification of a minor, if the minor has reached the age of 18 years.

(d) The Digital Identification issued to a minor shall be valid for any other purpose, save as provided for in paragraph (a) of this Article.

(e) The Registrar may require the submission of additional information, if the Registrar is satisfied that such information is necessary to verify the identity of the applicant or the minor.

(f) The provisions of this Article shall apply equally to both male and female minors, unless otherwise specified.

(g) Notwithstanding the provisions of this Article, the Registrar may issue a Digital Identification to a minor, if the minor is unable to register under the provisions of this Article, on account of any genuine reason.

(h) The Digital Identification issued to a minor shall be valid for any other purpose specified in the regulations made under this Article.

(i) The Registrar may require the submission of additional information, if the Registrar is satisfied that such information is necessary to verify the identity of the applicant or the minor.

(j) The provisions of this Article shall apply equally to both male and female minors, unless otherwise specified.

(k) Notwithstanding the provisions of this Article, the Registrar may issue a Digital Identification to a minor, if the minor is unable to register under the provisions of this Article, on account of any genuine reason.

(l) The Digital Identification issued to a minor shall be valid for any other purpose specified in the regulations made under this Article.

(m) The Registrar may require the submission of additional information, if the Registrar is satisfied that such information is necessary to verify the identity of the applicant or the minor.

(n) The provisions of this Article shall apply equally to both male and female minors, unless otherwise specified.

(o) Notwithstanding the provisions of this Article, the Registrar may issue a Digital Identification to a minor, if the minor is unable to register under the provisions of this Article, on account of any genuine reason.

(p) The Digital Identification issued to a minor shall be valid for any other purpose specified in the regulations made under this Article.

(q) The Registrar may require the submission of additional information, if the Registrar is satisfied that such information is necessary to verify the identity of the applicant or the minor.

(r) The provisions of this Article shall apply equally to both male and female minors, unless otherwise specified.

(s) Notwithstanding the provisions of this Article, the Registrar may issue a Digital Identification to a minor, if the minor is unable to register under the provisions of this Article, on account of any genuine reason.

(t) The Digital Identification issued to a minor shall be valid for any other purpose specified in the regulations made under this Article.

(u) The Registrar may require the submission of additional information, if the Registrar is satisfied that such information is necessary to verify the identity of the applicant or the minor.

(v) The provisions of this Article shall apply equally to both male and female minors, unless otherwise specified.

(w) Notwithstanding the provisions of this Article, the Registrar may issue a Digital Identification to a minor, if the minor is unable to register under the provisions of this Article, on account of any genuine reason.

(x) The Digital Identification issued to a minor shall be valid for any other purpose specified in the regulations made under this Article.

(y) The Registrar may require the submission of additional information, if the Registrar is satisfied that such information is necessary to verify the identity of the applicant or the minor.

(z) The provisions of this Article shall apply equally to both male and female minors, unless otherwise specified.
11. Unique Number Issuance

1/ Upon collection and pushing of Personal Data to the system as described under Article 9 of this Proclamation, the Institution shall issue to each Registrant a Unique Number that uniquely differentiates that person from others;

2/ The Unique Number shall be generated by electronic means in a confidential manner, and shall preserve the security and privacy of the Personal Data behind the number;

3/ One Unique Number shall be given only to one Registrant and shall remain immutable, irrevocable and permanent;

4/ Without prejudice to the Unique Number referred to in Sub-Article (2) of this Article, Alias Numbers for different work sectors, distinctively or based on the need of the Registrant, with a set validity period meant to shield the privacy of the Unique Numbers, allowing the Registrant to receive authentication service similar to what the Unique Number enables may be generated based on the working procedure of the Institution;

5/ The Unique Number described in Sub Article (2) of this Article is immutable, hence for the purpose of protecting the privacy of the Registrant it can be replaced by an Alias Number that may be printed on Digital Identification Credentials or can be used for other purposes;
6/ Any Registrant who has lost his Unique Number may recover from the Institution or from another entity authorized by the Institution up on effecting the necessary payment based on procedures put in place by the Institution;

7) Without prejudice to Sub-Article (4) of this Article, if the death of the Registrant is confirmed by the procedures of the Institution, the Institution shall has the obligation to make the Unique Number remains immutable and ensure that the Unique Number is not used for authentication service;

8) Without prejudice to Sub Article (3) of this Article an individual’s Digital Identification Unique number may be locked or disabled as per his request or by a court order. The detailed procedure shall be determined by a Directive to be issued by the Institution.

12. Digital Identification Credential

1/The Digital Identification Credential issued by the Institution and by other authorized entities shall contain the following personal data:

a) All the Data listed under Article 9 Sub Article (2) of this Proclamation;

b) facial Photograph referred to in Article 9 Sub Article (5) Paragraph (b) of this Proclamation;
4) Unique or Alias Number;

d) Date of issuance and date of expiry of the Digital Identification Credential; and

e) Other Data provided under Article 9 of this Proclamation subject to the decision of the Institution;

2/ The Digital Identification Credential must be renewed upon the recapture of biometric data; however, if the Digital Identification Credential has expired, it shall not be used for authentication services;

3/ Digital Identification Credentials may be issued by the Institution or by other bodies mandated by the Institution;

4/ The Institution shall have the obligation to renew the Digital Identification Credential after verifying the Registrant’s Personal Data collected before;

5/ A Registrant whose Digital Identification Credential is lost or damaged can apply for a replacement and obtain a new credential upon presenting proof of loss or attaching the damaged credentials as per the procedures put in place by the Institution;
6/ Any person who finds a lost physical Digital Identification Credential shall return it to the Institution or to a nearby police station.

13. Language

1/ Personal Data collected into the Digital Identification System and displayed on Digital Identification Credentials shall be in the working languages of the Federal Government, in the working language of the Regional Government where registration is took place and in English;

2/ Without prejudice Sub Article (1) of this Article, Personal Data may be recorded and Digital Identification Credential printed in additional local language as per a Directive to be issued by the Institution.


1/ Any Registrant shall notify to the Institution of the changes to his Personal Data collected to the Digital Identification System after Registration.

2/ The Institution or Registrar shall notify to the Registrant and let the Registrar updatated Data collected by Digital Identification System if the Data collected are misplaced or destroyed by any natural or man made disasters.
SECTION THREE
Relaying Parties and Authentication Service

15. Relaying Parties

1/ Any Relaying Party that wants to put Digital Identification as a mandatory requirement to provide service shall get approval from the concerned regulator.

2/ Relaying Parties may receive a Registrant’s Personal Data from the Institution or other Authentication Service Providers authorized by the Institution, to authenticat the individual’s identity based on the consent of the Registrant.

3/ Any Registrant that needs to access Digital Identification based services, can get Authentication Services from the Relaying Parties.

4/ Notwithstanding to Sub Article (2) of this Article Relaying Parties shall obtain authorization from the Institution before they start providing service.

5/ Notwithstanding to Sub Article (2) and Sub Article (4) of this Article, if the Relaying Parties can not obtain Data of the Registrant from the Institution, they have the right to give service using their own other method.
<table>
<thead>
<tr>
<th>6/ The duration of the retention period for Personal Data by a Relying Party shall be specified by a Directive of the Digital Identification Institution.</th>
</tr>
</thead>
<tbody>
<tr>
<td>16. Authentication Service Provision and Usage</td>
</tr>
<tr>
<td>1/ Digital Identification may be taken as a legal and sufficient evidence to proof or authenticate a Resident’s identity.</td>
</tr>
<tr>
<td>2/ Though the Institution is one of the authentication service providers, It may authorize an additional authentication service providers.</td>
</tr>
<tr>
<td>3/ Any Registrant that wants to receive Digital Identification based Authentication Service shall present Unique Number or a Digital Identification Credential with its Unique Number.</td>
</tr>
<tr>
<td>4/ When the Authentication Service Providers authenticate personal data, they shall provide only minimal necessary level of personal data based on the needs of the Relying party as authorized by the Institution;</td>
</tr>
<tr>
<td>5/ Authentication Service Providers as well as Relying Parties shall ensure the safety and security of the Personal Data they received from the Digital Identification System.</td>
</tr>
</tbody>
</table>
SECTION FOUR

Personal Data Protection, Security, Management and Grievance Redressal

17. Protection and Security of Personal Data

1/ The owner of any Personal Data collected for the Digital Identification System is the Registrant; Hence any authentication processes under the Digital Identification System shall be done with the consent of the Registrant.

2/ The Institution shall ensure that, the confidentiality of Personal Data is maintained in the course of collecting, registering, authenticating, storing, and processing of the same.

3/ Data collected in accordance with the principles set out in Article 6 Sub Article (3) of this Proclamation; no information shall be collected for the Digital Identification System other than those necessary to identify Residents and have direct support to the system.

4/ Any person may not collect, distribute, print, use, provide data or transfer a copy to a third party or body or disclose data collected with Digital Identification System without the Registrant’s consent.
5/ It is prohibited to disclose, transfer or modify the Personal Data of any Registrant, collected under the Digital Identification System in accordance with the Rules and Regulations without the Registrant's consent.

6/ Notwithstanding the Provisions of Sub Article (5) of this Article, the data may be disclosed or transferred to the relevant legal entity authorized by law or by court order.

7/ Summarized demographic reports and statistical data which will not disclose Personal Data collected with in digital identification system may be shared to legally authorized parties in accordance with the procedures of the Institution.

8/ Personal Data transmitted to a Relying Party from a Digital Identification System database following the working procedure, can be used only for that particular service for which it was requested; Relying Parties may store this information in their own database and use it only for their own use, without violating its original purpose.

9/ Without prejudice to Sub Article (7) of this Article, using of Personal Data obtained upon the consent of the Registrant for personal purpose other than they were designed for or sharing to the third parties is prohibited.
10/ During registration, a standard consent form prepared by Digital Identification System, which describe the Registrant’s rights and obligations shall be completed and signed by the Registrant as proof of consent.

11/ Without prejudice to Sub Article (10) of this Article, in case when a witness testifies for the Registrant, such witness shall fill in a standard consent form prepared by the Institution stating his voluntary consent, rights and obligations, the witness’s Unique Number or proof of Digital Identification registration and proof of identity, must be provided, signed and completed on the form.

12/ The Institution shall employ strong administrative, legal, procedural and technical safeguards to ensure the protection of Personal Data from either natural or man-made disasters, electronic attacks, theft, destruction and other similar losses.

13/ Personal Data collected for the Digital Identification System must be organized in a convenient manner and stored securely in a database managed by the Institution.
18. Data Fraud or Error

1/ When the Digital Identification of a Resident is confirmed to be fraudulent, the Institution may lock the Digital Identification, update the data or take other legal precautionary measures to block the fraudulent data from further use or may initiate suit or charge.

2/ Whenever the institution verifies that there is erroneous Personal Data it has the responsibility to rectify the error, without changing the Unique Number.

19. Personal Data Management

1/ The Digital Identification System shall be a reliable and robust system to securely and safely administer Personal Data.

2/ The Digital Identification System is tasked with maintaining Personal Data quality over time, including the responsibility of updating, re-verifying, renewing, temporarily locking or revoking Digital Identification Information.

20. Grievance and Complaint Redressal

1/ The Institution shall establish a complaint handling department and notify such establishments to its customers.

2/ Any person against whom Digital Identification service is provided and a decision is made has the right to lodge a complaint to the Institution.
3/ Any complaints and grievances that may be encountered in the course of service provision of the Institution shall be solved in accordance with the grievance filing and redressal Directive of the Institution.

4/ A party who is dissatisfied with the decisions of the Institution may file a complaint to the pertinent court.

SECTION FIVE
Miscellaneous Provisions

21. Duty to Cooperate

Any person when requested by concerned organ to render the necessary cooperation for the effective implementation of objectives and activities indicated in this Proclamation shall has the obligation to cooperate.

22. Criminal liability

1/ Any person who refuses to receive digital identification as a legal identification or refuse to provide services with Digital Identification issued upon verification of identity by the relevant authority based on this Proclamation, Regulation and Directives to be issued following this Proclamation or violates duty to cooperate under Article 21 of this Proclamation shall be punished with a fine from Birr Ten Thousand (10,000) to Birr One Hundred Thousand (100,000).
2/ Any Registrar who collected more data than needed to get digital Identification in violation of Article 17 Sub Article (3), (4) or (5) of this Proclamation shall be punished with fine from Birr Ten Thousand (10,000) to Birr One hundred Thousand (100,000).

3/ Any person who intentionally transfer data collected to receive Digital Identification to a third party in violation of Article 17 Sub Article (9) of this Proclamation shall be punished from 1(One) year to 5(Five) years or in accordance with the circumstance of the case up to 8(Eight) years rigorous imprisonment.

4/ If the crime provided under Sub Article (1) and (2) of this Article is committed by juridical person, it shall be punishable with fine from Birr Three Hundred Thousand (300,000) to Birr Eight Hundred Thousand (800,000).

5/ If the crime provided under Sub Article (3) of this Article is committed negligently the punishment shall be punishable from 6(Six) month to 1(One) year simple imprisonment or with fine from Birr Ten Thousand (10,000) to Birr Seventy Thousand (70,000).

6/ If the crime provided under Sub Article (3) of this Article is committed by a juridical person, it shall be punishable with fine from Birr One Hundred Thousand (100,000) to Birr Five Hundred Thousand (500,000).
23. Repealed Laws

No law or customary practice, inconsistent with the provisions of this Proclamation shall be applicable with respect to matters provided for by this Proclamation.

24. Transitory revisions

Notwithstanding Article 23 of this Proclamation, Digital Identification issued before the adoption of this Proclamation, shall be considered as issued based on this Proclamation and remain legal.

25. Power to Issue Regulation and Directive

1/ The Council of Ministers may issue Regulation necessary to enforce this Proclamation.

2/ The Institution may issue necessary Directives to implement this Proclamation and Regulations issued following this Proclamation.

26. Effective Date

This Proclamation shall enter into force on the date of its publication in the Federal Negarit Gazeta.

Done at Addis Ababa, On this 18th Day of April, 2023.

SAHLEWORK ZEWDIE
PRESIDENT OF THE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA