

# Ethiopia's Personal Data Protection Proclamation No. 1321/2024: A Legal Update

👤 Kiya Tsegaye    📅 October 16, 2026    ⌚ 7 min read

Ethiopia's first comprehensive data protection law is already in force with no grace period: businesses must register, appoint a data protection officer where required, and localise core data processing.

Ethiopia now has its first comprehensive data protection law. Proclamation No. 1321/2024 was published in the Federal Negarit Gazette (30th Year, No. 35) on 24 July 2024 and entered into force on publication (Art. 70). Its preamble cites the absence of detailed individual rights and of a dedicated regulator, and the need for a framework aligned with international standards. Kiya & Associates Law Office has prepared this note on the key provisions and what businesses should do now.

*This legal update builds on our earlier overview, [A New Dawn for Data Protection in Ethiopia](#), and focuses on the compliance duties and enforcement architecture.*

## At a Glance

- Regulator: the Ethiopian Communications Authority (Arts. 2(36), 5).
- Registration: controllers and processors must register before processing (Arts. 33–38).
- Breach clock: notify the Authority and affected individuals within 72 hours (Arts. 43–44).
- Data sovereignty: locally collected data must be stored in Ethiopia (Art. 22).
- Penalties: fines up to 4% of turnover and up to ten years' imprisonment (Arts. 59–60, 64).

## Scope and Regulator

The Proclamation covers automated processing, and non-automated processing of data forming part of a filing system (Art. 3(1)). It binds controllers and processors established in Ethiopia, and those abroad that use equipment here and have a local representative (Art. 3(2)), including federal and regional public bodies (Art. 3(3)). Household activity, need-to-know exchanges between government agencies, and data merely transiting Ethiopia are excluded (Art. 3(4)). The Ethiopian Communications Authority is the regulator (Arts. 2(36), 5), while the Ministry of Innovation and Technology sets policy (Art. 4).

## Principles, Consent, Sensitive Data and Rights

Processing must be lawful, fair, transparent, purpose-limited, adequate, accurate, kept no longer than necessary, secure and confidential, and must respect data sovereignty (Art. 6). Lawful grounds are consent, contract, legal obligation, vital interests, public health or public authority functions, and legitimate interests (Art. 7(2)). Consent must be free, informed, specific and active, cannot be bundled with other terms, and the controller bears the burden of proof (Art. 8).

Sensitive data — including ethnic origin, genetic and biometric data, health, political opinions, religious belief, criminal offences and communications data (Art. 2(5)) — is prohibited unless an exception applies, such as written consent (Art. 9); further categories may be added (Art. 10). For children under sixteen, parental consent and age verification are required, and marketing, profiling and profile merging are barred (Arts. 2(15), 11).

Individuals hold rights to be informed, access, rectification, erasure, objection (including to direct marketing), restriction, protection from solely automated decisions, and portability (Arts. 24–32). These rights last ten years after death and pass to lawful heirs (Art. 23).

## Core Compliance Obligations

- **Registration:** controllers and processors must register with the Authority before processing; the certificate lasts two years and may be cancelled after a 21-day show-cause notice (Arts. 33–38).
- **Data protection officer:** required for government bodies and where core activities involve large-scale regular monitoring or large-scale sensitive data (Art. 40).
- **Accountability:** records and logs of processing (Art. 46), impact assessments before risky processing (Art. 47), consultation with the Authority where high risk remains (Art. 48(2)), privacy by design and default (Art. 49), and destruction of data once its purpose lapses (Art. 50).
- **Breach:** the controller must notify the Authority within 72 hours, giving reasons if late, and inform affected individuals within 72 hours unless exceptions apply, such as encryption (Arts. 43–44). A processor must inform the controller without undue delay (Art. 43(3)).

## **Cross-Border Transfers and Data Sovereignty**

Data may go only to jurisdictions ensuring appropriate protection (Arts. 18–19), unless the controller proves adequacy and the Authority so determines, the individual gives explicit informed consent, the transfer is necessary for listed purposes, or it is made from a public register (Art. 20). The Authority may prohibit, suspend or condition transfers (Art. 21), and must authorise transfers where safeguards are lacking (Art. 48(1)).

Locally collected data must be stored on a server or data centre in Ethiopia, the Authority will designate “critical” data that may be processed only locally, and cross-border transfer of sensitive data needs its prior approval (Art. 22). Businesses relying on foreign cloud or group systems should review these arrangements first.

## **Enforcement and Penalties**

The Authority may issue an enforcement order allowing at least 21 days to comply, with a right of appeal (Art. 55). Complaints are decided within 21 days and appealable to the Federal High Court within 60 days (Art. 58). Administrative fines of up to four per cent of turnover apply where the offence is by an institution or concerns sensitive or children’s data (Arts. 59–60).

Criminal penalties (Art. 64) are one to three years’ simple imprisonment or Birr 60,000–100,000 for failing to notify a breach, secure data or follow the principles; three to five years or Birr 100,000–200,000 for denying erasure, objection, restriction or automated-decision rights; and five to ten years’ rigorous imprisonment or Birr 200,000–600,000 for re-identifying, selling or unlawfully transferring personal data.

## **What This Means Going Forward**

There is no grace period in the text: data already held must be processed in line with the Proclamation (Art. 68). Key details depend on Council of Ministers regulations and Authority directives (Art. 69), including registration requirements, critical data categories and fine amounts. Businesses should map their data, register, appoint a data protection officer where required, update notices and consent, prepare a 72-hour breach process, and review vendor, cloud and transfer arrangements.

### **Compliance Checklist**

- Map and classify the personal data you hold, and identify sensitive categories.
- Register with the Ethiopian Communications Authority before processing.
- Appoint a data protection officer where required.
- Refresh privacy notices and consent flows, and document your lawful bases.
- Stand up a 72-hour breach detection and notification process.
- Review cloud, vendor and cross-border transfer arrangements against Art. 22.

*This article is provided for general informational purposes only and does not constitute legal advice. For guidance specific to your circumstances, please contact Kiya & Associates Law Office.*