HIRKO & ASSOCIATES

Ethiopia's Data Sovereignty Regime: A Framework in Search of Enforcement

I. INTRODUCTION

On 24 July 2024, the Personal Data Protection Proclamation No. 1321/2024 (the "Proclamation") entered into force, establishing Ethiopia's first comprehensive legal framework for the protection of personal data. Among its most significant features is the recognition of data sovereignty as a statutory principle, introducing important requirements concerning the storage, processing, and cross-border transfer of personal data.

This legal update examines the principal data sovereignty and cross-border transfer requirements under the Proclamation, their practical implications for data controllers and processors, and the current state of implementation. The analysis is based on the legal framework currently in force and publicly available information as of August 2026.

II. DATA SOVEREIGNTY UNDER THE PROCLAMATION

The Proclamation expressly recognises data sovereignty as a fundamental principle of personal data protection. Article 6(7) requires personal data to be processed in a manner that ensures the sovereignty of the data. This principle is given practical effect through the Proclamation's requirements concerning local storage, critical personal data, and cross-border transfers.

The most significant requirement is contained in Article 22(1), which requires every data controller and processor to ensure that personal data collected or obtained locally is stored on a server or data centre located in Ethiopia. This establishes a general data localisation requirement and has potentially significant implications for organisations that rely on foreign cloud infrastructure or international data hosting arrangements.

The Proclamation also provides a stricter regime for categories of personal data that may be designated as "critical personal data." Under Article 22(2), the Ethiopian Communications Authority (ECA) may designate categories of personal data that must only be processed on servers or data centres located in Ethiopia. While the practical scope of this provision will depend on the categories ultimately designated by the ECA, it creates the possibility of a distinction between ordinary locally collected personal data, which is subject to local storage requirements, and critical personal data, which may be subject to broader localisation of processing activities.

A further restriction applies to sensitive personal data. Article 22(3) requires prior approval from the Authority for the cross-border transfer of sensitive personal data. This is particularly important for organisations whose operations involve health information, biometric or genetic information, religious or political information, criminal records, or other categories falling within the Proclamation's definition of sensitive personal data.

III. CROSS-BORDER TRANSFER OF PERSONAL DATA

The Proclamation does not impose an absolute prohibition on international transfers of personal data. Instead, it establishes a controlled framework under which transfers may take place where the required conditions and safeguards are satisfied.

Articles 18 and 19 establish an adequacy-based approach. A transfer may be permitted where the destination jurisdiction provides an appropriate level of protection. In assessing adequacy, the Authority may consider factors such as the nature of the data, the purpose and duration of processing, the country of origin and destination, the legal framework applicable in the receiving jurisdiction, and the technical and organisational security measures available there.

Article 20 further identifies circumstances in which cross-border transfers may be permitted, including where adequate protection exists, where the data subject has provided informed and explicit consent, where the transfer is necessary for contractual purposes, or where it is justified by important public interests, legal claims, or the vital interests of the data subject.

The Authority may also require evidence that appropriate safeguards are in place and may prohibit, suspend, or impose conditions on a transfer where the relevant requirements are not satisfied. In circumstances where adequate safeguards cannot be demonstrated, the Proclamation provides for prior authorisation by the Authority.

Accordingly, organisations should not assume that the use of an internationally recognised cloud provider or the execution of a contractual arrangement with a foreign service provider automatically makes an international transfer lawful. The location of the infrastructure, the nature of the data, the purpose of the processing, the applicable safeguards, and the legal basis for the transfer must all be considered.

IV. REGULATORY AND INSTITUTIONAL FRAMEWORK

The ECA is the principal supervisory authority under the Proclamation. Its responsibilities include supervising compliance, maintaining the relevant register, investigating complaints, taking enforcement measures, and making adequacy determinations concerning foreign jurisdictions.

The Proclamation also establishes a registration framework for data controllers and processors. Article 33 requires controllers and processors to register with the Authority before processing personal data. The registration process is intended to provide the regulator with information concerning the categories of data processed, the purposes of processing, the categories of data subjects, cross-border transfers, and the technical and organisational measures adopted to protect personal data. Registration is subject to periodic renewal.

The institutional framework therefore places a substantial responsibility on the ECA not only to receive registrations but also to develop the regulatory mechanisms necessary to supervise data processing activities and international data flows.

V. KEY COMPLIANCE REQUIREMENTS

The Proclamation imposes a broader set of compliance obligations beyond data localisation and cross-border transfers. Organisations whose processing activities fall within the relevant thresholds may be required to designate a Data Protection Officer. Article 40 is particularly relevant to government bodies, organisations conducting large-scale and systematic monitoring, and entities involved in large-scale processing of sensitive personal data.

Organisations should also consider whether their processing activities require a Data Protection Impact Assessment. Article 47 requires a DPIA for processing operations that are likely to result in risks to the rights and freedoms of data subjects. This is particularly relevant to activities involving systematic evaluation or profiling, large-scale processing of sensitive personal data, or systematic monitoring of publicly accessible areas.

Breach management is another important area of compliance. Article 43 requires notification to the Authority within 72 hours after becoming aware of a personal data breach where the notification requirement is triggered. Where the breach is likely to result in a high risk to the rights and freedoms of data subjects, Article 44 also requires communication to the affected data subjects.

The Proclamation further incorporates the principle of data protection by design and by default. Article 49 requires appropriate technical and organisational measures to be incorporated into processing activities so that data protection principles are effectively implemented and only the personal data necessary for a particular purpose is processed by default.

VI. ENFORCEMENT AND SANCTIONS

The Proclamation establishes both administrative and criminal consequences for non-compliance. The ECA has authority to impose administrative fines, with particularly significant penalties applicable to institutional violations and certain violations involving sensitive personal data or data relating to minors. In serious cases, administrative fines may reach up to four per cent of the institution's total worldwide turnover for the preceding financial year.

The Proclamation also establishes criminal liability for certain violations. These include failures relating to breach notification and security measures, unlawful processing, violations of certain data subject rights, unlawful re-identification or sale of personal data, and unlawful cross-border transfers. Depending on the nature of the violation, the applicable penalties may include imprisonment and monetary fines.

The existence of these sanctions demonstrates that data protection under the Proclamation is not merely a matter of internal corporate governance. Non-compliance may create regulatory, financial, operational, and, in certain circumstances, criminal exposure.

VII. CURRENT IMPLEMENTATION STATUS

Although the Proclamation has established a comprehensive statutory framework, its practical implementation remains at an early stage. The ECA has taken steps toward establishing the institutional and technological infrastructure required for implementation, including work relating

to the registration of data controllers and processors and the development of supporting regulatory instruments.

However, significant elements of the framework remain to be operationalised. Publicly available information indicates that the registration mechanism and supporting directives have been under development, while formal adequacy determinations for foreign jurisdictions and designations of critical personal data remain important outstanding regulatory matters.

There is also limited publicly available evidence of extensive enforcement through administrative fines, enforcement notices, or criminal proceedings under the Proclamation. This creates a distinction between the legal obligations established by the Proclamation and the current level of regulatory enforcement.

The absence of extensive enforcement activity, however, should not be interpreted as suspension of the law. The Proclamation remains the applicable legal framework, and organisations should therefore approach compliance on the basis that its requirements may increasingly be enforced as the ECA's regulatory capacity develops.

VII. CURRENT IMPLEMENTATION STATUS

Although the Proclamation establishes a comprehensive statutory framework for personal data protection and data sovereignty, its practical implementation remains at an early stage. The principal challenge is not the absence of a legal mandate, but the limited operationalisation of the institutional framework and regulatory powers contemplated by the Proclamation.

The ECA has been designated as the principal supervisory authority and has been vested with significant responsibilities, including registration of data controllers and processors, supervision of compliance, investigation of complaints, issuance of enforcement measures, making adequacy determinations, and exercising other regulatory powers provided under the Proclamation. However, as of August 2026, these functions do not appear to have been fully operationalised to the extent contemplated by the Proclamation. The Authority's existing institutional structure and operational capacity have not yet developed into a fully functioning data protection supervisory regime corresponding to the breadth of powers assigned to it under the Proclamation.

This is particularly evident in relation to the mechanisms necessary for the effective implementation of the data sovereignty regime. The registration framework for data controllers and processors, the issuance of supporting regulatory instruments, the determination of adequate jurisdictions, and the designation of categories of critical personal data remain important elements of the framework requiring further operationalisation. Consequently, there remains a significant gap between the statutory responsibilities assigned to the ECA and the practical exercise of those responsibilities.

The limited operationalisation of the ECA's data protection functions has also affected the practical enforcement of the Proclamation. There is currently limited publicly available evidence of systematic supervisory activities, enforcement notices, administrative fines, or prosecutions specifically undertaken under the Proclamation. This should not, however, be understood as

meaning that the Proclamation is legally inoperative or that its obligations are suspended. Rather, it reflects the current gap between the enactment of the legal framework and the development of the institutional and regulatory mechanisms required for its effective implementation.

The situation therefore presents a notable implementation gap. Ethiopia has enacted a relatively comprehensive statutory framework establishing data protection, data localisation, and cross-border transfer requirements, while the institutional infrastructure necessary to administer, supervise, and enforce those requirements remains in the process of development. The effectiveness of the regime will consequently depend not only on the existence of the Proclamation but also on the ECA's ability to establish the necessary organisational structures, procedures, technical capacity, registration mechanisms, regulatory instruments, and enforcement practices contemplated by the law.

For organisations subject to the Proclamation, the current implementation gap should not be treated as an exemption from compliance. Businesses should continue to assess their data processing activities against the requirements of the Proclamation and prepare for the progressive operationalisation of the regulatory regime. In particular, organisations handling significant volumes of personal data or engaging in international data transfers should consider the present period as an opportunity to address compliance gaps before the Authority's supervisory and enforcement functions become fully operational.

Finally, entities should ensure that their internal governance arrangements are capable of responding to data protection incidents and regulatory inquiries. This includes establishing breach escalation procedures, reviewing contracts with processors, assessing whether a Data Protection Officer is required, and conducting DPIAs for high-risk processing activities.

IX. CONCLUSION

Proclamation No. 1321/2024 establishes a significant legal foundation for data protection and data sovereignty in Ethiopia. Its local storage requirement, the potential localisation of critical personal data, and the restrictions applicable to international transfers collectively create a regulatory framework that organisations cannot reasonably disregard.

At the same time, the effectiveness of the framework will depend substantially on the continued development of the ECA's institutional capacity, the issuance of supporting regulatory instruments, the operationalisation of registration mechanisms, the determination of adequate jurisdictions, and the commencement of consistent supervisory enforcement.

For businesses, particularly financial institutions, fintech companies, telecommunications operators, technology companies, healthcare providers, and other organisations handling significant volumes of personal data, the appropriate approach is therefore to prepare for effective enforcement rather than wait for it. Mapping data flows, reviewing cloud arrangements, assessing international transfers, strengthening security controls, and establishing internal data protection governance can significantly reduce future regulatory exposure.

Ethiopia's data sovereignty regime is therefore no longer merely a legislative concept. The statutory framework is already in place. The principal question is now how quickly the remaining institutional and regulatory mechanisms will develop to give the framework full practical effect.

Disclaimer

This legal update is provided for informational purposes only and does not constitute legal advice. Organisations should obtain specific legal advice based on their particular data processing activities, technology infrastructure, contractual arrangements, and regulatory obligations.