FACTSHEET: ETHIOPIA

Last updated: 31 March 2020
Prepared by Justin Bryant
Revised by Tshepiso Hadebe

FAST FACTS

Population: 114,001,984
Capital: Addis Ababa
Prime Minister: Abiy Ahmed Ali
2019 Freedom House Score: 19/100
Data Protection Law? No

LAW

Although the right to privacy is enshrined in the Ethiopian constitution, the current laws do not provide full protection to this right, especially in the realm of personal data. While Ethiopia circulated a draft comprehensive data protection law in 2009, the past decade has seen no implementation of such a law.

PERSONAL DATA

The Freedom of the Mass Media and Access to Information Proclamation No. 590/2008, which applies to public bodies, identifies the following categories of information about an identifiable individual as *personal data*:

- medical, education, academic, employment, financial transaction, professional or criminal history;
- ethnic, national or social origin, age, pregnancy, marital status, colour, sexual orientation, physical or mental health, wellbeing, disability, religion, belief, conscience, culture, language, or birth;
- an identification number, symbol, or other identifier assigned to the individual, address, fingerprints, or blood type;
- personal opinions, views, or preferences, except as they relate to another individual;
- views or opinions on grant proposals, awards, or prizes granted to another individual, provided such views or opinions are not associated with the other individual's name;
- views or opinions of others about the individual; or
- an individual's name, in combination with other personal data, or alone, if it could reasonably be linked to personal data. (An exception applies for persons deceased for more than 20 years.)

COLLECTION AND PROCESSING

Personal data. must be collected and processed with due care and only for an intended lawful purpose.

REGISTRATION AND ENFORCEMENT

There is no data protection authority or scheme for registration of data controllers.

CROSS-BORDER TRANSFER

Personal data transfers must occur for an intended lawful purpose with the prior written consent of the data subject.

SECURITY AND BREACH PROTOCOL

The Computer Crime Proclamation No. 958/2016 mandates that service providers implement reasonable and necessary security measures to protect confidential network data from unlawful and unnecessary access. Upon the discovery of a breach, they must immediately notify the Information Network Security Agency and the police and take appropriate steps toward rectification.

Read the legal notice and terms of use for this factsheet.