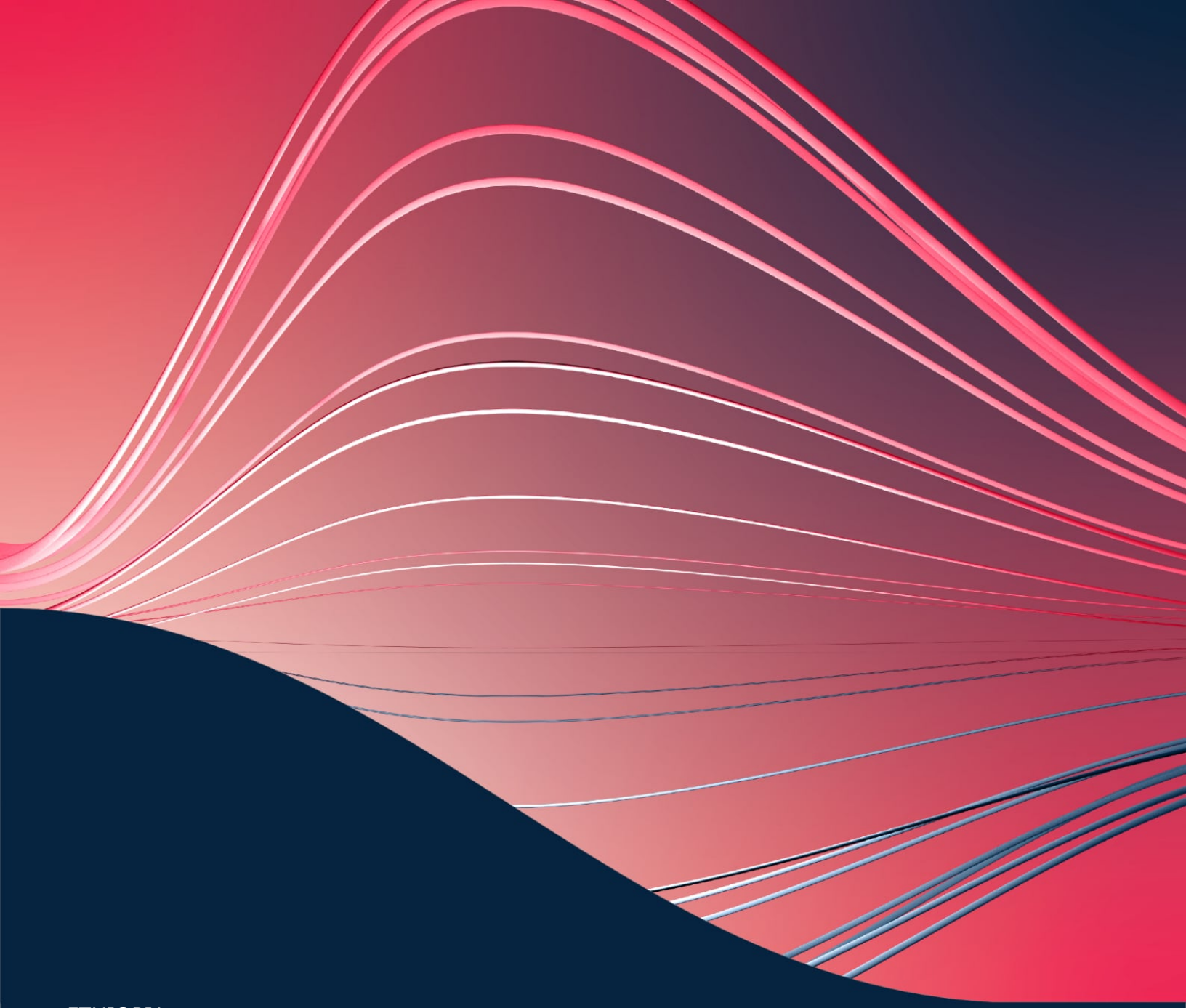


ETHIOPIA

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. As we step into 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

Europe

Established data protection laws in Europe continue to evolve through active regulatory guidance and enforcement action. In the United Kingdom, the UK government has proposed reforms to data protection and e-privacy laws through the new Data (Use and Access) Bill ("**DUAB**"). The DUAB follows the previous government's unsuccessful attempts to reform these laws post-Brexit, which led to the abandonment of the Data Protection and Digital Information (No.2) Bill ("**DPDI Bill**"), in the run-up to the general election. Although the DUAB comes with some bold statements from the government that it will *"unlock the power of data to grow the economy and improve people's lives"*, the proposals represent incremental reform, rather than radical change.

United States

In the United States, legislation on the federal and in particular state level continues to evolve at a rapid pace. Currently, the US has fourteen states with comprehensive data privacy laws in effect and six state laws will take effect in 2025 and early 2026. Additionally, at the federal level, the new administration has signaled a shift in enforcement priorities concerning data privacy. Notably, there is a renewed focus on the regulation of artificial intelligence (AI), with an emphasis on steering away from regulation and promoting innovation. This includes the revocation of previous executive orders related to AI and the implementation of new directives to guide AI development and use.

In the realm of children's privacy, many of the new administration's supporters in Congress have indicated a desire to make the protection of children on social media a top priority, and new leadership at the Federal Trade Commission (FTC) appears aligned on this goal, albeit with a willingness to take another look at the recently adopted amendments to the Children's Online Privacy Protection Act (COPPA) Rule. Health data

privacy remains a critical concern, with a handful of states following Washington state's lead in enhancing or adopting health data privacy laws. On the international data transfer front, Executive Order (E.O.) 14117 " Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" as supplemented by the DOJ's final Rule will impact companies transferring data into certain jurisdictions, such as China, Iran and Russia. Another area of focus for companies with an EU presence will be the Trump administration's approach to the Privacy and Civil Liberties Oversight Board, as it is a critical pillar of the EU/UK/Swiss-US Data Privacy Framework.

Asia, the Middle East, and Africa

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia, with new laws in India, Indonesia, Australia and Saudi Arabia, as well continued new data laws and regulations in China and Vietnam. The ever-evolving data laws, as well as the trend towards regulating broader data categories (beyond personal data), in these regions continue to raise compliance challenges for multi-national businesses.

Emerging trends in data governance

Unlocking data, regulating the relentless advance of AI, creating fairer digital markets and safeguarding critical infrastructure against the ever growing cyber threat, continue to impact and overlap with the world of data protection and privacy. Perhaps most notably, the EU have introduced a raft of new laws forming part of its ambitious digital decade, which will bring huge change to businesses operating within the EU. With the rapid adoption of artificial intelligence enabled solutions and functionality, data protection supervisory authorities have been closely scrutinising the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate date protection compliance into the core design and functionality of their AI systems. In the midst of this, the privacy community found itself at the centre of an emerging debate about the concept of 'AI governance'. This is not a surprising development – AI systems are creatures of data and the principle-based framework for the lawful use of personal data that sits at the heart of data protection law offers a strong starting point for considering how to approach the safe and ethical use of AI. As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services to enrich data. Whilst privacy professionals cannot tackle the AI challenge alone, expect them to continue to be on the front lines throughout 2025 and beyond.

Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

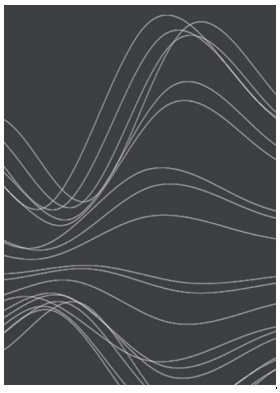
Africa key contact

Monique Jefferson
Director
monique.jefferson@dlapiper.com
Full bio

Americas key contact

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

Andrew Dyson
Partner
andrew.dyson@dlapiper.com
Full bio

Ewa Kurowska-Tober
Partner
Head of Intellectual Property and Technology, Poland
ewa.kurowska-tober@dlapiper.com
Full bio

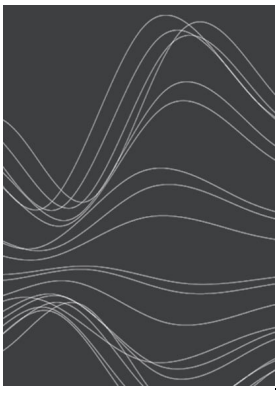
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Middle East key contact

Rami Zayat
Partner
rami.zayat@dlapiper.com
Full bio

Editors

Kate Lucente
Partner
kate.lucente@us.dlapiper.com
Full bio



Lea Lurquin
Associate
lea.lurquin@us.dlapiper.com
Full bio

Ethiopia

LAST MODIFIED 12 JANUARY 2023

Data protection laws

Ethiopia has several laws that relate to privacy and data security, including:

- The 1995 Constitution of the Federal Democratic Republic of Ethiopia;
- Tthe 2005 Criminal Code of the Federal Democratic Republic of Ethiopia:
- The 1960 Civil Code, the Computer Crime Proclamation No. 958/2016;
- Freedom of the Mass Media and Access to Information Proclamation No. 590/2008 (as amended by the Media Proclamation No. 1238/2021);
- Federal Advocacy Service Licensing and Administration Proclamation No.1249/2021;
- Telecom Fraud Offence Proclamation No. 761/2012;
- Registration of Vital Events and National Identification Cards Proclamation No. 760 /2012 (as amended);
- Federal Tax Administration Proclamation No.983/2016;
- Authentication and Registration of Documents' Proclamation No.922/2015;
- Electronic Signature Proclamation No.1072/2018;
- Communications Service Proclamation No.1148/2019;
- Electronic Signature Proclamation No.1072/2018;
- Electronic Transaction Proclamation No.1205/2020;
- National Bank of Ethiopia (NBE) Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020;
- NBE Financial Consumer Protection Directive No. FCP/01/202

Definitions

Definition of Personal Data

No specific definition is generally applicable.

The Freedom of the Mass Media and Access to Information Proclamation No. 590 /2008, applicable to government entities, is understood to generally define personal data as information about an identifiable individual that relates, but is not limited, to:

- medical, education, academic, employment, financial transaction, professional or criminal history
- ethnic, national or social origin, age, pregnancy, marital status, color, sexual orientation, physical or mental health, well-being, 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 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 could reasonably be linked to personal data (exception applies for persons deceased for more than 20 years).

Ethiopian Communications Authority's Consumers Rights and Protection Directive 2020 defines personal information as private information and record relating to consumers leading to identify such consumer such as his identity, address or telephone number and / or traffic and billing data and / or other personal information.

Definition of Sensitive Personal Data

Sensitive personal data is not defined.

National data protection authority

There is no data protection authority.

Registration

There is no requirement to register databases or personal data processing activities.

Data protection officers

There is no requirement to appoint a data protection officer.

Collection and processing

Though Ethiopia has not enacted a specific law to address personal data collection and processing issues, the country's scattered legislative framework is understood to require that personal data be collected and processed with due care and only for an intended lawful purpose. Obtaining express consent for collecting and processing of personal data is also a requirement under those scattered provisions.

Transfer

No specific geographic transfer restrictions apply in Ethiopia.

However, existing law provides that personal data transfers must be based on the prior written consent of the person whose data is to be transferred and only for an intended lawful purpose.

Security

There are no specific data security requirements.

The Computer Crime Proclamation No. 958/2016 requires service providers to implement reasonable and necessary security measures to protect confidential computer traffic data disseminated through their computer systems or communications services from unlawful and unnecessary access.

Ethiopian Communications Authority's Sim Card Registration Directive requires Telecommunication Operators to take all reasonable steps to ensure the security and confidentiality of its subscribers' registration details.

Breach notification

There is no general breach notification requirement in Ethiopia.

However, the Computer Crime Proclamation No. 958/2016 requires service providers with knowledge that a crime stipulated by the Proclamation (including breach of privacy via unauthorized access) has been committed by a third party through the computer system it administers to immediately notify the Information Network Security Agency, report the crime to police, and take appropriate measures.

Ethiopian Communications Authority's Sim Card Registration Directive under Article 24 obliges a telecommunication operator to notify the Ethiopian Communications Authority of any data breach that compromises subscribers' information within seven (7) business days from discovery of the breach. The operator shall also notify the affected subscriber of such breach.

Enforcement

Ethiopian courts are responsible for enforcing data protection and privacy provisions in the law.

Electronic marketing

Electronic Transaction Proclamation No.1205/2020 backed by Electronic Signature Proclamation No.1072/2018 regulate aspects of electronic marketing in addition to general contract law and commercial law provisions.

Online privacy

There are several provisions in Ethiopian law to regulate online privacy. For example, the Computer Crime Proclamation No. 958/2016 criminalizes the unauthorized access to, and illegal interception and damage of, computer data.

The Proclamation further prohibits the use of computer systems to disseminate advertisements absent addressee consent.

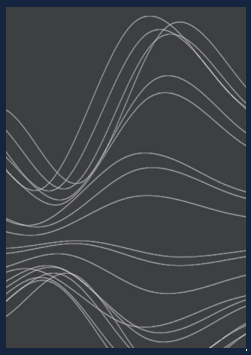
The new Media Proclamation obliges online Media to protect the data of users and obtain explicit consent from users when circumstances requiring users' data to be made available to third parties.

Data protection lawyers

Benyam Tafesse
Head, Employment, IP & Aviation Practices
Mehrteab Leul & Associates
benyam@mehrteableul.com

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com