LIBERIA

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.

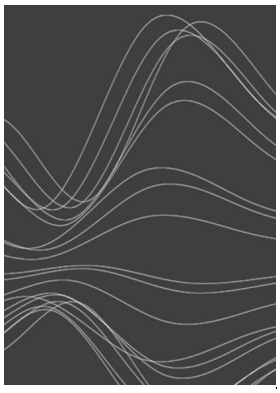
Africa key contact

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

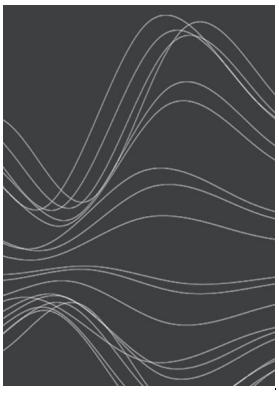
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

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

Liberia

LAST MODIFIED 23 FEBRUARY 2024

Data protection laws

Data Privacy Protection Laws.

Definitions

Definition of Personal Data

Personal Data is not defined by existing laws. Data is however, defined variously by different statutes and legal instrument in Liberia as follows:

- Financial Intelligence Unit Act of 2012: "Data" means: *representations, in any form, of information or concepts".*
- Central Bank of Liberia ("CBL") E-Payment Regulation: "Data integrity" means *"the assurance that information that is in-transit or in storage is not altered without authorization"*
- The ECOWAS Supplemental Act of which, Liberia is a signing member defines personal data as *"any information relating to an identified individual or who may be directly identifiable by reference to an identification number or one or several elements related to their physical, physiological, genetic, psychological, cultural, social, or economic identity".* Accordingly, it can be concluded that that (i) cards numbers and (ii) account numbers from which a person can be directly identified qualify as sensitive personal information / data.

Definition of Sensitive Personal Data

There is no Liberian law that defines sensitive persona data.

National data protection authority

No specific national data protection agency or authority exists in Liberia, and besides a broad statement in the Liberian Constitution that *"no person shall be subjected to interference with his privacy of person, family, home or correspondence except by order of*

a court of competent jurisdiction", there is no dedicated privacy law whether of person or in respect of data, not to mention any dedicated data protection authority.

Admittedly, Liberia is a signatory to The ECOWAS Supplemental Act of which, requires member States, including Liberia, to establish National Data Authority within their jurisdiction. However, Liberia has not yet established such authority.

Registration

In terms of "Spatial Data", Liberia Institute of Statistics and Geo-Information Services (LISGIS) is the public agency responsible for the collection of statistical and geographic information that are used to produce maps."

However, entity(ies) whose business requires the collection of data are required to register and receive the requisite permit / license from the government entity controlling / overseeing the sector in which the entity(ies) would be conducting business. Every permit / license issued by the requisite government authority is renewable.

Data protection officers

There is no known or publicly designated Protection Officer, or Officers in Liberia. In the same vein, there is no law requiring the appointment or creation of such posts whether in public or private entities dealing with data.

Collection and processing

Section 5.15.1 of the National Information and Communications Technology Policy of 2019 regulates the lawful processing of personal data. Its states that:

a. Personal data will be processed fairly and lawfully;
b. Personal data will be obtained only for one or more specified and lawful purposes, and will not be further processed in any manner incompatible with their purpose or those purposes;
c. Personal data will be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
d. Personal data will be accurate and where necessary, kept up to date;
e. Personal data processed for any lawful purpose or purposes will not be kept for longer than is necessary for that purpose or those purposes;
f. Appropriate technical and organizational measures will be taken against unauthorized or unlawful processing of personal data and the protection of children;
g. Data collectors will be required to disclose use of personal data to consumers.
h. Collected personal data will be rigorously protected from unauthorized access by any Parties.

Section 51(5) of the Telecommunication Act states that "Service providers shall ensure that customer information and customer communications are protected by security safeguards that are appropriate to their sensitivity".

Section 3.1.1 of the 2017 AML / CFT Regulations for Financial Institutions in Liberia states that "financial institutions shall obtain and maintain documentary records for each client or customer to verify by reliable and independent source documents (such as a passport, a driver's license, or national identification documents)".

Section 3.1.7 of the 2017 AML / CFT Regulations for Financial Institutions in Liberia provides that the required KYC information must be collected before financial institutions establish any relationship with a person. That is, prior to opening a bank account or performing walk in transactional services for non-account holders

Transfer

The transfer of data out of Liberia is not specifically addressed by any Liberian law. However, Article 36 of the ECOWAS Act, as relied on in Liberia as a secondary source of law, restricts data controller from transferring personal data outside an ECOWAS country except said non-member ECOWAS country provides "*an adequate level of protection for privacy, freedoms and the fundamental rights of individuals in relation to the processing or possible processing of such data*". In such a case, the data controller shall notify the Data Protection Authority, which is the Liberia Telecommunications Authority (LTA), prior to transferring any personal data.

Section 9(c) of the CBL E-Payment Regulation (though governing the Banking and Finance sector of Liberia, provides that "*the system (used or being used) should be hosted locally to provide ease of support and guarantee data ownership; however, if the system is hosted in another jurisdiction, licensed institutions shall ensure that the information requested are provide promptly and that the CBL has unfettered access to reports generated by the system*".

Security

Section 9.1 of the CBL Regulations Concerning the Licensing and Operations of Electronic Payment Services in Liberia ("E-Payment Regulation") provides as follows:

- *"All e-payment service providers shall ensure that personal information of customers obtained during the course of operations is used, disclosed, retained and protected as agreed";* and
- *"They shall ensure the security, Integrity, Confidentiality and Availability of data and services by adopting prevailing international standard(s) as well as those prescribed by Central Bank of Liberia from time to time."*

Breach notification

There is generally no breach notification requirement, nor any dedicated agency or entity to which such notification must be made.

Mandatory breach notification

Whenever a private action is contemplated through the courts, it is mandatory that the accused is apprised of the matter in order to inform the prospective defendant of the allegation against him or her. This is usually accomplished through the issuance of the appropriate Writ issued by the court which is served upon the Defendant.

Enforcement

Enforcement is generally by a private right of action, but there are few administrative sanctions under some statutes and regulations, such as regulations governing the financial, insurance and telecommunications sectors, for violation of customer privacy by divulging confidential information without authorization.

Electronic marketing

Section 13.46(1) of the Liberia Electronics Transaction Law (2002) states that: *"a person who has access to any record, book, register, correspondence, information, document or other material in the course of performing a function under or for the purposes of this Law shall not disclose or permit or suffer to be disclosed such record, book, register, correspondence, information, document or other material to any other person".* However, Section 13.46(2) of the Act provides that the above-quoted provision of Sub-section 1 does not apply to disclosure:

- Which is necessary for performing or assisting in the performance of a function under or for the purposes of this Law;
- For the purpose of any criminal proceedings in Liberia or elsewhere;
- For the purpose of complying with a requirement made under a rule of law with a view to instituting a criminal proceeding in Liberia or elsewhere; or
- Under the direction or order of a court.

Online privacy

There are no specific provisions under Liberian laws relating to on-line privacy. However, data collectors are required to exercise the maximum protection of consumer's protection and shall not disclose any information about a consumer to a third party except where (i) the institution is required by law to disclosed such information, or (ii) the disclosure is made with the expressed consent of the consumer. Data collectors are required to ensure the integrity and adequacy of their IT and Security system.

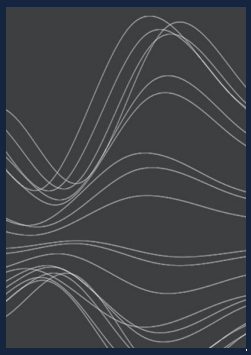
Data protection lawyers

Cllr. Mark M.M. Marvey
Partner
Heritage Partners & Associates Inc.
mmarvey@hpaliberia.com

Atty. Beyan G. Mulbah
Associate
Heritage Partners & Associates Inc.
bmulbah@hpaliberia.com
View bio

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