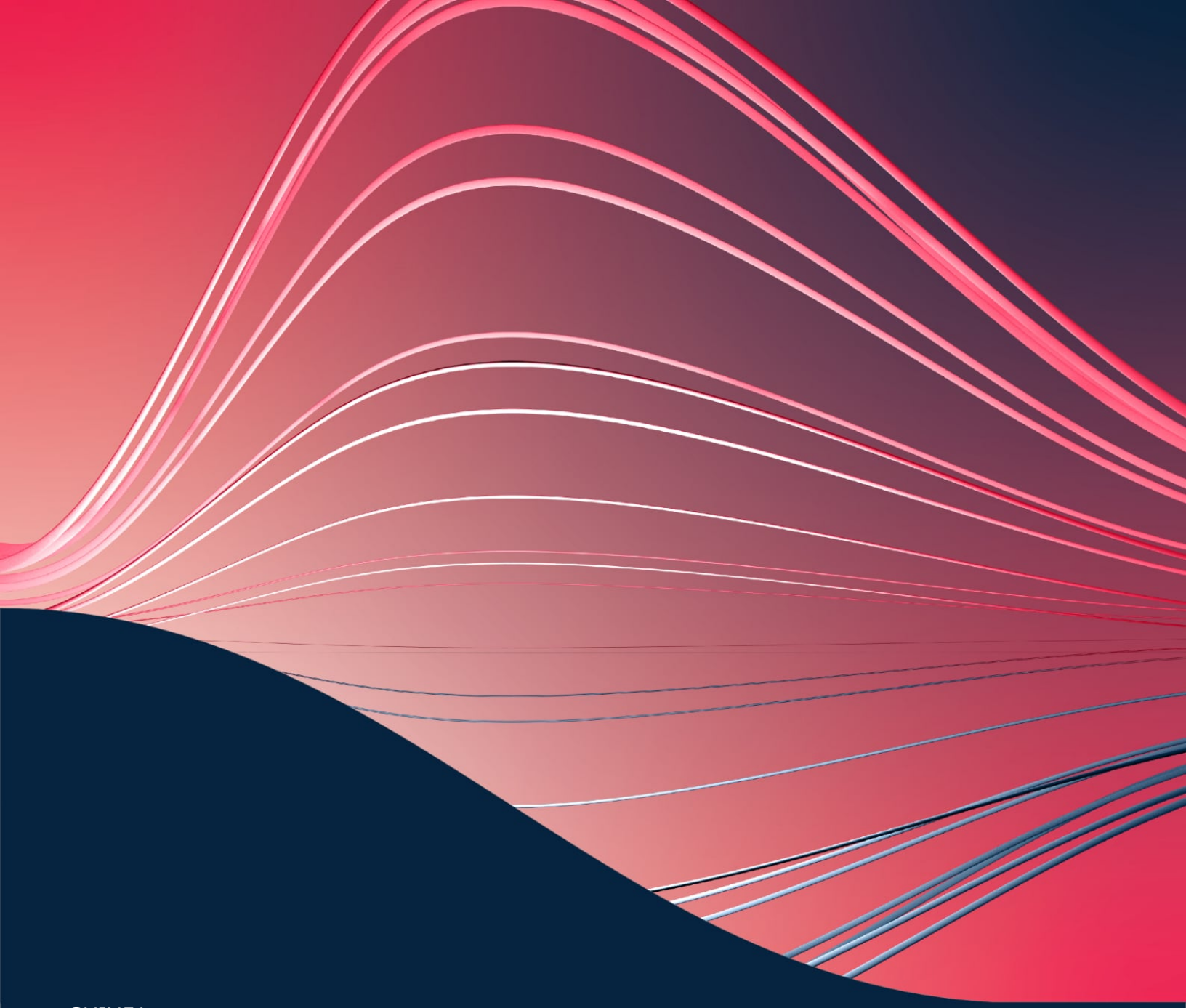


GUINEA

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.

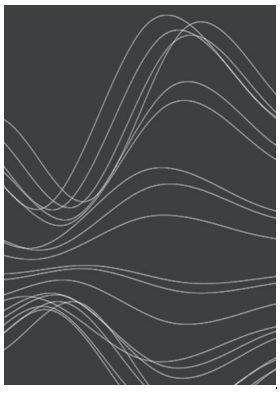
Africa key contact

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

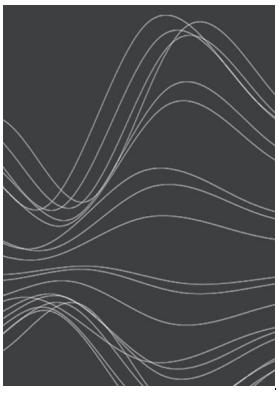
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

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

Guinea

LAST MODIFIED 20 DECEMBER 2021

Data protection laws

Law n° L/2016/037/AN dated July 28, 2016, on Cybersecurity and Personal Data Protection in the Republic of Guinea regulates personal data.

Definitions

Definition of personal data

Article 1 of Law No. L/2016/037/AN defines personal data as any information of any kind and regardless of its medium, including sound and image, relating to an identified or identifiable natural person directly or indirectly, by reference to an identification number or to one or more factors specific to his or her physical, physiological, genetic, mental, cultural, social or economic identity.

Definition of sensitive personal data

According to Article 1 of Law No. L/2016/037/AN, sensitive data is all personal data, relating to religious, philosophical, political, trade union opinions or activities, sexual or racial life, health, social measures, prosecution, criminal and administrative sanctions.

National data protection authority

It is provided for by Article 47 of Law on Cybersecurity and Personal Data Protection in the Republic of Guinea that the authority in charge of personal data protection shall be established by regulatory means. The establishment of this authority is still not effective.

Registration

Law on Cybersecurity and Personal Data protection in the Republic of Guinea provides that the processing of personal data is subject to a prior declaration or request for authorisation of the competent authority designated by regulation.

The declaration or request for authorisation may be sent to the authority in charge of personal data protection by post, in person at the premises of the said authority or by any other means against the delivery of an acknowledgment of receipt in due form.

The authority in charge of personal data protection has a period of two months to decide on any declaration or request submitted or addressed to it. This period may be extended by two additional months provided that the personal data protection authority can justify its decision or the extension.

The declaration or request for authorisation must include the commitment that the protection meets the requirements of the law on Cybersecurity and Protection of Personal Data and any other regulations or laws in the Republic of Guinea relating to personal data protection.

At the end of this declaration, the competent authority issues a receipt and, if necessary, by electronic means.

The applicant may then implement the processing operation upon receipt of the receipt. However, the applicant is not relieved of any responsibility.

Processing operations carried out by the same organisation and having identical or related purposes may be subject to a single declaration. The information required under the declaration shall be provided for each of the processing operations only insofar as it is specific to said declaration.

Law on Cybersecurity and Personal Data Protection also provides that the modalities for filing declarations or request for authorisation for the processing of personal data shall be determined by presidential decree. This decree has not yet been implemented.

Data protection officers

A data controller will have the option to appoint a data protection officer. According to article 14 and following of Law on Cybersecurity and Personal Data Protection, the data protection officer must be a person qualified to perform such tasks. He must keep a list of the processing operations carried out which is immediately accessible to any person who requests it, and may not be subject to any sanction by his employer as a result of the performance of his duties.

The appointment of a data protection officer by the data controller must be notified to the authority responsible for personal data protection. This appointment must also be brought to the attention of the employer's staff representative bodies.

Collection and processing

Law on Cybersecurity and Personal Data Protection exempts the processing of personal data from the formalities of declaration, notably in the case of:

- Processing of data used by a natural person exclusively in the course of his or her personal, domestic or family activities;

- Processing of data concerning a natural person, the publication of which is prescribed by a legal or regulatory provision;
- Processing of data whose sole purpose is the keeping of a register which is intended for exclusively private use; etc.

Furthermore, it is also provided that certain matters or actions are subject to prior authorisation by the competent authority before being implemented, these include:

- Processing of personal data relating to genetic and medical data and scientific research in these fields;
- Processing of personal data relating to offences, convictions and security measures pronounced by the competent courts;
- Processing of personal data relating to a national identification number or any other identifier of the same kind, in particular telephone numbers;
- Processing of personal data containing biometric data;
- Processing of personal data for reasons of public interest, in particular for historical, statistical or scientific purposes;
- The proposed transfer of personal data to a third country.

Requests for processing shall be submitted by the controller or his/her legal representative. However, the authorisation does not exempt its holder (data controller) or his representative from their responsibility towards third parties.

Transfer

The data controller may be authorised to transfer such data to a third country only if the State ensures a higher or equivalent level of protection of the privacy, fundamental rights and freedoms of individuals with regard to the processing to which such data is or may be subject.

Before any effective transfer of personal data to the third country, the data controller must obtain prior authorisation from the personal data protection authority. Any transfer of personal data to a third country is subject to strict and regular control by the personal data protection authority, in the light of its purpose.

Security

According to Law on Cybersecurity and Personal Data Protection, the processing of personal data is confidential, it must be carried out exclusively by persons acting under the authority of the Data controller, and only on his instructions.

The Data controller is required to take all necessary precautions, in view of the nature of the data, and in particular to prevent it from being distorted, damaged or accessed by unauthorised third parties.

Breach notification

Law on Cybersecurity and Personal Data Protection provides that the authority in charge of personal data protection may pronounce the following measures against the Data controller:

- A warning to the said controller who does not comply with the obligations resulting from the Law on cybersecurity and Personal Data Protection to which he is subject;
- A formal notice or summons to cease or to cease the breaches noted, within the time limit set by said protection authority.

Enforcement

Law on cybersecurity and Personal Data Protection sets out administrative, criminal, recidivism and civil liability as well as additional publication of sanctions for breaches of the provisions of said statute.

Electronic marketing

Law L/2016/035/AN on electronic transactions in the Republic of Guinea provides that any advertisement, whatever its form, as soon as it is accessible or likely to be accessible by electronic communications, must be clearly identified as an advertisement. It must also allow the identification and identifiability of the natural or legal person on whose behalf it is made.

Advertisements and notably promotional offers, such as discounts, premiums or gifts, as well as competitions or promotional games, sent by electronic mail, must be clearly, precisely and unequivocally identifiable on the subject of the mail as soon as they are received by the addressee or, if technically impossible, in the body of the message.

The conditions for taking advantage of promotional offers, as well as for participating in promotional courses or games, when offered by e-mail, should be clearly specified and easily accessible to the public.

Pursuant to Law on electronic transactions in the Republic of Guinea, direct marketing by sending messages through an automatic calling machine or SMS, fax or e-mail or any other electronic means of communication using, in whatever form, the contact details of a natural person who has not expressly given his or her prior consent to receive direct marketing through these channels or means is prohibited.

However, direct marketing by e-mail, regardless of the means used, is permitted if:

- The contact details of the recipient of the mail have been collected, with full knowledge of the facts, directly from him/her;
- The direct prospecting is addressed to subscribers or customers of a natural or legal person whose details have been collected with their full knowledge of the facts, for similar products and services that it offers them.

Online privacy

The Law on Cybersecurity and Personal Data Protection does not provide any specific rules governing online privacy.

However, the law prohibits and punishes with a prison sentence of one (1) to five (5) years and a fine of 30,000,000 to 200,000,000 Guinean francs for carrying out or attempting to carry out direct prospecting by any means of communication using, in any form whatsoever, the personal data of a natural person who has not expressed his /her prior written consent.

In particular, it provides that any person has the right to object, on request and free of charge, to the processing of personal data concerning him or her and intended for prospecting purposes.

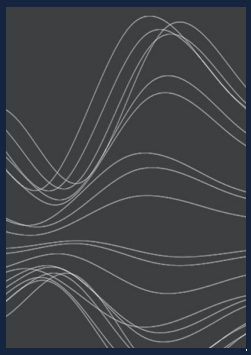
Data protection lawyers

Mohamed Sidiki Sylla
Managing Partner
Sylla & Partners
msylla@syllapartners.com
View bio

Alpha Toubab Millimono
Associate
Sylla & Partners
amillimono@syllapartners.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