EQUATORIAL 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.

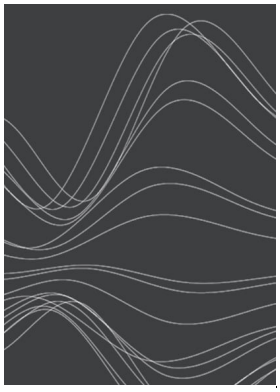
Africa key contact

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

Americas key contact

Andrew Serwin
Partner
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

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

Ewa Kurowska-Tober
Partner
ewa.kurowska-tober@dlapiper.com
Full bio

John Magee
Partner
john.magee@dlapiper.com
Full bio

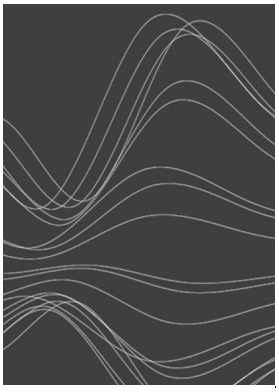
Middle East key contact

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

Editors

James Clark
Partner
james.clark@dlapiper.com
Full bio

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



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

Equatorial Guinea

LAST MODIFIED 6 MARCH 2025

Data protection laws

The applicable law is the Personal Data Protection Law Num. 1/2016 dated 22 July.

Definitions

Definition of Personal Data

The Personal Data Protection Law under art.4 defines personal data as *"any information, testimony or review concerning a person specifically identified or identifiable"*.

Definition of Sensitive Personal Data

The law does not provide a definition of sensitive personal data. However, art.41(d) consider as a mayor infringement the treatment or given out of personal data in relating to conscience liberty, affiliation or political ideology, health, sex life, race, tribe, religion or any other discrimination form without the express authorization of the owner.

National data protection authority

The Governing Data Protection Body.

Registration

The General Data Protection Registry (art. 33) is the organ responsible for registration under its Technical Secretariat which takes charge of the registration of public and private personal data files and of carrying out all actions entailing the modification, creation or suppression of personal data through authorised books.

Data protection officers

The Governing Data Protection Body through its Technical Secretariat is responsible for ensuring the administration of personal data files, regardless of their ownership, is done in due compliance with the provisions of the law.

Collection and processing

Arts. 6 and 9 of the applicable law determines that only personal data that are adequate, accurate, truthful, complete and not excessive in relation to the scope and purpose of their collection may be used, prohibiting the collection of such data by fraudulent and unlawful means.

In this regard, an interested parties to whom personal data are requested must be previously expressly informed in a concise and unequivocal manner and must be informed about the purpose and consequences of the collection, the destination and the recipients of the information, about the mandatory or optional nature of their response to the questions asked, about the effects of the refusal to provide them, as well as the identity and address of the person responsible for the processing or its representative.

The processing of data by third parties according the law must be subject to a contractual agreement under which a third parties must agree in writing to process the data solely and in accordance with the instructions authorised by the owner, that is, the data must not be used or applied for a different purpose or communicated to third parties (art.8).

Transfer

Art. 21 is to the effect that:

- Personal data obtained by the General administration of the state cannot be communicated or given out unless it is for historic or, statistics of scientific purposes. However, personal data could be communicated between the public administration and other public organs or institutions.
- Private holders of personal data cannot communicate or give out personal data found in their possession unless by a court order instructed by a competent court.
- For the performance of any of the above, the holders of the data have to be notified of the purpose for which their data is to be communicated or given out. Notwithstanding, consent will not be needed from the owner of the data unless the data was made available to the public, and it is likely to be communicated to other public or private files.

Security

Art. 11 determines that, the data controller or data processor must adopt the necessary technical and organisational measures to ensure the security of the personal data processed, ensuring their preservation and avoiding their alteration, loss, unauthorised processing or access. In this sense, personal data must not be recorded in files, systems or processing centres that do not meet the security conditions for the integrity, confidentiality and guarantee of the same.

Breach notification

The breach of notification constitutes a minor infringement when the data was obtained from the person concerned (art. 39 C) and a major infringement when the data was not obtained from the person concerned (art. 40 C).

Mandatory breach notification

The law does provide for a mandatory breach duty. Notwithstanding, it provides that in the case of a severe or major breach likely to affect a fundamental right or personal data the sanctioning organ may require the person responsible to restrain the use, communication, give out, or the illegal transfer.

Enforcement

The enforcement process applied to determine and impose the sanctions is adjusted to the principles, rules and norms of administrative procedure at the request of an audience by the interested party. During the audience, other enforcement measures can be adopted by the sanctioning organ to ensure compliance of the final resolution and to secure the application of the sanctions. However, these measures have a provisional character (art.45).

Where the infringement is committed in a public file, the sanctioning organ has to pass a resolution ordering the dismissal or correction of the infringement, as well as propose the application of disciplinary proceedings against the offenders (art.45).

The resolution of the sanctioning organ is elevated to a higher authority, which must then verify and determine the applicable sanctions against the infringement.

Electronic marketing

Not regulated by the personal data protection law. However, art. 22 of the Internet Communication Law Num. 1/2017 dates January is to the effect that commercial electronic communications such as adverts and promotions must conform with the data protection laws in relation to the abstention, creation and maintenance of files. More also, data used for such purposes must be clear and identifiable.

Online privacy

Not regulated by the law.

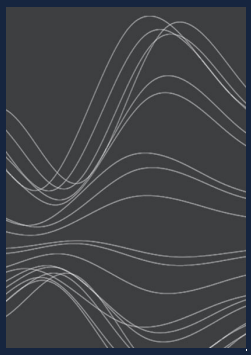
Data protection lawyers

Maria Cheswa Alogo Django
Junior Associate
Centurion Law Group
maria.django@centurionlg.com

Pablo Mitogo Akele
Associate
Centurion Law Group
pablo.mitogo@centurionlawfirm.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