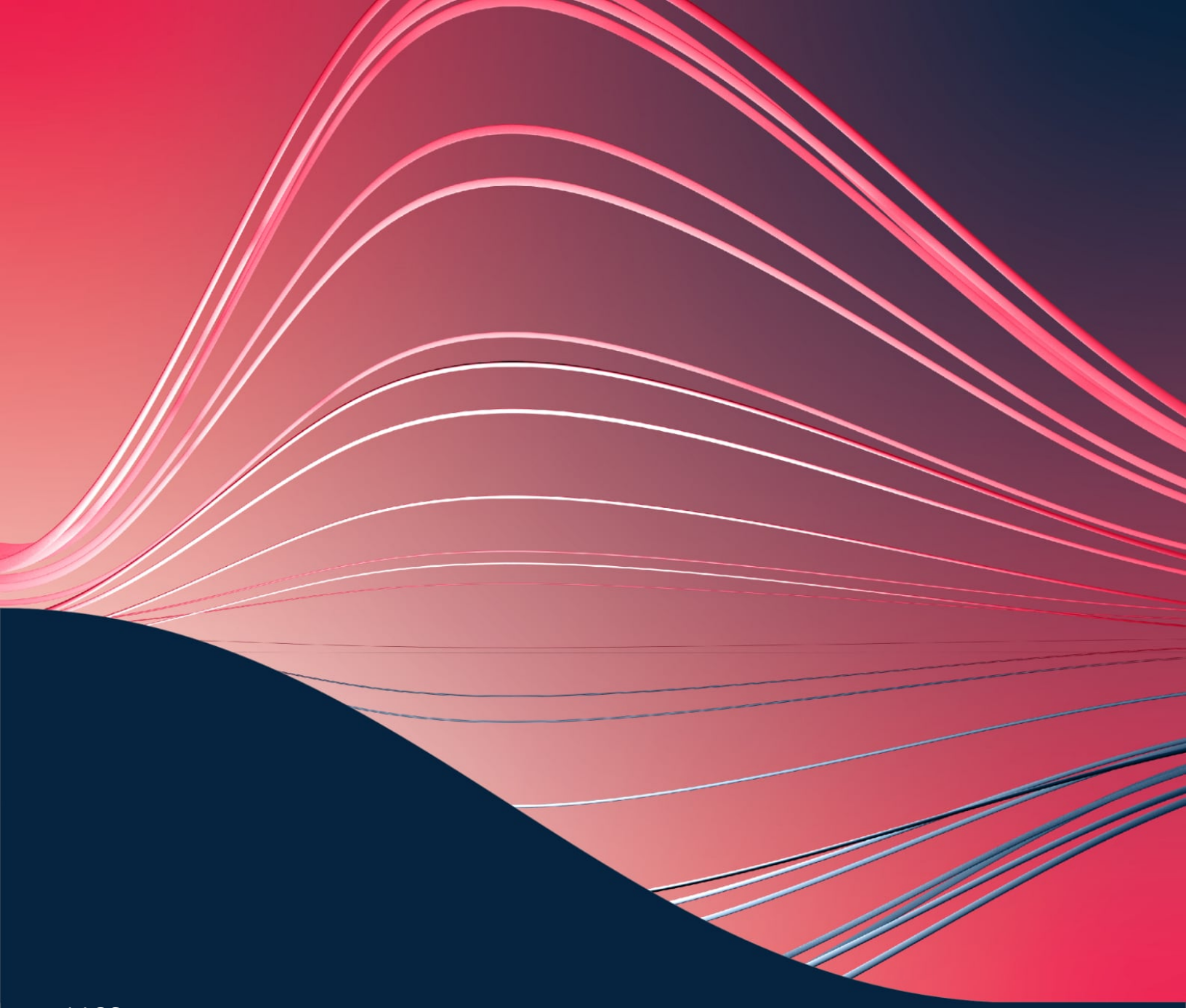


LAOS

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.

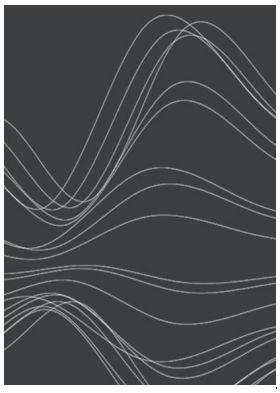
Africa key contact

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

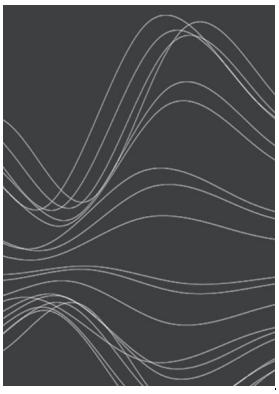
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

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

Laos

LAST MODIFIED 8 JANUARY 2025

Data protection laws

In Laos, the comprehensive regulatory framework on data privacy focuses on data in its digital form – electronic data – and none other.

From 2012, Laos has introduced this framework by circulating relevant information only. This trend has accelerated since 2015 with the publication of the Law on Cyber Crime. Issues pertaining specifically to the protection of electronic data are regulated by the Law on Electronic Data Protection and the subsequent Instructions on the Implementation of the Law on Electronic Data Protection, as follows:

- Law on Electronic Transactions (2022);
- Law on Cyber Crime (2015);
- Decision on the Penalties of the Law on Cyber Crime (2017);
- Law on Electronic Data Protection (2017);
- Penal Code (2017);
- Instructions on the Implementation of the Law on Cyber Crime (2018);
- Instructions on the Implementation of the Law on Electronic Data Protection (2018).

In addition, for both professionals or non-professionals, the authorities have provided a series of guidelines of best practices for the use of software and hardware, social media platforms, and better protection of electronic data.

The two main pieces of regulation relating to data privacy are the Law on Electronic Data Protection and the Instructions on the Implementation of the Law on Electronic Data Protection.

Definitions

Definition of Personal Data

Article 3, Section 12 of the Law on Electronic Data Protection defines "personal data" to mean electronic data of an individual, legal entity, or organization.

Definition of Sensitive Personal Data

The Law on Electronic Data Protection aims to protect any type of electronic data. The law categorizes electronic data roughly into three types: (i) general data, (ii) sensitive data (a literal translation would be "specific data"), and (iii) prohibited data. Depending on its nature, personal data may fall under one of these three categories. Accordingly, there is no "sensitive personal data" so to speak. Given this, personal data may fall under the category of sensitive data.

Sensitive data is information "that an individual, legal entity, or organization cannot access, use, or disclose if [they] have not received consent from the Information Owner, or the relevant organization" (Article 10).

A list of examples of sensitive data is provided in the Instructions on the Implementation of the Law on Electronic Data (2018), which includes "information on customers, financial information, CV, history of medical treatment, race, religion, project plan, budget plan, official secret, etc." (Section 3). The list is not exhaustive, and there is no official guidance to anticipate what other data may be considered sensitive data apart from these examples.

National data protection authority

The Law on Electronic Data Protection (2017) originally delegated the Ministry of Post and Telecommunications (MPT) to handle matters related to the protection of electronic data. The MPT has now been renamed Ministry of Technology and Communication (MTC) and is the main administration in charge of issues pertaining to electronic data privacy across the country. The MTC is assisted by its departments located in each of the 17 provinces that compose Laos.

In its tasks to analyze and respond to digital issues and threats, the MPT was originally assisted by the Lao Computer Emergency Response Team (LaoCERT), which was established in 2012. LaoCERT is now a Division under direct supervision of the Department of Cyber Security in the MTC and is the agency on the front lines that receives reporting of security breaches from individuals or legal entities operating in Laos and / or complaints of offenses committed online.

Registration

There is no registration required for Data Protection Officers in Laos, or for any legal entities or individuals with a national data protection authority, as the case may be in other jurisdictions.

Data protection officers

Under the Law on Electronic Data Protection, there is no data protection officer so to speak. The law introduces the idea that a team or an employee is required to supervise the protection of sensitive data; no information is provided on the duties and rights of

such team or employee, or their scope of work. Moreover, the team or employee in charge of the protection of sensitive data is not required to register with any authority.

Collection and processing

The collection of information is defined under the Instructions on the Implementation of the Law on Electronic Data Protection as "*the compiling of information in a database... for the convenience of access, monitoring, and use*...".

The Law on Electronic Data Protection speaks literally of "administration" of data. Administration of electronic data refers to the management and arrangement of data, which includes the collection, copying, submission, receipt, maintenance, and destruction of electronic data. This administration of data is carried out by the Data Administrator, which is defined as an "individual, legal entity, or organization which has the duty to administrate electronic data, such as: a Ministry, an Internet Data Center, a Telecommunications Service Provider, an Internet Service Provider, or a Bank." Apart from this definition, and the examples provided in the law, the Lao regulatory framework does not provide official guidance on who may or may not fall under the definition of Data Administrator.

By law, all data, general or sensitive, requires consent from the Information Owner to be collected. However, there is no information on how this consent may be collected.

Information Owner is defined as the individual, legal entity, or organization who / which is the owner of the electronic data. In this regard, the law does not necessarily identify the Information Owner as an individual only, or an individual who may be identified according to personal data that relates to him / her. The law only provides that the Information Owner is the entity that "owns" the information.

Sensitive data is more regulated as it requires the approval from the Information Owner for the access, use, and disclosure of sensitive data. At the time of the collection, the Information Owner must be informed of:

- the identity of the Data Administrator;
- the purpose of the collection of the information;
- the type of information that will be collected;
- the rights of the Information Owner, which include:
  - the right to amend the information provided;
  - the right to stop the sending or transfer of information to third parties;
  - the right to delete the information collected per request, or at the time that the purpose of the collection of the information expires.

Also, the Data Administrator and the Information Owner have the duty to ensure that the information provided is correct — it does not contravene local regulations, and does not affect the country's socio-economic development, national stability, or social order.

Transfer

The Law on Electronic Data Protection provides that the transfer of data must abide by the following requirements:

- the Information Owner has given its consent for the transfer of the electronic data, and the individual or legal entity;
- transferring the electronic data ensures that the receiving entity can protect the electronic data properly;
- documents concerning important information, such as financial, banking, investment, and accounting information, must be encrypted;
- information which is transferred or submitted must not be distorted;
- the transfer must be in line with the agreement between the sender and the recipient; and
- submission or transfer of data must be stopped when the receiver of the data does not intend to receive the information anymore.

The law does not address whether the requirements above should be applied to all individuals or entities, or only to the Data Administrator.

In addition, the Law on Electronic Data Protection emphasizes that any individual, legal entity, or organization contemplating sending or transferring personal data or official data (pertaining to governmental bodies) out of Laos must obtain the consent of the Information Owner, and ensure that such submission or transfer does not contravene the Lao laws without further details.

Security

Generally, the Law on Electronic Data Protection requires the Data Administrator to ensure the following regarding the storage / maintenance of electronic data:

- there is a team or employee responsible for the administration of sensitive data;
- there is, among other things, an adequate system to store or use the data, and a data safeguard system to protect the data;
- there is a backup system for destroyed or deleted data;
- information is recorded by way of another appropriate method (e.g. paper, magnetic storage), and the appropriate measure is used to guarantee good maintenance;
- a risk assessment is conducted on the protection system at least once a year, and any failures uncovered during the inspection are corrected;
- access to the system is inspected, and protected from any intrusion, virus, or other risks;
- any adverse events that have occurred or are about to occur are immediately solved; and
- the information that is under the responsibility of the Data Administrator is protected.

Breach notification

There is no mandatory breach notification in Laos under the Law on Electronic Data Protection. Individuals and legal entities facing a breach may make a notification, but to seek assistance and recommendations on how to solve the breach, and not for the sake of transparency.

However, in 2020, the Bank of Lao PDR issued the Decree on Consumer Protection Concerning Financial Services. Like the Law on Commercial Banks, enacted in 2023, the decree reiterates the importance of financial service providers (e.g. commercial banks) protecting their customer's confidential information. However, unlike the Law on Commercial Banks, the Decree does mention a duty to maintain the confidentiality of " personal information".

The Decree provides that in the event that information relating to customers is breached, the financial service provider has an obligation to record the incident and immediately notify the affected customers. No details are provided on what specifically must be recorded or notified. Likewise, the language used in the original document does not provide any assistance in interpreting the meaning of the term "affected." The term for "affected" that is used in the Lao language version of the Decree is a term that is normally used to denote persons who have suffered negative consequences or damage from an act. In the event that the breach of information causes an important adverse impact, or if there is a large-scale breach, a report must be submitted to the Bank of Lao PDR. However, there is no definition of "important adverse impact" or " large scale breach." Moreover, no specific sanction is provided for failing to submit the report.

The Law on Electronic Data Protection does not provide sanction for breach of the notification obligation. On the other hand, the Penal Code provides that any person disclosing the private confidential information of another person during the performance of their profession or duties, and who causes damages to the other person, will be liable to imprisonment of a term of three to six months and a fine between LAK 3 million (approx. USD 137) and LAK 10 million (approx. USD 458). However, Penal Code does not define "private confidential information", nor does it state whether the disclosure of information must be intentional. To date, there is no official guidance clarifying whether the Penal Code applies to scenarios where customer data is breached as a result of a technical failure or other such incidents.

Enforcement

The enforcing authorities with regard to electronic data protection are:

- Ministry of Technology and Communications (MTC);
- Economic Police; and
- Lao People's Court.

The Department of Cyber Security does not have by law the authority to issue fine or sanctions.

Electronic marketing

The Decision on Protection of Consumers Using Telecommunications and Internet Services (2020) regulates unsolicited commercial communications (e.g. phone calls or messages) to consumers, with the following restrictions:

- such calls and messages are prohibited from 8:00 to 17:00, Monday to Friday;
- no more than 10 unsolicited commercial communications are allowed per month, per individual;
- no more than two unsolicited commercial communications are allowed per day.

The decision provides that any individual or legal entity intending to use unsolicited commercial communications for their goods or services must receive the consent of the telecommunications or internet service provider of the prospects they plan to call. The decision does not offer guidance on how the relevant service provider's consent may be obtained. Rather, the decision requires the telecommunications and internet service providers to ensure that unsolicited commercials communication are made by authorized persons. In addition, the decision delegates these providers to monitor the distribution of unsolicited commercial messages, thereby ensuring that these limits are not breached.

Consumers who receive unsolicited commercial communications can file a complaint with the MPT and resolve subsequent disputes with the relevant service provider. The decision also notes that consumers can voice complaints or seek guidance via one of the following official hotlines:

- 1510 – Ministry of Industry and Commerce;
- 1516 – Prime Minister's Office;
- 156 – National Assembly.

The Ministry of Industry and Commerce's website is also expected to become an available channel for complaints in the future.

Online privacy

As provided, the collection of data must receive the consent of the relevant Information Owner.

On the other hand, based on the main laws and regulations above, it is difficult to anticipate the category of data cookies and location data according to the ambiguous definitions of general data, sensitive data, and personal data.

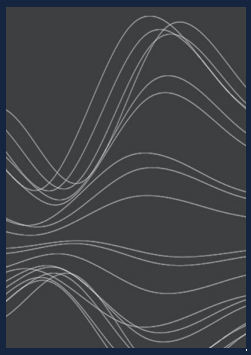
Data protection lawyers

Prisna Sungwanna
Partner and Director
Tilleke & Gibbins
prisna.s@tilleke.com
View bio

Naiyane Xaechao
Associate
Tilleke & Gibbins
naiyane.x@tilleke.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