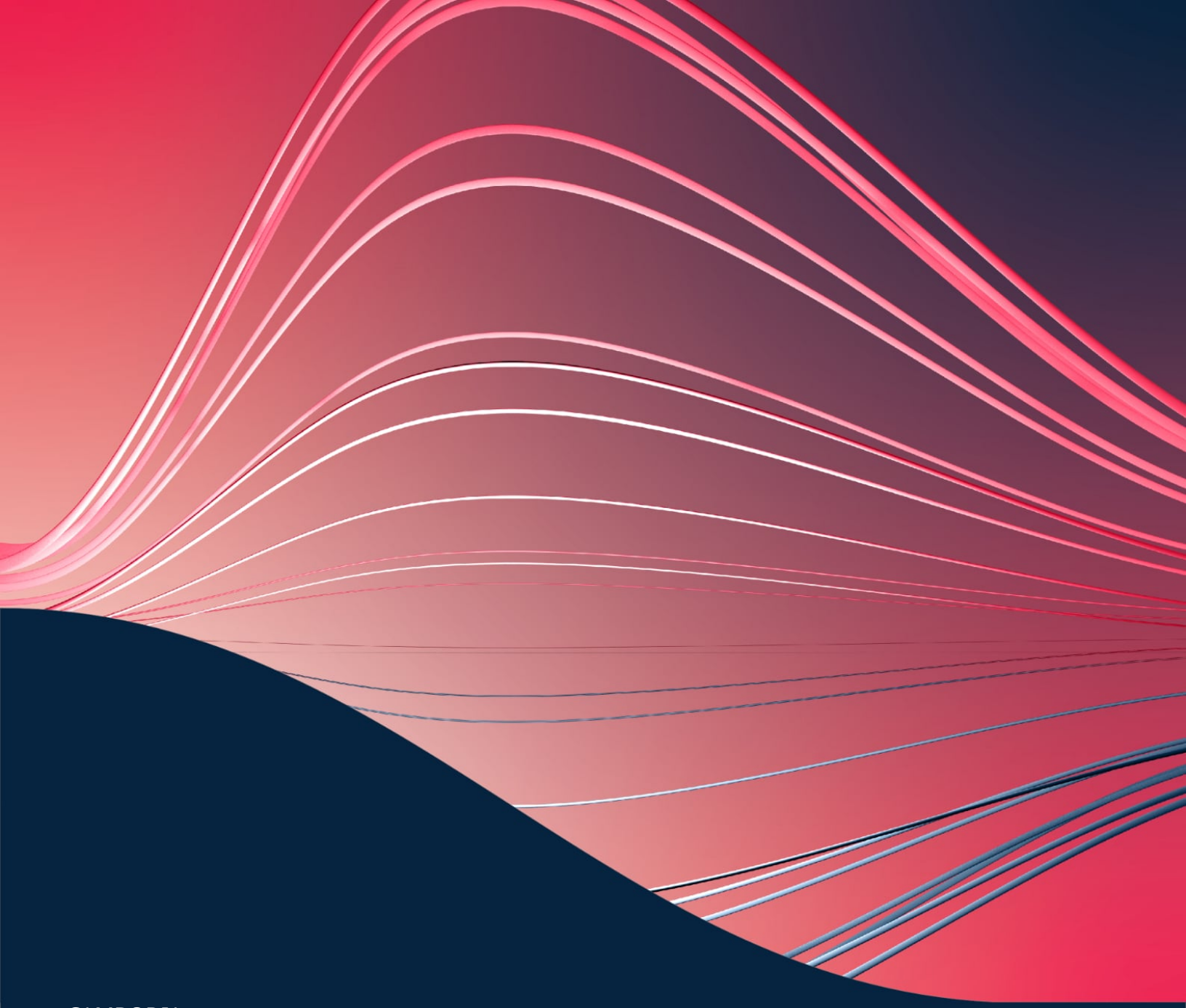


CAMBODIA

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.

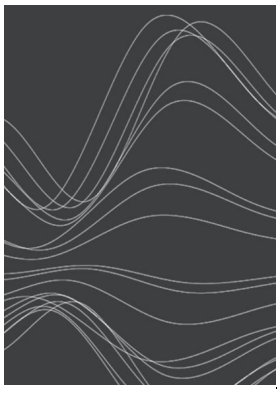
Africa key contact

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

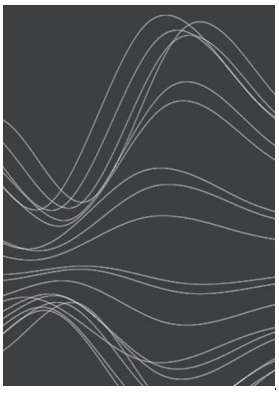
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

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

Cambodia

LAST MODIFIED 20 JANUARY 2025

Data protection laws

The Ministry of Post and Telecommunications (**MPTC**) announced on 19 February 2021 their intention to prepare a comprehensive personal data protection law after finalizing the draft cybersecurity law.

On 22 December 2021, the Royal Government of Cambodia issued Sub-Decree No. 252 on the Management, Use, and Protection of Personal Identification Data (only available in Khmer) (Sub-Decree 252) in order to promote broad policy objections, such as:

- ensuring the protection of peace and order;
- serving the public interest; and
- promoting national development by improving the provision of services.

However, Sub-Decree 252 only applies to "personal identification data" owned by the Ministry of Interior (MOI) and does not apply to personal identification data used by other entities.

In September 2023, the MPTC made available to select private organizations and companies a Draft Law on Personal Data Protection for their review and comment. However, it has not been made available to the public as of writing. Therefore, the information provided regarding the data protection law should be used as a reference and not considered final, as the draft law has not been officially released to the public. The Draft Law on Personal Data Protection establishes rules, principles, and mechanisms to govern the collection, use, and disclosure of personal data. Its main objective is to safeguard the privacy rights of individuals and encourage the lawful and responsible use of personal data.

The E-Commerce Law contains provisions for the protection of consumer data that has been gathered over the course of electronic communications. The E-Commerce Law is thereby restricted in scope to virtual and / or digital data protection.

Other matters pertaining to data protection typically fall under the right to privacy, which is protected in broad terms under the Constitution of the Kingdom of Cambodia

2010, the Civil Code of the Kingdom of Cambodia 2007, the Criminal Code of the Kingdom of Cambodia 2009, the Code of Criminal Procedure of the Kingdom of Cambodia 2010, and other specific laws such as the Banking Law.

Definitions

Definition of Personal Data

Cambodian law does not specifically define the term "personal data," or discuss what specific information constitutes personal data.

The E-commerce Law defines the term "data" as "a group of numbers, characters, symbols, messages, images, sounds, videos, information or electronic programs that are prepared in a form suitable for use in a database or an electronic system".

According to the Draft Law on Personal Data Protection, personal data is defined as information pertaining to an individual that can directly or indirectly identify them. This information includes, but is not limited to, names, identification numbers, location data, and online identifiers. As the Law on Personal Data Protection has not yet been implemented, this definition should not be regarded as official.

Therefore, due to the absence of a definition of "personal data", it remains plausible that any data of a data subject may be viewed by the regulatory and enforcement authorities as personal data of that data subject. As such, conventional data, such as full names, national identification numbers, passport numbers, photographs, video, images, phone numbers, personal email addresses, biometric data, IP addresses, and other network identifiers, etc., may arguably constitute personal data.

Definition of Sensitive Personal Data

There is no express definition of what constitutes sensitive personal data. That said, based on laws applicable to persons and entities in other sectors (such as healthcare and banking), the types of data below are generally considered to be of a more sensitive nature, and thus should be handled with more stringent data protection mechanisms:

- medical data;
- financial data;
- personal data of children; and
- personal identifiers (e.g. national identification cards and passport details).

As there is no clear limit as to the scope of what may be considered sensitive data, any data of a data subject should be prudently treated as sensitive data to the greatest extent possible.

National data protection authority

Since Cambodia does not have any dedicated laws on data protection, there are no regulatory or enforcement authorities that are specifically tasked with handling, overseeing or implementing personal data protection matters in Cambodia.

That said, the following governmental bodies may have substantial powers over data protection matters:

- the Ministry of Commerce ("**MOC**");
- the Ministry of Post and Telecommunications ("**MPTC**"); and
- the Ministry of Interior ("**MOI**").

Registration

Since Cambodia does not have any dedicated laws on data protection, there are no specific registration requirements for data controllers, data processors, or data processing activities.

Data protection officers

Since Cambodia does not have any dedicated laws on data protection, there are no specific requirements in Cambodia to appoint data protection officers who are specifically tasked with handling, overseeing or implementing data protection matters in Cambodia.

Collection and processing

As Cambodia has not enacted any dedicated or comprehensive data protection laws, there are no laws or regulations in Cambodia that explicitly and specifically discuss the concept of collection and processing of data. Under current practice, matters pertaining to data protection and privacy generally fall under the right to privacy that is protected in broad terms under Cambodia's Constitution, specific legal provisions under the Civil Code, the Criminal Code, and other specific laws such as the Banking Law and the E-Commerce Law. However, none of the legislations mention a consent requirement.

Under the Draft Law on Personal Data Protection, which is subject to further revisions, the term "data controller" is defined as a natural person, private legal entity, public establishment of administrative character, or public entry that determines the purpose and means of collecting, using, or disclosing personal data. On the other hand, a "data processor" is defined as a natural person, private legal entity, public establishment of administrative character, or public entry that processes personal data on behalf of a data controller or public authority.

The Draft Law on Personal Data Protection contains provisions on consent requirement for collecting, using, or disclosing personal data and further stipulates that the principles of personal data protection include:

- lawfulness, fairness, and transparency;
- purpose limitation;
- accuracy of personal data;
- retention limitation;

- security safeguards; and
- accountability.

Transfer

There are no existing regulations or provisions on the restriction of the transfer of data, including international transfer, except for licensed banks and financial institutions licensed by the National Bank of Cambodia, which need to follow guidelines under the Technology Risk Management Guidelines. Those guidelines contain provisions that restrict the international transfer of data.

Security

Article 32 of the E-Commerce Law directly addresses matters of data protection in the course of electronic communication.

Service providers that electronically store consumers' private information must take all reasonable security measures to avoid loss, modification, leakage, and / or unauthorized disclosure of all consumer data. The E-Commerce Law notes, however, that disclosures are allowable with the consent of authorities, or with the consent of the individual whose data is being disclosed. The E-Commerce Law does not provide specific guidelines as to how or what mechanisms are required. It is simply required that any measures could be used as long as they could reasonably protect the data from loss, or unauthorized access, use, alteration, or disclosure without authorization or illegally.

The E-Commerce Law also prohibits any encryption of data that may be used as evidence for any accusation or offence. This obligation potentially allows governmental authorities to order the decryption of data implicated in an investigation.

The E-Commerce Law also makes a blanket prohibition on certain forms of cybercrime, including interference with any electronic system for the purpose of accessing, downloading, copying, extracting, leaking, deleting, or otherwise modifying any stored data in bad faith or without authorized permission.

Article 47 of the Banking Law prohibits those who participate in the administration, direction, management, internal control, or external audit of a covered entity, and employees of the latter from providing confidential information pertaining to statements, facts, acts, figures, or the contents of accounting or administrative documents of which they might have become aware through their functions. However, this professional secrecy obligation cannot be used as a ground for nondisclosure in relation to requests by supervisory authorities, auditors, provisional administrators, liquidators, or a court dealing with criminal proceedings.

In case the service provider is not under the scope of the E-Commerce Law or Banking Law, the obligations under the laws of general application that require protection of the right to privacy and the obligation to protect data from unauthorized access should apply when a service provider collects, uses, discloses and processes data of the subject.

Furthermore, the Draft Law on Personal Data Protection requires the data controller to protect personal data under its possession or control by setting up a security system to prevent unauthorised access, collection, use disclosure, copying, modification or disposal, or similar risks; and the loss of any storage medium or device on which personal data is stored. The data processor must also take security measures to prevent loss or unauthorised or unlawful access, use, modification, or disclosure of personal data.

Breach notification

Currently, there is no breach notification requirement under Cambodian law. However, it is anticipated that the requirement for data controllers and data processors to notify the competent authority and the affected data subjects will be enforced once the Draft Law on Personal Data Protection comes into effect.

Enforcement

Since there are no regulatory or enforcement authorities that are specifically tasked with handling, overseeing or implementing personal data protection matters in Cambodia, the enforcement of the data protection would generally fall under the auspice of authorities across various sectors:

- the Ministry of Commerce;
- the Ministry of Post and Telecommunications; and
- the Ministry of Interior.

Electronic marketing

Since Cambodia does not have any dedicated laws on data protection, there are no special requirements when obtaining consent for marketing purposes. The E-commerce Law suggests that it is not necessary to obtain consent from the individual to send marketing communications as long as each marketing communication has clear and straightforward opt-out instructions and the individual has not previously exercised his / her opt-out right. Electronic marketing in Cambodia is subject to the general laws relating to digital marketing issues including:

- Law on Consumer Protection, which prohibits "unfair practices" in relation to consumer transactions. Unfair practices include unfair sales; bait advertising; unfair solicitation sales; demanding or accepting payments without intention to supply goods or services per the purchase order; making a false claim or representation of some business activity; coercion by force and mental threats; pyramid schemes; selling goods bearing a false trade description; and any other unfair practices.
- Law Concerning Marks, Tradenames and Acts of Unfair Competition, is relevant to comparative advertising. The following acts are considered acts of unfair competition: all acts that create confusion with the establishment, the goods, or the industrial, commercial or service activities of a competitor; false allegations in the course of trade of such a nature as to discredit the establishment, the goods, or the industrial, commercial or service activities of a competitor; and indications or

allegations of the use of marks which, in the course of trade, misleads the public as to the nature, manufacturing process, characteristics, suitability for their purpose, or quantity of the goods.

- Telecommunications Law, which prohibits all activities against the principles of fair, free, equal, and effective competition.
- Other regulations on the Management of Advertisement on Website, Social Network, Mass Media and Mobile Phone Operators.

Online privacy

As mentioned under the Collection and Processing and Transfer sections, the current regulations generally recognize the right to privacy and the obligation to protect data from unauthorized access. Those regulations do not specifically distinguish online privacy from privacy in general.

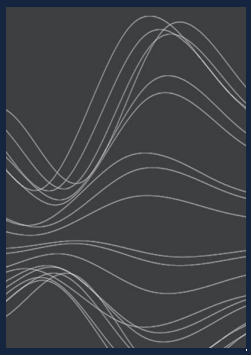
Data protection lawyers

Jay Cohen
Partner and Director
Tilleke & Gibbins
jay.c@tilleke.com
View bio

Sochanmalisphoung Vannavuth
Associate
Tilleke & Gibbins
sochanmalisphoung.v@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