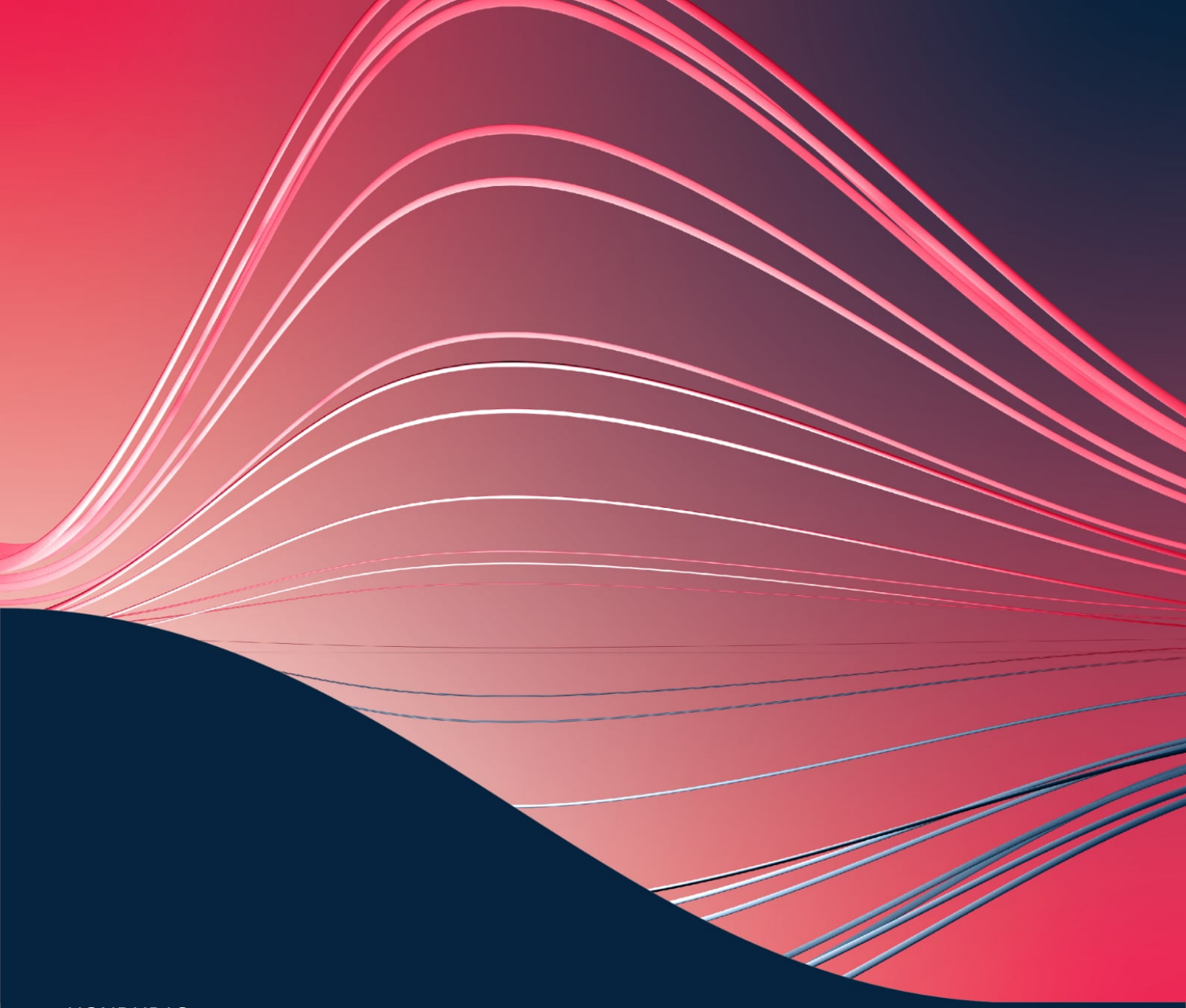


HONDURAS

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.

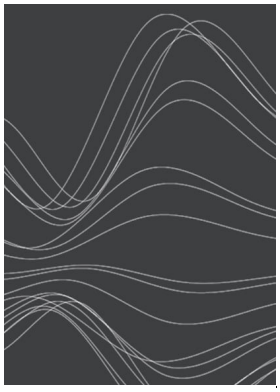
Africa key contact

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

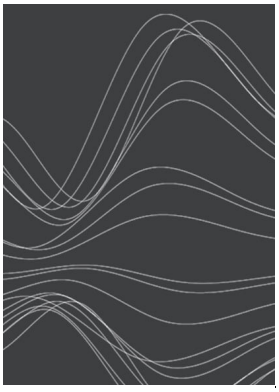
Middle East key contact

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

Honduras

LAST MODIFIED 10 FEBRUARY 2025

Data protection laws

Personal data protection is regulated mainly in:

National Constitution: Article 182 provides the constitutional protection of habeas data, giving individuals the right 'to access any file or record, private or public, electronic or hand written, that contains information which may produce damage to personal honour and family privacy. It is also a method to prevent the transmission or disclosure of such data, rectify inaccurate or misleading data, update data, require confidentiality and to eliminate false information. This guarantee does not affect the secrecy of journalistic sources.'

Law of the Civil Registry (Article 109, Decree 62-2004). This law refers only to public personal information that is contained in the archives of the Civil Registry.

Law for Transparency and for Access to Public Information (Article 3.5, Decree 170-2006). This law enables the access of any person to all the information contained in public entities, except that which is classified as 'Confidential.' It also extends the constitutional protection of habeas data and forbids the transmission of personal information that may cause any kind of discrimination or any moral or economic damage to people.

Rulings on the Law for Transparency and for Access to Public Information (Article 42, Accord 001-2008). Provide a definition of databases containing personal confidential information, and requires data subject consent, prior to the use of it by any third party.

In addition, the Law for the Protection of Confidential Personal Data (the “Law”) is currently in discussion in the Honduran Congress. Congress has approved the first chapters of the Law. The complete approval of the Law and the date for when the Law will enter into force is expected in the first half of 2019.

Definitions

Definition of personal data

Public Personal Data under the Law of the Civil Registry is defined as: Public Data whose disclosure is not restricted in any way, and includes the following:

- Names and surnames
- ID number
- Date of birth and date of death
- Gender
- Domicile (but not address)
- Job or occupation
- Nationality
- Civil status

Definition of sensitive personal data

The Law for Transparency and for Access to Public Information defines 'Sensitive Personal Data' as: "Those personal data relating to ethnic or racial origin, physical, moral or emotional characteristics, home address, telephone number, personal electronic address, political participation and ideology, religious or philosophical beliefs, health, physical or mental status, personal and familiar heritage and any other information related to the honor, personal or family privacy, and self-image."

Other definitions:

- Consent: Written and express authorization of the person to whom the personal data refers in order to disclose, distribute, commercialize, and/or use it in a different way as it was originally given for
- Confidential Information: Information provided by particular persons to the government which is declared confidential by any law, including sealed bids for public tenders
- Classified Information: Public information classified as that by the law, and / or by resolutions issued by governmental institutions

National data protection authority

Two entities are responsible for enforcing personal data protection:

1. National Civil Registry
   http://www.rnp.hn
2. Institute for the Access to Public Information
   http://www.iaip.gob.hn

Registration

Only Obligated Entities must inform the Institute for the Access to Public Information of their databases. Obligated Entities are:

- Government institutions

- NGO's
- Entities that receive public funds, and
- Trade unions with tax exemptions

The Institute for the Access to Public Information will maintain a list of the databases of the above-mentioned entities.

Data protection officers

Only Obligated Entities must appoint a data protection officer.

Collection and processing

Individuals, companies, and / or Obligated Entities that collect personal data may not use sensitive personal data or confidential information without the consent of the person to whom such information relates.

However, consent is not required to use or transfer personal data in the following cases:

- If the information is used for statistical or scientific needs, but only if the personal data is provided in a way that it cannot be associated with the individual to whom it relates
- If the information is transmitted between Obligated Entities, only if the data is used in furtherance of the authorised functions of those entities
- If ordered by a Court
- If the data is needed for the purpose it was provided to the individual or company to perform a service. Such third parties may not use personal information for purposes other than those for which it was transferred to them
- In other cases established by law

Transfer

Individuals and / or companies may not transfer, commercialize, sell, distribute or provide access to personal data contained in databases developed in the course of their job, except with the express and direct written consent of the person to whom that data refers, subject to certain exceptions.

Security

The Institute for the Access to Public Information has the authority to require all Obligated Entities to take necessary security measures for the protection of the personal data they collect and / or use.

The current legislation neither clarifies nor specifically identifies the security policies or security mechanisms that Obligated Entities must comply with.

As a general statement, the Institute for the Access to Public Information has to ensure the security of all Public Information, of all information classified as confidential by public entities, of all sensitive personal data, and of all information to which the current legislation gives a secrecy status.

Breach notification

Breach notification is not required.

Enforcement

The Institute for the Access to Public Information may receive complaints about abuses regarding the collection of personal or confidential data.

The Institute will impose corrective measures and establish recommendations for those persons or companies who disclose personal data, sensitive personal data or confidential data without authorization.

Electronic marketing

There is no law or regulation that specifically regulates electronic marketing.

Online privacy

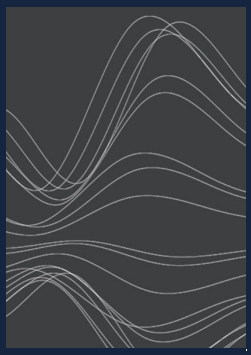
There is no law or regulation that specifically regulates online privacy.

Data protection lawyers

Julio Alejandro Pohl Garcí a-Prieto
Associate
Gufa Law
julio.pohl@gufalaw.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