VENEZUELA

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

Venezuela

LAST MODIFIED 12 DECEMBER 2022

Data protection laws

There is no specific legislation about data privacy or data protection in Venezuela, however, there are isolated provisions in some existing laws that regulate certain aspects related to data protection (e.g., Law on Privacy Protection of Communications, the Special Law against Computer Crimes, the Organic Law on Prevention, Conditions, and the Working Environment, and the Civil Code, Communications from the National Superintendency of Banks).

Likewise, the Constitution of the Bolivarian Republic of Venezuela (the **"Constitution")** establishes general principles that serve as a framework for the protection of information. These principles were developed by decision No. 1318 of the Supreme Court of Justice ("TSJ" for its Spanish acronyms) of August 2011, guarding the honour, privacy, intimacy, self-image, confidentiality, and reputation of individuals. The principles are:

- Principle of free will, which implies the need of a prior, free, informed, unequivocal and revocable consent for the use, and collection of personal data.
- Principle of legality, according to which the collection of personal data entails that the limitation to information self-determination is a result of a legal provision.
- Principle of purpose and quality, which means that the collection of personal data must respond to predetermined purposes, motives, or causes that are not contrary to constitutional and legal provisions, also a prerequisite to obtain valid consent. Data can only be extracted and treated for the fulfilment of specific, explicit, and legitimate purposes related to the activity of those who get them. This principle entails the necessary proportionality in the collection of data, which must be adequate, relevant, and not excessive.
- Principle of temporality or conservation, under which the data should be preserved until the purposes or objectives that its collection are achieved.
- Principle of accuracy and self-determination, which means that the data must be complete, accurate and up to date, in response to the real situation of the person as the data may be subject to control by the individuals whose data is collected. The interested party must have clear and expeditious procedures to obtain from the

person responsible for the use or receipt of the information: the confirmation of the use of data; the purposes of such registers and its recipients; the rectification or cancellation of inaccurate, inadequate, or excessive data, and; the knowledge of such modifications by those whose wrong information has been communicated.

- Principle of foreseeability and integrity: Although the rights relating to the collection of information should be initially aimed at protecting the rights of the individuals whose information is collected, the analysis of the impact that the collection of data has on such rights cannot be isolated and without reference to data that may be collected in other registries.
- Principle of security and confidentiality, which implies the guarantee of confidentiality, of no alteration of data by third parties, and of access to such data by the competent authorities in accordance with the law. The data must be protected from alteration, loss, accidental destruction, unauthorised access, or fraudulent use. This protection goes as far as preventing international data transfers to States whose legislation does not guarantee a level of protection similar to the one described.
- Principle of guardianship, which means that in addition to having judicial protection to enforce the right to access the information and obtain knowledge of the use of the personal data, there should be public entities that ensure the right to the protection of personal data with powers to create or implement simplified models and based on technical standards to measure the level of efficiency of the structures and procedures in place and the level of protection of the personal data.
- Principle of liability, under which a violation of the right to the protection of personal data gives rise to liability and the imposition of civil, criminal, and administrative penalties, as the case may be.

Also, Article 28 CRBV sets the right for individuals to access their personal information stored in public or private records, to know for what use such information will be recorded, and, rectify or destroy it when incorrect or when it unlawfully affects their rights. Although there is no legal regulation in this regard, the TSJ has agreed to the possibility of maintaining this information and personal data in systems or records, stored in a way that a profile of them can be done with the purpose of using the information for personal gain or for third parties, as long as the rights set in Article 28 CRBV are respected. According to this Article, a double right is guaranteed: (i) to collect information about people and their goods, and (ii) access to such information that has been collected and is reflected in the records. However, whoever collects the information or data of the individuals or their goods, shall respect the right of the people to protect their honour, privacy, intimacy, self-image, confidentiality, and reputation, all of this provided in Article 60 CRBV.

Additionally, the decision also stipulates that the particular data that someone keeps for study purposes, or for personal use or to fulfill professional objectives, which do not form a system capable of designing a total or partial profile of individuals are not subject to these principles, since they lack a general projection. However, records that, when cross-referenced with others, make it possible to outline a profile of the private life of individuals, or of their economic situation, political tendencies, etc., could be part of the records protected by the Constitution. The mere potential of intersecting and complementing the data of a registry, with the information stored in others that complete it, makes the set of records susceptible to the rights referred to in article 28 of the Constitution.

Definitions

Definition of Personal Data

There is no legal definition of “Personal Data” in Venezuelan legislation.

Nonetheless, decision No. 855 of the TSJ, of May 8, 2012, gave us the following definition of Personal Data: *“Any information related to an identified or identifiable individual”.*

Likewise, any Personal Data must be processed fairly and responsibly for particular purposes, on the basis of the data subject's consent or as a consequence of some other legitimate basis, provided by law.

Definition of Sensitive Personal Data

There is no legal definition of “Sensitive Personal Data” in Venezuelan legislation.

However, in decision No. 1335 of the TSJ, of August 8, 2011, in a case on the sensitive and personal data in a medical record, the TSJ expressed that any such data must be handled under the strictest confidentiality and privacy controls, and its content must not be disclosed.

The decision says that sensitive and personal data is a person’s most genuine and authentic assets, and, as such, is the absolute owner and holder of all that information, only that person can grant permission for its use and treatment.

Under this decision, we can conclude that any person’s intimate data can also be considered to be Sensitive Personal Data, and, as such, must be confidential, be duly guarded and only that person can grant permission for its use and treatment.

National data protection authority

There is no National Data Protection Authority in Venezuela.

Registration

There is no legal requirement to register before any National Data Protection Authority.

Data protection officers

There is no legal requirement to appoint a Data Protection Officer.

Collection and processing

The collection and processing of Personal Data must adhere to the previously explained general principles dictated by the Constitutional Chamber of the TSJ.

Transfer

According to the general principles dictated by the TSJ, there is a protection against the transfer of data to States whose legislation does not guarantee a level of protection similar to the one described.

In addition, in terms of labor law, the employee's consent is required to transfer personal data to third parties. There are companies that voluntarily develop their own data protection policies or apply their headquarters policies or international standards for this matter.

Security

According to the general principles dictated by the Constitutional Chamber of the TSJ, there is a guarantee of confidentiality, of no alteration of data by third parties, and of access to such data by the competent authorities in accordance with the law. The data must be protected from alteration, loss, accidental destruction, unauthorised access, or fraudulent use.

Breach notification

There is no legal obligation to disclose a data breach.

Mandatory Breach Notification

It is not mandatory to disclose a data breach.

Enforcement

When it comes to labor matters and records of employees, the Organic Law on Prevention, Conditions and Working Environment ("**LOPCYMAT**" for its Spanish acronym) sets forth in Article 53 the following rules on certain data and privacy protection:

- Section 10: the right of the employees to access information contained on health screenings, as well as the confidentiality of the results with respect to third parties. (According to Article 27 of the LOPCYMAT, disclosure of health results to certain third parties is permitted with the employee's consent. Also, per Article 119 of the LOPCYMAT, failure to comply with the obligation of section 10 may result in a fine ranging from 26 to 75 tax units ("**T.U.**") for each worker exposed.
- Section 11: the confidentiality of employees' personal health data. (According to Article 120 LOPCYMAT, failure to comply with the obligation of section 11 may result in a fine ranging from 76 to 100 T.U. for each worker exposed.
- Section 16: the privacy of employee's correspondence and communications, as well as free access to all data and information relating to the employee.
- The fines or sanctions for non-compliance according to LOPCYMAT are:

- Article 27: disclosure of health results to certain third parties is permitted with the employee's consent.
- In addition, per Article 119, failure to comply with the obligation of section 10 may result in a fine ranging from 26 to 75 T.U. for each worker exposed.
- Article 120: failure to comply with the obligation of section 11 may result in a fine ranging from 76 to 100 T.U. for each worker exposed.

Electronic marketing

Electronic Marketing is allowed, but any collection and processing of Personal Data must adhere to the previously explained general principles dictated by the TSJ.

Online privacy

There is no specific legislation about online privacy in Venezuela, but we advise to adhere to the previously explained general principles dictated by the TSJ if there is going to be any processing or collection of Personal Data.

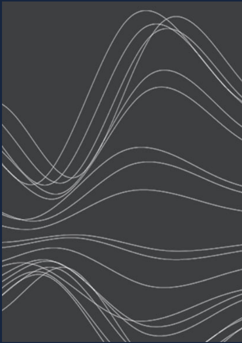
Data protection lawyers

Maria Cecilia Rachadell
Partner
InterJuris Abogados S.C
maria.rachadell@interjuris.com
View bio

Juan José Delgado
Partner
InterJuris Abogados S.C
juanjose.delgado@interjuris.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

This publication is for general information only. The information presented is not legal advice, and your use of it does not create a lawyer-client relationship. All legal matters are unique and any prior results described in this publication do not guarantee a similar outcome in future matters. DLA Piper is a global law firm operating through DLA Piper LLP (US) and affiliated entities. For further information, please refer to dlapiper.com. Attorney Advertising. Copyright © 2025 DLA Piper LLP (US). All rights reserved.