

Latin American Data Privacy Law

Aline Fachinetti

Guillermo Larrea

Paula Vargas

Session Leaders



Aline Fachinetti

DPO and Manager
Americas Region
Edenred



Paula Vargas

Director of Privacy
Policy & Engagement,
Latin America
Facebook



Guillermo Larrea

Jones Day (Mexico)
Cybersecurity, Privacy and
Data Protection with focus
on Latin America

- **SESSION GOAL** - *Explore the complexity of the latest regulatory developments and data privacy trends in Latin America, a region experiencing rapid digital transformation.*
- **AGENDA**
 - Welcome/Introductions
 - Context & Overview
 - Specific Laws/Details
 - *Break*
 - Issues, Hot Topics & Discussion
- **METHODOLOGY:**
 - Interactive presentations & dialogue/Q&A

Context & Overview

Overview



Panorama of LatAm Data Privacy



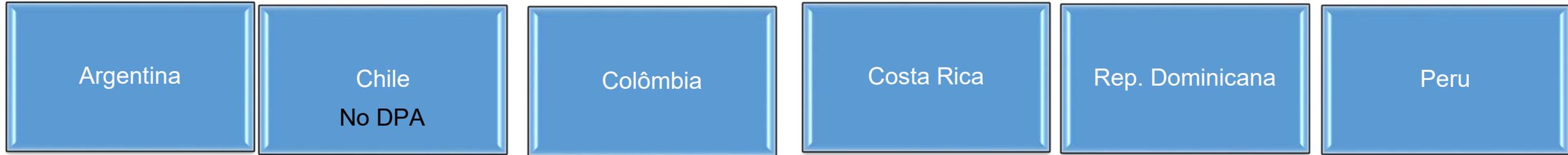
All jurisdictions in the region recognize some kind of concept of privacy

Right of access to personal data of public sphere and Habeas Data, are almost always recognized

Most of Latin American countries have data protection agencies

Overview-Enacted Laws

Pre GDPR



Post GDPR



Overview—Bills being discussed



Argentina

Bolivia

Chile

Costa Rica

Paraguay

** Bolivia: there are two bills under consideration.*

Overview-Regional Soft Law

Organization of American States (OAS)

- Updated Data Protection Principles
- Neurorights Declaration

Ibero-American Network of Data Protection Authorities

- Guidelines for Health Data Processing during the Pandemic
- Guidelines for Processing Personal Data in the Cloud
- Guidelines for Artificial Intelligence

Overview-Related Regulation

Digital Platforms Bill in Chile

Neurorights Bill & Constitutional
Reform in Chile

Amendment to Consumers Law
in Chile

Artificial Intelligence Bill in Brazil

Fake News Bill in Brazil

Evolution of LatAm Data Privacy Law

First Wave

- Chile (1999), Argentina (2000), Paraguay (2000)

Second Wave

- Uruguay (2008), Mexico (2010), Peru (2011), Colombia (2012)
- Costa Rica (2011), Nicaragua (2012) [Dominican Rep. 2013]

THIRD WAVE

- Mexico (2017), Brazil (2018), Uruguay (2018), Ecuador (2021)
- Panama (2019), El Salvador?

Specific Laws/Details

Mexico



TERRITORIAL SCOPE



Applies to data processing carried out in Mexico or on behalf of a data controller established in Mexico.



Partially extraterritorial. Unlike the GDPR, doesn't apply to controllers outside of Mexico. But it does apply to foreign processors if processing for a data controller in Mexico.

THE PLAYERS

Data Owner



Data Controllers

Data Processors

PERSONAL DATA



Identified Identifiable

SENSITIVE DATA

Racial or Ethnic Origin



Political Views

Religious or Moral Beliefs

Health Conditions

Genetic Data



Sexual Preference



Union Membership

CONSENT

Express Consent
Required for financial data and sensitive data.



Implied Consent
Not opting out is implied as consent.



PRINCIPLES OF DATA PROCESSING

Legitimacy

ensure data processing is in compliance with law

Consent

obtain consent of the data owner before processing begins

Information

inform data owner via a privacy notice

Quality

personal data must be exact, complete, pertinent, correct, and up-to-date.

Purpose

personal data may only be processed for the purposes set out in the privacy notice



Loyalty

prioritize the protection of the data owner's interests

Proportionality

process data necessary to the stated purposes

Minimization

reasonably try to limit processing personal data to the minimally necessary

Accountability

data controllers are responsible and will be held accountable for the processing of personal data



RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Privacy Notice



Data Protection Officer (DPO)



Security Program



Accountability



méxico

Federal Privacy Law



Mexico's Federal privacy law is called the Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

LAWFUL PROCESSING

Personal data may be processed for any reason stated in the privacy notice with the implied consent of data owners.

Personal data can be processed without consent when:

- permitted by law
- data obtained from public sources
- data dissociated from the data subject
- contract with data subject
- emergency that could harm data subjects or their property
- healthcare purposes
- authorized by resolution of the competent authority



DATA BREACH NOTIFICATION

When a data breach materially affects the data owner's property or moral rights, the data controller must immediately report the breach to the data owner. There is no duty to notify the regulatory authority for personal data (INAI).



ENFORCEMENT

Enforced by the National Institute of Transparency, Access to Information, and Personal Data Protection (INAI)

Fines

Maximum fines of up to 320,000 times of the Mexico City minimum wage.

If violations include sensitive data, fines can be doubled.

Imprisonment



DATA TRANSFER

Data transfers require the consent of the data owner.

Consent can be implied if the transfer is stated in the privacy notice.

Exceptions to Consent:

- pursuant to legal purposes
- medical reasons
- between parent and subsidiary companies with common control
- necessary for a contract
- necessary to public interest
- necessary for judicial proceeding



INTERNATIONAL DATA TRANSFER



Unlike the GDPR, no requirement that countries have an adequate level of data protection.

International data transfers require a written contract.

RIGHTS OF DATA SUBJECTS

ARCO Rights – acronym based on rights of access, rectification (correction), cancellation (blockage/erasure), and objection



Right to Access

Right of Objection



Right of Rectification

Right of Cancellation



www.teachprivacy.com
Privacy Training by Prof. Daniel J. Solove

Mexico

Current overview

Slow progress in personal data protection legislation, but soft law is increasingly being implemented as good practices.

Mexico must modify its legislation to adhere to Convention 108+.

Mexico is not a suitable third country, according to European Union standards for the free flow of personal data transfers.

Mexico is currently an observer of the Budapest Convention, but has not ratified or modified its regulations.

There is asymmetry in data protection laws and need supplemental actions.

Good standard level, but effectiveness is much lower.

Although it is possible to cover privacy issues in the private sphere, the public sphere is neglected.

The National Digital Strategy published in August does seem to provide enough support for data protection or privacy.

The National Digital Strategy is based on the principle of austerity and has the following privacy related shortcomings:

- Lack of clarity on technology and telecommunications issues
- Lack of analysis of the current market and route for security and infrastructure.
- Lack of budget, solid data on where Mexico is today, previous diagnosis and thermometer to measure progress.

The INAI imposed fines for 32 million pesos to individuals and companies that breached the LFPDPPP during the first semester of the 2021.

Sanctioned sectors are financial and insurance services (17.8 million pesos); information in mass media, (10.1 million pesos), and retail trade (2.9 million pesos).

Most frequent conducts are the processing of personal data in contravention of the principles; and irregularities in the Privacy Notice.

50 Sanction Imposition Proceedings were initiated and 35 from previous years were concluded.

166 Rights Protection Proceedings were initiated; 95 of right of Access to personal data, 16 the right of Rectification, 61 the right of Cancellation and 30 the right of Opposition to the processing of data.

From January to June 2021, 820 complaints have been filed before the INAI for the improper use of personal data in the private sector and 47 in the public sector.

Mexico Sanctions

Mexican lawyers sued the company that owns the world's leading search engine.

On March 9th After a five-year litigation, a civil court of Mexico City ruled against the accused individual and the company.

The lack of material authorship does not detract the company from their liability for the moral damage, since they must respond for their negligent activity.

An individual created a defamatory blog and the search engine company uploaded it to their platform, both were forced to repair the moral damage caused to the plaintiff.

This sentence also obliges to publish and disseminate the sentence on the company's official page.

This precedent establishes a criterion on the liability of technology giants for negligent behavior in the operation of their social networks or platforms.

Public

- **National Transparency Platform**
 - Intermittent behavior due to a cyber attack and hack.
 - Activities were quickly resumed.
 - No personal data was breached.



Mexico

Initiative to reform federal law

A Mexican senator presented a bill to amend the Data Law



Proposes obligation of providing data breach notifications to the data owners and to the INAI (max. 72 hours)

Currently, the LFPDPPP only imposes the obligation to notify when economic or moral rights are significantly affected

Mexico

Initiative to reform federal law

Obligation of the controllers to appoint a representative or implement a mechanism to comply with their obligations within Mexican territory



What constitutes the data subjects' economic rights for purposes of a breach

Mexican senate approves bill for the National Registry of Cellphone Users



Mexican Senate approved the bill to reform the Federal Law of Telecommunications and Broadcasting, providing for a national register of cellphone users



This register will be mandatory and will contain the following data:

- Cellphone number and time of the SIM card's activation



The INAI filed an unconstitutionality action before the SCJN and the suspension was granted on June 29th.



The INAI filed an unconstitutionality action before the Supreme Court of National Justice against National Registry of Cellphone Users



- Full name of the line holder
- Nationality
- Official identification number with photograph and unique population number
- Biometric data of line holder

National registry of cellphone users

It also grants undue power to the Federal Telecommunications Institute.



The SCJN has yet to determine whether the unconstitutionality action proceeds or not.

The Deputies Chamber budget does not contemplate resources to implement such registry.



TELECOMMUNICATIONS
INSTITUTE
APPROVES FILING
UNCONSTITUTIONALITY
ACTION

Conflicts articles 6 and 7 of the Constitution and access to telecommunications services, which are fundamental rights.

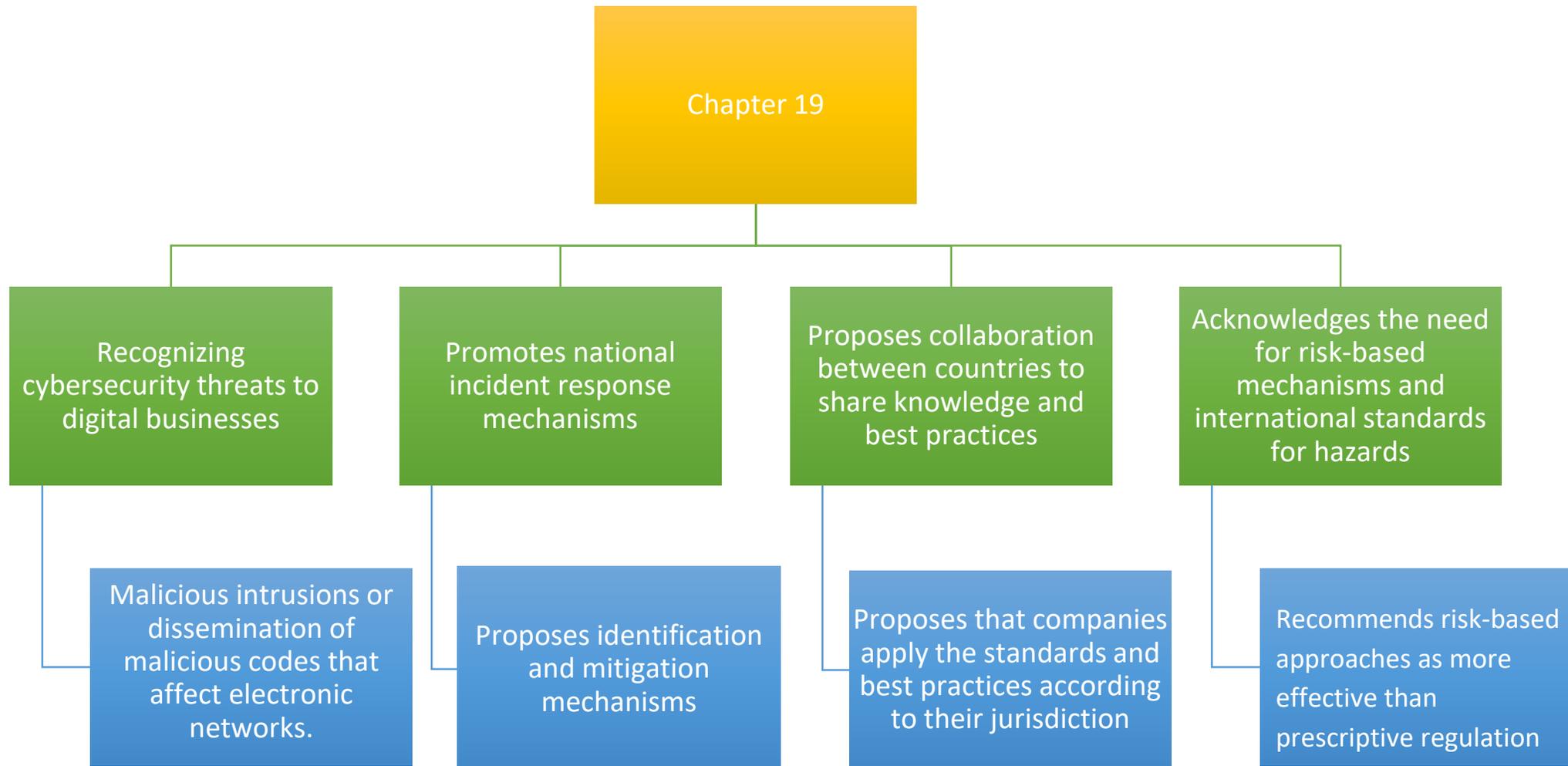


Main characteristics

- It does not maintain a specific model.
- It is more specific than the TPP / CPTPP.
- Encourages OECD principles and APEC principles.
- Encourages compatibility and interoperability.
- Recognizes the CBPR system as a valid mechanism for international transfers.
- Establishes the application of legal frameworks that must be necessary and proportionate.
- Encourages cooperation and compatibility among the three countries.
- Adds a clear definition of personal data.
- Provides a legal framework that provides for the protection of personal information.
- Encourages cooperation between government agencies in personal information protection investigations.

Prohibitions

- Prohibition of restrictions on cross-border data transfer flow, except:
Legitimate public policy objective, + (i) non-arbitrary measure (ii) non-discriminatory measure (iii) non-excessive measure.



Recommendations

- Elaboration of impact analysis, for example:
 - Data transfers made by the company
 - Security in digital platforms
- Recognition of data protection principles
- Reinforcement of compliance programs
- Implementation of mechanisms to identify and mitigate malicious intrusions
- Adoption of digital security measures and preparation for cybersecurity incidents



Brazil's LGPD



Brazil's LGPD



ANPD— Brazil's Authority



Topic	Start of regulation		
	1º/2021	1º/2022	2º/2022
ANPD's Internal Rules	•		
ANPD's Strategic Planning	•		
SME simplified rules	•		
Sanctions	•		
Incidents notification	•		
DPIA	•		
DSRs		•	
DPO		•	
International Transfer		•	
Lawful basis			•

Argentina



SCOPE AND APPLICABILITY

Applies to the collection and processing of personal data of Argentina residents in Argentina.

The law also applies to data processors located outside of Argentina that process personal data on behalf of a controller in Argentina.



THE PLAYERS

Data Subject

Controller
Processor

Data Protection
Authority (DPA)



PERSONAL DATA

Identified

Identifiable



SENSITIVE DATA

Sensitive data can be processed under a more limited set of circumstances than regular personal data. Sensitive data includes information about:

- racial or ethnic origin
- religious or philosophical beliefs
- political opinion
- trade union or political affiliation
- health or sex life
- biometric data when its use may result in discrimination



RESPONSIBILITIES OF CONTROLLERS AND PROCESSORS

Registry of
Databases



Confidentiality



Provision of
Accurate Data



Security



Time Limitation
for Data
Processing



Respond to Data
Subject Requests

PRINCIPLES OF DATA PROCESSING

Legality

Processing data must comply with law.

Quality

Data must be accurate, pertinent, and not excessive. Incomplete or inaccurate data must be deleted or replaced.

Security

Personal data must be protected.

Liberty

Processing data can only be done with free, express, and informed consent, unless an exception applies.

Confidentiality

Every person involved in the processing of data must guarantee confidentiality.



ARGENTINA'S PDPL



DATA TRANSFER

Generally, data transfers to third parties require the data subject's consent.

Data transmissions from controllers to their processors don't require consent. A contract is required.



INTERNATIONAL DATA TRANSFER

Requires adequate level of protection for intl data transfers.

Exceptions to adequacy include data subject consent, when necessary for the data subject's medical treatment, or when for banking or stock exchange operations, among other things.

Data transfer to countries without adequate levels of protection can occur with use of model contracts, DPA approval, or BCRs.



INDIVIDUAL RIGHTS

Right to Be Informed

Right to Update and Rectify

Right to Access

Right to Challenge Automated Decisions

Right to Deletion



ENFORCEMENT

Enforced by the Data Protection Authority (DPA).

The DPA can issue fines of up to 100,000 Argentine pesos – which is about US \$1,700.



Possible criminal penalties with jail fine up to 3 years. Suspension and closure of data processing activities.

Data subjects can bring lawsuits for violations.

PROCESSING DATA WITHOUT CONSENT

Personal data can be processed without consent when the data is:

- publicly accessible
- contained in databases (limited to disclose no more than names, ID numbers, taxpayer ID numbers, occupations, dates of birth, or addresses)
- used for the exercise of government powers or legal obligations
- necessary for the fulfillment of contractual, scientific, or professional obligations
- used for transactions by financial entities regarding information of their clients
- used for advertising purposes when the data only identifies the belonging of a data subject to generic groups based on similar preferences or behaviors



DATA BREACH NOTIFICATION

No data breach notification requirement.

However, the DPA has issued a guideline recommending that data controllers and processors notify the DPA of data breaches.



Convention 108+

- International cooperation.
- Foreign Affairs and Worship Commission already approved.
- Updated global standards.
- Ratification expected by the end of the year.

Tendency to create legal "precedent" through sanctions.

- In order to protect privacy
- Take into account international standards, even if they are not current law.
- Current law has outdated sanctions.

Colombia



SCOPE AND APPLICABILITY

Applies to the collection and processing of personal data that occurs in Colombia about its residents.



Recently interpreted to apply to organizations outside of Colombia.



PRINCIPLES OF DATA PROCESSING

Legality

Processing data must comply with law

Purpose

Processing data must be for a legitimate purpose.

Liberty

Processing data generally requires the express and informed consent of data subjects.

Accuracy or Quality

Data must be accurate, complete, clear, up-to-date, verifiable, and comprehensible.

Transparency

Data subjects must be informed about the existence of data related to them.

Access and Limited Circulation

Data processing can only be done by authorized entities. Personal data can't be improperly disclosed.

Security

Personal data must be protected.

Confidentiality

Every person involved in the processing of data must guarantee confidentiality.



THE PLAYERS

Data Subject



Controller



Processor



Data Protection Authority (DPA)



PERSONAL DATA

Identified



Identifiable

SENSITIVE DATA

Sensitive data is defined as any data that affects the individual's intimacy or whose improper use may cause discrimination. Sensitive data includes information about:

- racial or ethnic origin
- religious or philosophical beliefs
- political opinion
- trade union or political organization membership
- health or sex life
- genetic or biometric data



LAWFUL PROCESSING

Six lawful bases to process personal data include:

- consent
- data requested by gov't entities pursuant to law
- data of a public nature
- in cases of medical, or sanitary urgency
- for historical, statistic, or scientific purposes authorized by law
- data in the civil registry of citizens available to the public (ID number, last names, and place and date where the ID was issued)



CONSENT

Consent must be informed and given prior to the data processing. For consent to be informed, the controller must notify data subjects about the purpose of the data processing and their legal rights, among other things.

Silence or inaction are not valid consent.

Data subjects can withdraw consent at any time.

Exception: No consent required for personal data of "public nature" (ID numbers, professionals, public or court documents)



RESPONSIBILITIES OF ORGANIZATIONS

National Registry of Databases



Data Protection Officer (DPO)

Respond to Data Subject Requests



Internal Processes and Policies



Accountability



Time Limits For Data Processing

Security



Colombia's

General Personal Data Protection Law

INDIVIDUAL RIGHTS

Right to Know, Update, and Rectify



Right to Request Proof of Consent

Right to Complain



Right to Revoke Consent and Request Deletion



Right to Complain



Right to Access



Right to Know the Use of the Data



ENFORCEMENT

Enforced by the Data Protection Authority (DPA). Maximum fine is up to 2,000 minimum statutory monthly wages (about US \$500,000).



Possible criminal penalties with jail time. Suspension and closure of data processing activities. Data subjects can bring lawsuits for violations.



DATA TRANSFER

Generally, data transfers to third parties require the data subject's consent.

Data transmissions from controllers to their processors don't require consent if there is a contract.



INTERNATIONAL DATA TRANSFER



Requires adequate level of protection for intl. data transfers.

Exceptions to adequacy include consent or conformity declaration by DPA for a specific data transfer.



TEACHPRIVACY

www.teachprivacy.com
Privacy Training by Prof. Daniel J. Solove

Colombia

Current overview

Currently, data protection legislation is defined as homologous and similar to the GDPR.

Extensive coordination with foreign data protection agencies.

The SIC works hand in hand with the different industries for the creation of public policies.

Regulatory sandbox project on Artificial Intelligence

- The protection of personal data is highlighted.

Approval of the *Borrón y Cuenta Nueva* Law

- This law obliges financial institutions to notify debtors before a negative credit report is created for them.
- Awaiting of executive sanction.

Publication of non-binding guidelines

- Data protection in the cloud, the principle of proven liability in international transfers, handling of cybersecurity incidents, the treatment of personal photos and best practices for e-commerce.

OTHER issues, Hot Topics and Discussions