
GDPR's extraterritorial scope and Update on the Global GDPR Mandates in Latam

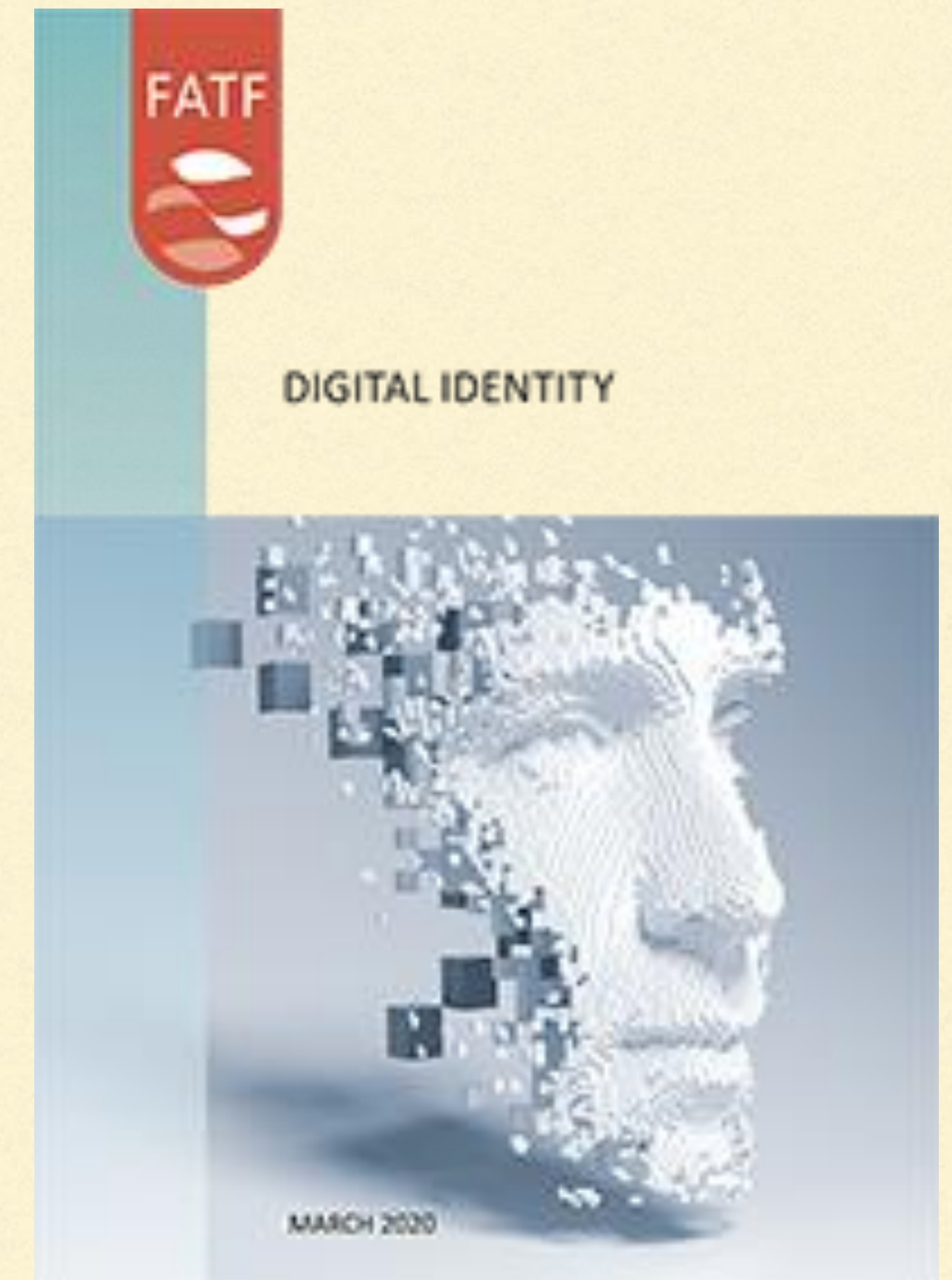
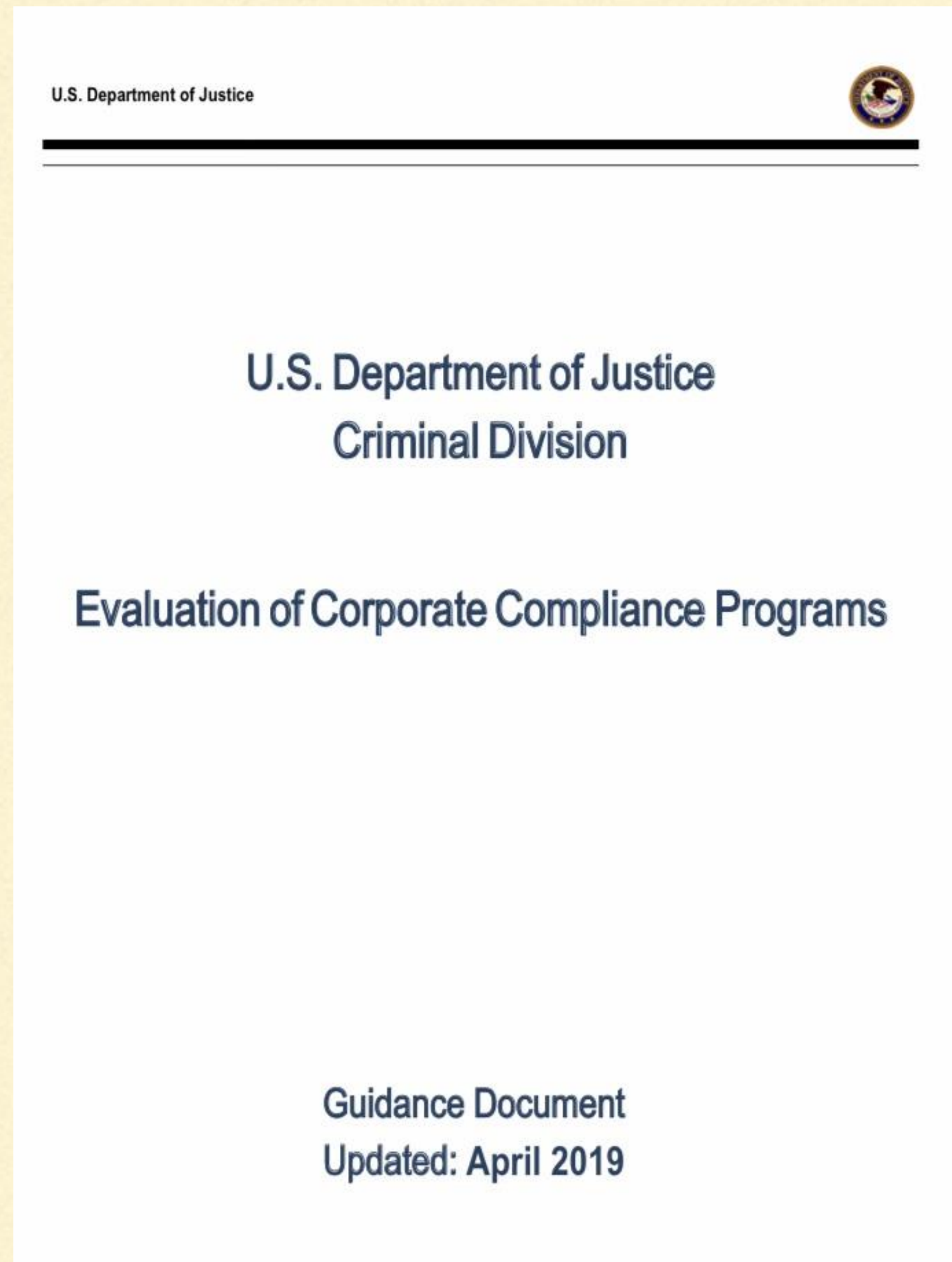


-
- Paula Andrea Aravena
 - Managing Director



Compliance Board Group

In 2019 steps were taken **to align international compliance regulation** to prevent financial crime and cybercrime.



China

Codes of ethics for artificial intelligence.

Zeng Yi, director of the **BAAI**
(Beijing Academy of Artificial Intelligence)

<https://www.baai.ac.cn/news/beijing-ai-principles-en.html>

"To promote the progress of society and human civilization **to advance the sustainable development of nature and society**".



Japan



Masahiko Tominaga, from the Ministry of Internal Affairs and Communications of Japan.

"To start thinking about the challenges of evaluating, implementing and managing risks and responsibilities, in terms **security, cybersecurity, privacy and **ethics**".**

EUROPE

The Digital Single Market

Is a strategy of the European Commission to guarantee that all people, companies and member states have equal access to internet throughout the EU in order to encourage participation in **digital economy** and society.

GDPR

The general data protection regulation is applicable from 25 May 2018, is considered a model framework for data privacy laws around the world.



Latin America

Countries with data protection laws

Mexico, Costa Rica, Dominican Republic, Colombia, Peru, Brazil, Argentina, Uruguay, Chile.

In Chile the data protection legislation is currently under discussion to comply with GDPR standards along with renowned national experts and Senators and Deputies.

Countries with initiative of data protection laws

Guatemala, Panama, Ecuador.



Country	Data Protection Regulations
ARGENTINA	<ul style="list-style-type: none"> ❖ Law N° 25.326 ❖ Law N° 26.9521
BRAZIL	❖ Law N° 13.709/18 or General Data Protection Law (LGPD)
CHILE	<ul style="list-style-type: none"> ❖ Law N° 19.628 on Protection of Private Life. (There is an initiative to modify this Law).
COLOMBIA	<ul style="list-style-type: none"> ❖ Statutory Law 1.581, of October 17, 2012 ❖ Decree 1.377 of 2013 that partially Regulates Law 581 of 2012
COSTA RICA	<ul style="list-style-type: none"> ❖ Law N° 7.975 ❖ Law N° 8.968
ECUADOR	❖ Initiative for the Organic Law for the Protection of the Rights to Privacy and Privacy on Personal Data
MEXICO	<ul style="list-style-type: none"> ❖ Federal Law for Personal Data Protection by Private Persons. ❖ Regulations for Personal Data Protection by Private Persons.
PANAMA	❖ Draft Law N° 665 on Protection of Personal Data
PARAGUAY	<ul style="list-style-type: none"> ❖ Law N° 1.682 ❖ Law N° 1.969
PERU	<ul style="list-style-type: none"> ❖ Law N° 29.733 of Protection of Personal Data ❖ Regulation of Law N° 29.733
DOMINICAN REPUBLIC	❖ Law N° 172-13
URUGUAY	<ul style="list-style-type: none"> ❖ Law N° 18.331 on Protection of Personal Data and Habeas Data Action ❖ Decree 414/2009 ❖ Law N° 19.030

GDPR	ARGENTINA	BRAZIL	CHILE
	<ul style="list-style-type: none"> ❖ Law N° 25.326 ❖ Law N° 26.9521 	<ul style="list-style-type: none"> ❖ Law N° 13.709/18 or General Data Protection Law (LGPD) 	<ul style="list-style-type: none"> ❖ Law N° 19.628 on Protection of Private Life. (There is an initiative to modify this Law).
Extraterritorial application	No	Yes, it is established that the Law applies any treatment regardless of the medium, country of residence or oasis where the data is located.	No. (It only refers to data processing by public or private entities).
Database Registration	Yes	No	No
Information / Consent	It is mandatory to previously inform the holders about the treatment that their personal data may receive. Consent must be free, express and informed, in writing or granted by another comparable means.	Holders must be informed about the conditions of the treatment. Consent must be free, informed and unequivocal.	Written consent it is required, it must be free, informed and unequivocal.
Rights of the holders of personal data	Right to information, access, rectification, updating and deletion.	Confirmation of existence of the treatment, access, correction, anonymization, portability, suppression, to know the data communications made, to know the consequences of not granting consent, and revocation of consent.	Information, rectification, cancellation and blocking
Foreign transfer restrictions	Yes (The transfer of personal data of any kind with countries or international or supranational organizations that do not provide adequate levels of protection is prohibited).	Yes, adequate guarantees are required for transfers to third countries.	There are no specific provisions on international data transfers.
Security measures	The necessary technical and organizational measures must be adopted to guarantee the security and confidentiality of personal data.	Yes, the obligation to have technical and administrative security measures is established to carry out the data treatment.	Although there are no specific provisions on security measures, article 11 establishes the obligation to secure data.
Violation notifications	It is not required	Yes, the authority and the owner must be informed within a “reasonable” period.	There are no specific provisions on security breaches.

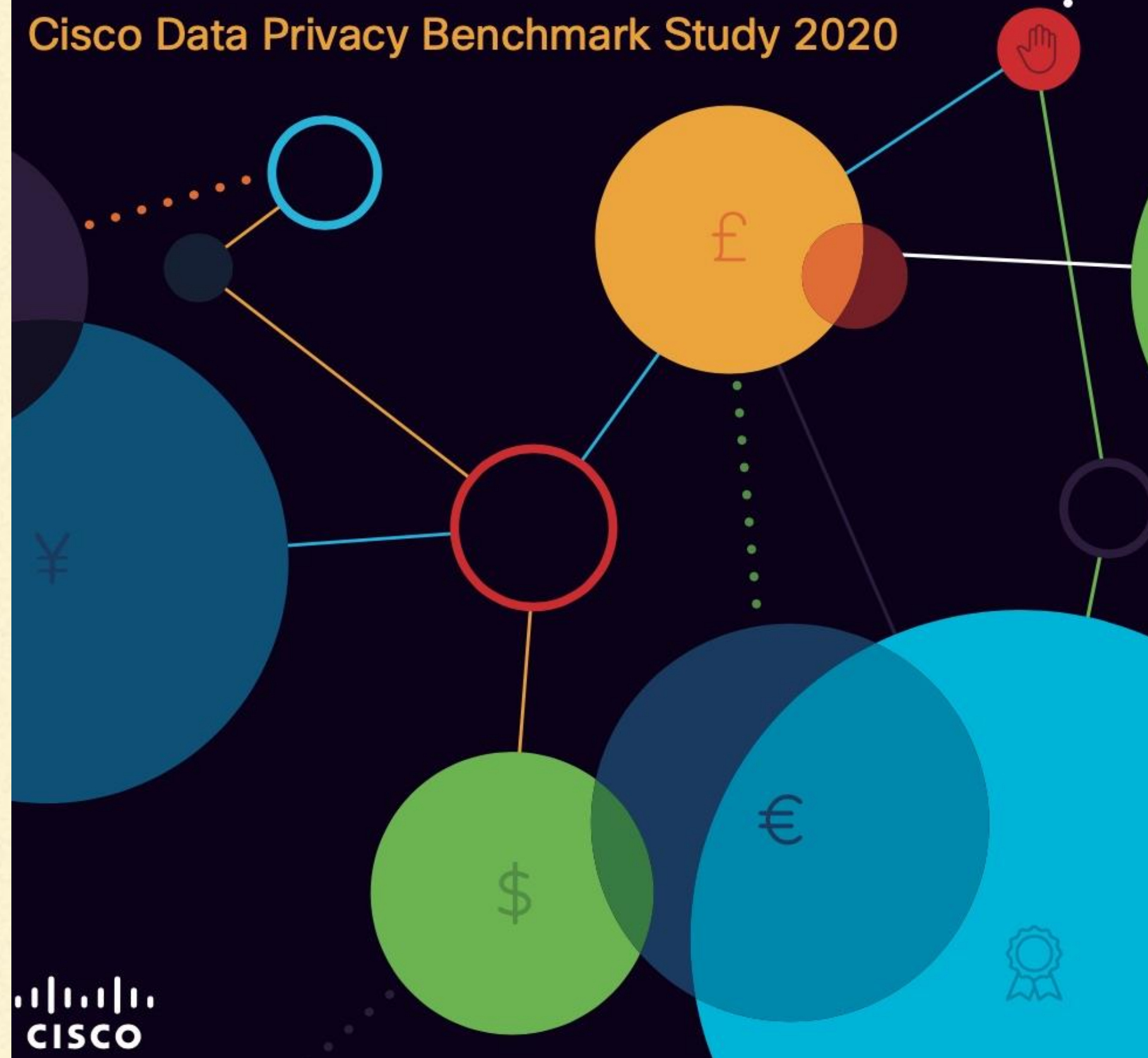
GDPR	COLOMBIA	COSTA RICA	ECUADOR
	<ul style="list-style-type: none"> ❖ Statutory Law 1.581, of October 17, 2012 ❖ Decree 1.377 of 2013 that partially Regulates Law 581 of 2012 	<ul style="list-style-type: none"> ❖ Law N° 7.975 ❖ Law N° 8.968 	<ul style="list-style-type: none"> ❖ Initiative for the Organic Law for the Protection of the Rights to Privacy and Privacy on Personal Data
Extraterritorial application	Yes. Resolution 1321 (Facebook case of January 2019) Law 1581 is applicable to the processing of personal data regardless of whether the Data Controller or the Data Processor is physically located in the territory of the Republic of Colombia	No. It is only applicable to personal data that appear in automated or manual databases, of public or private organizations, and to any form of subsequent use of this data.	
Database Registration	Yes. The databases must be registered with the Superintendence of Industry and Commerce.	Yes. It is established that Prodhab must keep a registry of databases.	
Information / Consent	You must have a Notice and Privacy Policy. Consent must be prior, express and informed	The data processing must be reported. Consent must be express in writing (physical or electronic means).	
Rights of the holders of personal data	Right of access, know how to update and rectify your data, revocation of authorization, file complaints for infractions of the law	Right of access and rectification, deletion and consent to the transfer of your data	
Foreign transfer restrictions	Yes. Transfer to third countries that do not guarantee adequate levels of protection is prohibited.	Yes. They are subject to the express consent of the owner.	
Security measures	Yes. There must be technical, human and administrative measures that are necessary to grant security to the records, avoiding their adulteration, loss, consultation, use or unauthorized or fraudulent access.	Yes. Technical and organizational measures are required.	
Violation notifications	Yes, the data protection authority must be informed.	There is no provision in this regard.	

GDPR	MEXICO	PANAMA	PARAGUAY
	<ul style="list-style-type: none"> ❖ Federal Law for Personal Data Protection by Private Persons. ❖ Regulations for Personal Data Protection by Private Persons. 	<ul style="list-style-type: none"> ❖ Draft Law N° 665 on Protection of Personal Data 	<ul style="list-style-type: none"> ❖ Law N° 1.682 ❖ Law N° 1.969
Extraterritorial application	Yes. It is established that the legislation may be applied to managers regardless of their location, in case the responsible party is not established in Mexico.	No	There are no forecasts in this regard.
Database Registration	It is not required.	No	There are no forecasts in this regard.
Information / Consent	It is necessary to inform the holders about the treatment of their data through the Privacy Notice. Consent must be free, specific and informed.	The owners must be informed about the use of their data. Consent must be granted by means that allow its traceability.	The owners must be informed about the treatment of their data.
Rights of the holders of personal data	Right of access, rectification, cancellation and opposition	Right of access, rectification, cancellation and opposition.	Information and update.
Foreign transfer restrictions	Yes. The receiving person in charge must assume the same responsibilities as those corresponding to the person in charge of communicating the data.	Yes. Standards must be established to those provided for in Panama legislation.	There are no forecasts in this regard.
Security measures	Yes. Physical, technical and administrative security measures are required.	Aspects of personal data security are not specified.	There are no forecasts in this regard.
Violation notifications	No. (In public sector regulations if required).	Aspects of personal data security are not specified.	There are no forecasts in this regard.

GDPR	PERU	DOMINICAN REPUBLIC	URUGUAY
	<ul style="list-style-type: none"> ❖ Law N° 29.733 of Protection of Personal Data ❖ Regulation of Law N° 29.733 	<ul style="list-style-type: none"> ❖ Law N° 172-13 	<ul style="list-style-type: none"> ❖ Law N° 18.331 on Protection of Personal Data and Habeas Data Action ❖ Decree 414/2009 ❖ Law N° 19.030
Extraterritorial application	Yes. It is established that the legislation may be applied to managers regardless of their location.	There is no legal provision in this regard	Yes, when the person in charge of the database or treatment is not established
Database Registration	Yes, it is necessary to register the data banks with the National Registry of Data Protection.	There is no legal provision in this regard	Yes. They must be registered in the URCDP Registry of Personal Databases
Information / Consent	It is necessary to inform the holders about the treatment to which their personal data will be subjected in a detailed, simple, express and unequivocal way. Consent must be free, prior, express, informed and unequivocal.	The owner must be informed in advance about the treatment to which their personal data will be subjected. The consent must be free, express	The owner must be informed about the treatment of their personal data. Consent must be unequivocal, simple, clear and free.
Rights of the holders of personal data	Right to information, access, update, inclusion, rectification, deletion, prevent supply, opposition, objective treatment, guardianship and compensation.	Access, rectification, cancellation, opposition and compensation	Right to information, access, update, inclusion, rectification, and deletion.
Foreign transfer restrictions	Yes. Transfers are subject to the consent of the owner and an adequate level of protection of the transferred personal data must be guaranteed.	Yes, the consent of the owner is required and that it is allowed according to the Law.	Yes. They require prior authorization from the data protection authority.
Security measures	Yes. Technical, organizational and legal security measures are required.	Yes. The duty of security on personal data is established.	Yes. Technical and organizational measures are required to guarantee security.
Violation notifications	There is no legal provision in this regard.	There is no legal provision in this regard	Yes, the holders must be informed when they may affect their rights.

From Privacy to Profit: Achieving Positive Returns on Privacy Investments

Cisco Data Privacy Benchmark Study 2020



January 2020

How GDPR can help to create a robust business with Latam

In its most recent Data Privacy study Cisco calculated a **ROI for privacy**, and it shows that most organizations are getting a **positive return on their privacy investments**.

The respondents around the world recognize the importance of complying with **GDPR**.

(Survey of 2800 security professionals in 13 countries included **Mexico** and **Brazil**)

Average privacy returns by country

Global average: Benefits = 2.7 times investment

N=2543



Keep training your team

4 of 5

Top causes of **data breaches** are due to **human** or **process error**.

Information Commissioner's Office (ICO), 2018.



I hope this information will be helpful to you all.
