COSMOS
Navigate the Compliance Universe

CEP Magazine - March 2025

Mónica Ramírez Chimal (mramirez@asserto.com.mx, linkedin.com/in/mramirezchimal) is Partner and Founder of consulting firm Asserto RSC in Mexico City, Mexico.

Beyond the privacy notice

By Mónica Ramírez Chimal, MBA

What does your company do to comply with data protection laws? If your answer is a privacy notice, sorry to tell you, your company isn't complying.

There are four common mistakes:

1. People think the law only applies to companies, but it doesn't. It also applies to individuals who gather data from others, like doctors, accountants, photographers, etc.
2. People ask for more information than is needed; the more information you handle, the more controls you need.
3. People apply a general privacy notice for any information gathered. Some even get their privacy notice online or copy it from other companies. The privacy notice must be custom-made based on the company's processes and controls.
4. People don't check what type of information they're gathering. There's a difference between asking for someone's name and address versus having their medical records, taking their photo, or recording a video.

Data protection laws vary from country to country, but they align to protect people's and companies' data from being used without their consent (e.g., through leaks, data loss, failures in the storage system).

In Latin America, there were 1,185,242 ransomware attacks between June 2023 and July 2024—3,247 per day. Brazil, Mexico, Ecuador, and Colombia were the most attacked countries in the region, respectively.[1]

Mexico, Colombia, Chile, Argentina, Peru, Brazil, Bolivia, Ecuador, Paraguay, and Uruguay already have data protection laws in place. They were developed mainly because of the influence of the EU data protection framework.

So where do you start? These questions can help you know what to do no matter the country:

- Where is the data collected from (directly from the person, through the website, etc.)?
- What type of information is needed (name, address, phone, email, age, gender, religion, etc.)?
- Why is the data needed? This must be answered according to what the company or individual provides.
- Where is the data? Create a map to show where the data is and who has access to it.
- Is a copy of the data needed? If so, where is it? Who has access?

- Is the data shared? If so, by whom and why? Check if your agreements with third parties cover data protection.
- When and how is the data deleted?

With the answers to these questions, you can start complying with the appropriate laws, and the privacy policy, procedure, and notice can be developed. Alerts can also be set up, and staff can be trained. All of this will help create a culture of privacy.

Stay tuned for the next *Compliance in LATAM*!

1 Kaspersky, "América Latina registra un aumento del 2.8% en los intentos de ataque de ransomware," October 28, 2024, https://latam.kaspersky.com/about/press-releases/america-latina-registra-un-aumento-del-28-en-los-intentos-de-ataque-de-ransomware.