Why companies in Mexico should reassess their compliance with data privacy protocols — and their risk of a data breach

08 January 2018

According to the Constitution of Mexico, the protection of personal data is a fundamental right of all Mexican citizens. Under federal law, individuals also have a right to access, change, oppose, or suppress their personal data. Although all private companies process data, some are not sufficiently familiar with Mexico's data privacy principles and regulations, and many may not have an up-to-date assessment of their own risk of a data breach. In addition, they may not be aware that the Mexican Supreme Court's recent shift in perspective regarding personal injury cases may herald a change in the way data privacy breaches are handled in the future.

In this hoganlovells.com interview, Federico De Noriega Olea, a partner at Hogan Lovells in Mexico City, explores the impact of Mexico's data privacy regulations on private companies, discusses the unique approach of Mexican regulators to data privacy enforcement, and offers advice as to how companies can stay compliant.

What would you advise private companies in Mexico do now to ensure they have strong and compliant data privacy protocols in place?

De Noriega Olea: Typically what I would recommend they do first is take an assessment and inventory of what kind of data they process — whether it's consumer data, big data, or just business-to-business data.

I'd say the second step would be to see how they process that information and for what purposes they use the information. Processing is what they do with the information. For instance, whether they simply hold the information in order to have contact information for the client to collect receivables or enforce contracts, or if they send marketing communications of their own products and services to the customer database.

Or, if they want to take it one step further, if they sell the data to third parties or strategic partners so they can jointly market the product to customers. We want to understand what the uses are for this data.

After a company makes that general assessment, what's the next step they should take?

De Noriega Olea: The next step would be to identify the risks related to, and the uses they make of, those databases. They should ask questions such as, what is the risk of any data breach? Does the company have a risk of customers complaining about certain uses of those data? Have customers consented to such uses? Are customers aware of how the company is processing their information and what kind of information the company has on their customers?

Companies should also try to do a gap analysis or a compliance analysis and see how far they are with respect to their compliance with legal principles and statutory obligations related to data privacy and cybersecurity.

Does Hogan Lovells help companies in Mexico do these types of risk assessments?

De Noriega Olea: Yes, of course. We help companies assess compliance, do gap analysis, and implement solutions from the compliance and legal compliance side. To do a cybersecurity assessment, we typically partner with someone else — a technical expert, because we need to add some technical system experience to that. But we certainly have done many assessments of the kind I am describing and have helped companies perform them internally.

You mentioned legal compliance. For your clients, what specific Mexican data privacy regimes should they be aware of?

De Noriega Olea: The first thing you need to establish is whether it's a private company or a government-owned company. They each have different regulations. We deal mostly with private companies, not with Mexican government entities.

For private companies, there's a statute in Mexico, which is sort of modeled on EU law, called the Federal Law on the Protection of Data Held by Private Parties. This statute regulates both the principles and general requirements that companies must comply with, with respect to data processing, including requirements such as sending privacy notices, putting security measures in place, and naming a data protection officer.

In addition, companies should be aware of how, generally speaking, data subjects or data owners can exercise their rights to access, rectify, cancel, and suppress the information that companies have about them.

And the last thing they should know, which is important, is the sanctions that the regulator — the data protection authority — may impose on companies that breach legal requirements.

If private companies don't meet their obligations, what do they risk in terms of penalties, sanctions, or fines?

De Noriega Olea: They risk an administrative penalty, and the sanctions are mostly just monetary fines. The highest fine that the regulator may impose is about US$1.5 million for each infringement, but that can be doubled if the breach relates to sensitive personal information; in those cases, the fine could be as much as around US$3 million.

Aside from fines, companies that breach data protection laws may be subject to civil liability, although we haven't seen any cases of civil liability or someone claiming or fighting a civil liability lawsuit filed against them for breach of data protection laws.

In limited cases, infringements may lead to criminal liability but malicious intent is a condition to criminal liability in most of those cases.

Do you anticipate that at some point there will be civil liability law cases related to breaches of data privacy?

De Noriega Olea: I think that one thing that has prevented individuals — because the law protects only individuals — from filing civil lawsuits against private companies is the fact that our damages laws in Mexico provides only for remedies such as direct and immediate damages, and do not contemplate consequential or punitive damages. When there is a data protection breach, it's very hard to prove that there was direct and immediate damage from that breach. The standard of proof is very high.

Now this may change, because a couple of years ago, our supreme court started opening a window toward awarding punitive damages and consequential damages in certain personal injury cases, and not cases that are data privacy related. But this is just to say that our whole damages framework and damages laws may have been amended by supreme court precedent recently, and that may give rise to other claims, including civil liability claims derived from data protection breaches.

You said that companies are obligated to send data privacy notices. Is there anything in particular they should know about those notices?

De Noriega Olea: I think one thing to consider of a Mexican regulator is that the enforcement cases they try are mostly related to specific compliance with the requirements that the data privacy notice must have. They interpret those requirements very narrowly and very much to the letter of the law, which makes it very difficult to comply with all of the requirements. This has provoked very lengthy privacy notices in Mexico because there's a list of requirements, but the list is very specific and all the information that the regulator wants to see in the privacy notice is very comprehensive.

To give you an example, one company was sanctioned — not with the highest fine or anything close to that — but it was sanctioned just because they failed to indicate the municipality where the office was located, even though the full street address was included. They simply failed to indicate in which municipality their building was. Just for that minor omission, the regulator imposed a fine.

The Mexican regulator reviews a checklist of everything they want to see in the privacy notice and try to find any single omission. Even if the privacy notice complies with the spirit of the law and the intent of the law, any single omission they find may trigger a fine. In 2017, there haven't been as many enforcement cases, but in the years before, there were numerous cases.

About Federico De Noriega Olea

With more than 10,000 hours of experience in corporate transactions, Federico De Noriega Olea is widely recognized for his deep experience in the financial sector. As a partner in the Mexico City office, he advises clients on financial transactions, mergers and acquisitions, and data privacy issues, including data processing, data transfers, and security breaches. His approach combines a robust knowledge of the legal issues with practical solutions and risk-mitigation strategies.

Contacts

Federico De Noriega Olea

Partner

> Read the full article online