LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

THE POLITICS OF PRIVACY

28 October 2013
Alison O'Connell

Data privacy is the new compliance frontier for Latin American GCs, with a rapidly growing legislative framework in the region. Members at LACCA Miami discussed why now is the time to update policies

Potential fines of €100 million or 5 per cent of company revenue catch a GC's eye. The EU's new rules on data protection, passed last week, strengthen significantly the requirements on businesses which have data passing through any EU country, as well as the potential fines for breaches.

The EU rules are part of a continuing trend in much of the world to regulate data access and transfer, particularly across borders. Multinationals increasingly need to be aware of how they manage data, how they use it, what happens after they use it and overall how they comply with a bipolar regulatory trend across the globe.

Part of this is a government reaction to continuing technological advances and to 'Big Data' – the awareness that there has been more data collected in the last two years than since the beginning of mankind. "In our mobile device era, the issues of privacy are getting more complex because the technology shifts take place faster than ever before, outstripping the ability of law and regulation to keep up – making it a particularly tough time for GCs and compliance in terms of advising international businesses," says Harriet Pearson, a partner at Hogan Lovells, at the recent LACCA meeting in Miami.

With both technology and the law both evolving so quickly, it is tough for GCs to keep up – particularly when there is no coherent global approach, are there is emerging in the field of anti-corruption law. Indeed, the EU and the US have fundamentally different approaches to the concept of data protection – with the US preferring a much lighter regulatory approach.

"The major difference between [the US and EU] models is that for historical reasons, data privacy in the EU is a fundamental matter of human rights, while in the US it is geared more towards consumer protection," says José Arce, director of compliance and privacy officer at Assurant. The US only regulates some industries, such as the financial and healthcare sectors; everything else remains subject to their own industry laws and common law.

Under the EU directive on the other hand, if data collection is identifiable to an individual then its collection, use, management and disposal are all regulated, and this is done so comprehensively from start to finish. "The key term in Europe is "personal data," added Pearson. "The EU framework regulates every aspect of a company's handling of personal data."

The EU rules matter because Latin America, like many other parts of the world, tends towards the EU model of heavy regulation and protection of citizens' data. Most of the region's countries have some form of habeas data - designed to protect information self-determination and essentially means that individuals can request access to any personal data about them held in a database – as a constitutional right, despite slight differences from country to country. For example, in Brazil, the habeas data first included in the Constitution of 1988 applies to records or databanks of government agencies or of agencies of a public character; in Paraguay other hand, the provision was extended to include all governmental, public or private databases in its 1992 Constitution.

Beyond that, the specific legislative coverage over the region is getting fuller. Chile and Argentina were the first enact data protections law in1999- 2000, and for a number of years were the only Latin American countries to have done so. However, Uruguay followed suit in 2008, then Mexico in 2010; since then, a flurry of laws have been passed, by Colombia, Costa Rica, Peru, Trinidad & Tobago and Nicaragua (see here for more details on each of the laws in Pearson's presentation).

Almost all of the regions frameworks are focused mainly on ensuring that individuals are provided with adequate notices from businesses regarding the collection, use, and disclosure of data and therefore, consent can be used as a tool to facilitate access and transferring of information in the region. However, while there are many similarities between the laws, important differences remain too , as Arce notes "it is a dynamic landscape where there are many different laws, different levels of enforcement, where all countries are at slightly different stages of development." (see here for Arce's comparative table on the requirements of the laws, page 10).

The legislative overhaul looks unlikely to stop there - many governments in Latin America are now moving toward exploring new or more enhanced privacy laws. Chile is expected to enhance its 1999 law. In Brazil, data protection is a hot topic right now, amid the recent NSA spying allegations; the government has even gone as far as proposing legislation that would force internet companies to store data collected in Brazil within the country, rather than in a cloud system, though the proposal would prove very difficult to implement. The country is also considering its own omnibus protection law.

While the laws are in place, the region has seen very little enforcement so far – Argentina, which has had a law in place for the longest, has never sanctioned a company. However, that is likely to change, and many countries that already have laws in place are also looking at increasing enforcement. Mexico, having stepped up the power of its data protection authority, the Federal Institute for Access to Information and Data Protection (IFAI), is one of the first out of the starting blocks, recently announcing a fine of US$1 million against one of the country's largest banks for violating data protection laws. While this is only a start, the general consensus is that many other countries will soon be following suit.

Multinational data rules

Above and beyond local legal requirements, GCs also have to be aware of the complex web of rules because of the nature of international commerce – any company with customers, suppliers or business partners in another country will inevitably engender some cross-border data transfer issues; companies with subsidiaries elsewhere even more so. "While respecting domestic laws, companies are increasingly aware of the importance of reconciling in some way the procedural differences between national privacy frameworks for purposes of international business operations and trade – otherwise these cross-border issues pose the potential to be non-tariff trade barriers," Pearson explains.

"If you work for an international company, as soon as you have access to personal data across borders you have to consider international privacy issues. Domestically, you may also have obligations but you especially get a headache when managing compliance with multiple and potentially conflicting frameworks, " she adds.

The EU is particularly concerned about where data about its citizens goes, so it can be sure that the destination country also has rules which will require the same level of data protection. The key word here is 'adequate' - and almost none of the countries in the Americas have adequate data protection, according to the EU. The US most certainly does not; Argentina, the first country in Latin America to adopt data protection laws, is does. That means that companies, restricted from moving data out of the EU to these countries, need to come up with mechanisms under the law to protect the data when moved across borders.

The issue is not only in the moving of information across borders, it is also the access to information that can be equally as challenging. Just looking up information from one country into another is enough to trigger cross border issues. These rules – described as "completely unworkable from a practical perspective" by one participant in the discussion - reflect mainframe era computing and not the instant, online environment in which companies operate. Nonetheless, they have been copied by other regulating bodies.

Big Data is not just a challenge for companies, it is also an opportunity. It gives companies the ability to know much more about its customers and their buying habits, and to target products better. However, such exploitation, while valuable, increases risk too – and thus the burden on legal and compliance. "The chances are that the marketing and business function within your company are already creating programmes to get more value out of data, so GCs and compliance officers need to make sure that they manage the risks of violation of law, breach of contract, or reputational damage to the company," says Pearson.

Overall, these issues create a major concern for counsel dealing with cross border privacy and data protection issues. How can you practically achieve compliance jurisdiction by jurisdiction without creating unnecessary barriers to the business, or even unwitting trade barriers? In essence, how do you give data a passport?

One size does not fit all

The good news for Latin American GCs is that you still have time to consider the issues at hand calmly, with no real fear of a heavy-handed local enforcement action – for now. "In Latin America the legal framework

is still relatively young – although progressing rapidly -- so it's a good time to take steps to build a practical compliance programme including legal mechanisms for data transfer," says Pearson.

The first step is to do an internal assessment. Take a look at what the procedures are for your company internationally, and do a little audit of the countries you deal with and their requirements. By doing so, see what you can use, extend or adapt to your existing policies and customise what you need to.

Knowing what exactly what type of information your company handles is also key. "One size does not fit all," says Arce. "Is your company handling sensitive information such as health, criminal records, credit records, etc, or is it payment information? Is it personal identifiable information which is not considered sensitive by applicable law, or is it HR information?" Find out what you are dealing with as this will affect the type of regulations you face.

Angel Olivas, regional compliance officer for Johnson Controls, noted that, as with anti-corruption compliance, companies' obligations extend beyond their own direct operations. "Some of the due diligence procedures that now require businesses to have a clear understanding of what their partners are doing inevitably brings with it a clash of data protection issues," he says. Companies must follow the data, to confirm that third parties have the appropriate security and that they do not use data in a way that runs against the obligations that you have.

Current IT habits make this all the more relevant. Cloud computing has replaced country-specific data centres, and more services are outsourced. Many companies are therefore using third party contractors who store information in a cloud system, so it is becoming essential to make sure you know where the information is collected, where it resides, and who has access to it in order to be aware of which local laws apply. This is particularly important since more and more companies are employing mobile technology – which has an even less clear regulatory status.

However, following the data can be a nightmare. "What happens when you employ companies to store data? I have found that HR often do not know where the data is stored and who has access to it," says Bettina Freire, associate general counsel at Avnet.

Once you have a good awareness of how your company and its third parties, you will also have a much better concept of the risks being faced. Some companies which find themselves at risk of an enforcement action, or even just a reputational issue, are beginning to employ 'incident teams', like crisis management teams, that would be ready to mobilise and advise the company in case of a breach. "This is a very active area which is becoming more and more common, with some going one step further and purchasing insurance for instances such as these," says Pearson.

Companies in Latin America may not find themselves at that stage yet. But the time has come to implement these concepts into your compliance programme, given the velocity of change in the region. "What is interesting is that 10 years ago we would not be discussing Latin America in regards to these issues," says

Pearson, "there wasn't enough activity from a legal or regulatory perspective. Now however, there is critical mass and many countries have emerged and come onto the scene with their own requirements."

There may be no enforcement actions yet – but few doubt that they will come, sooner or later. Now is the time to ensure that your company is not the subject of the first to be launched.