GDR NEWS

Latin America steps up data privacy legislative and enforcement efforts

07 May 2019

*Holland & Knight partner **Adam Bookbinder**, associates **Mara O'Malley and Javier Robledo** and legal intern **Timothy Andrea** consider developments over the last few months that showcase Latin American countries' increased data privacy efforts.*

Developments over the past several months demonstrate that Latin American countries are increasingly engaging in both legislative changes and enforcement efforts to protect the privacy of their residents' personal data. Colombia made this especially apparent through its recent **investigation** into Facebook's data security practices.

First published on the Global Data Review website, May 2019

Other countries, including Brazil, Argentina, and Chile, have taken substantial legislative steps towards implementing data privacy regimes similar to the GDPR.
While it is too early to assess the impact of these changes, these countries are sending a clear message that they will protect the privacy of their residents' data just as the EU countries and state governments in the US have done.

Colombia
On 24 January 2019, Colombia's Superintendency of Industry and Commerce (SIC) sent a message to companies worldwide when it issued a resolution requiring Facebook to do a better job of protecting Colombian residents' personal data. The SIC has authority to investigate entities that process personal data and to order non-compliant entities to bring themselves into compliance. The SIC can also prohibit entities from collecting or processing personal data if there is evidence that there are risks to the data the entity holds or processes.

The SIC's Facebook investigation resulted from troubling international revelations about Facebook's security practices. For example, through the "Facebook Platform" programme, third-party developers of Facebook-compatible apps were able to access stores of personal data the company had collected. The SIC specifically cited Cambridge Analytica's misuse of the personal data of more than 50 million Facebook users, including nearly 150,000 in Colombia, to manipulate users through fake news. The SIC also noted that towards the end of 2018, Facebook notified users that more than 800 developers had accessed both public and private photographs of more than 5 million users without their consent.

The SIC relied heavily on findings from other countries' data regulators that had investigated Facebook – most notably, the UK Information Commissioner's Office, which **fined** Facebook £500,000 (€564,726) as a result of the Cambridge Analytica incident. Ultimately, the SIC found that

Facebook's measures to protect the data of its 31 million Colombian users were insufficient and ineffective, despite Facebook's assurances to the contrary.
To address these deficiencies, the SIC ordered Facebook to strengthen its data security posture in several ways, including developing and implementing a written security programme that Facebook must periodically test for effectiveness. The company must also adjust its contracts with third parties to ensure that all data processing complies with Colombian law.

The SIC's resolution relies on several different provisions of Colombian law relating to the protection of personal data, which is defined as any information relating to or that could be associated with one or multiple identified or identifiable natural persons. In particular, Colombia's Constitution explicitly provides for the protection of personal privacy and personal data, as does **Colombia's data protection legislation**.
Violations of these laws can result in monthly fines for as long as the violation continues, the suspension of personal data processing, and the immediate and permanent shutdown of operations involving sensitive data (such as data related to a person's religion or race).

Whether Colombia will impose any of these penalties on Facebook remains to be seen. Facebook had four months from 24 January 2019 to implement its improved security measures, meaning that it must take the required steps by 24 May or be in violation of the SIC's resolution. Whether and how Facebook will respond, and what the Colombian government will do if it finds Facebook's response insufficient, are open questions. What is clear is that how this situation plays out will be an indicator of whether Latin American countries interested in protecting their residents' data have the ability to alter the behaviour of the largest global corporations.

First published on the Global Data Review website, May 2019

GDR NEWS

Brazil

Brazil has taken active steps towards implementing a national privacy regime, most recently by **authorising** the creation of the National Data Protection Authority in December 2018 through an executive order. The executive order came only four months after the August 2018 passage of Brazil's first omnibus data protection legislation, known as the **LGPD**.

The LGPD, which is scheduled to take effect by August 2020, is premised on two fundamental rights set forth in Brazil's Federal Constitution: the right to privacy and the right to the secrecy of correspondence. The LGPD is modeled on the GDPR. It closely tracks many of the GDPR's key provisions, including data subject rights, the data protection officer requirement, and the bases for processing personal data.

The LGPD will govern the processing of two categories of data – personal data and sensitive personal data. Personal data is only vaguely defined as "information related to an identified or identifiable natural person," and it remains an open question whether this definition will be clarified before the LGPD goes into effect in 2020. Sensitive personal data is defined as "personal data on racial or ethnic origin, religious belief, public opinion, affiliation to union or religious, philosophical or political organisation, data relating to the health or sex life, genetic or biometric data, whenever related to a natural person." Not surprisingly, the LGPD provides greater protections for sensitive personal data.

While the December 2018 executive order authorised the creation of the ANPD, Brazil's Congress must still approve this order for it to take effect. Assuming the Congress does so, the ANPD will have authority to issue necessary regulations interpreting the LGPD. The ANDP will also assess LGPD violations and impose fines when appropriate.

First published on the Global Data Review website, May 2019

Argentina

Argentina's legislature is **considering** a bill introduced in September 2018 that would significantly reform the nation's data privacy laws in ways that would make them similar to the GDPR.

The bill codifies core rights of data subjects, including the right to access a copy of the personal data held by processors and the right to have personal data deleted once processing is complete. The bill also sets out different forms of consent that data subjects must provide, depending on the type of personal data being collected. For example, explicit (as opposed to implicit) consent is required for international transfers and for collection of information about race, religion, and sexual orientation – all of which is considered sensitive data.

The bill also requires entities that control or process data to implement internal procedures to protect personal data; procedures to assist data subjects in exercising their rights; and internal or external audits to ensure compliance. Other key obligations include reporting security incidents without undue delay, if possible within 72 hours of learning of the incident; and, for entities processing sensitive data on a large scale, designating a data protection officer.

Finally, the bill establishes penalties for non-compliance. Beyond issuing fines and warnings, the National Data Protection Authority can impose a suspension of data processing until entities adopt corrective measures. And if the processing activities involve sensitive data, the authority can immediately and permanently close processing operations.

Chile

As in Argentina, Chile's legislature is considering legislation that would make important changes to the nation's data privacy laws. The bill was **introduced** in January 2017 and the latest set of changes proposed by legislators were formally **submitted** to the Senate in June 2018. Multiple steps are still required before the bill can be adopted and implemented, but it

appears likely that Chile will join the other Latin American countries looking to enhance their residents' data privacy.
Like the Argentinian legislation, the Chilean bill would require entities controlling or processing data to obtain consent from data subjects and explicit consent for sensitive data and international transfers. It would also require entities to adopt technical, organisational and training measures to guarantee data safety and would require entities to report security breaches without undue delay.

The proposed legislation would also create a new data protection agency in Chile, the Personal Data Protection Agency, which would be responsible for ensuring compliance with data privacy laws and regulations, creating general guidelines for the implementation of those laws and regulations, and conducting investigations and imposing fines.

This bill would also implement a novel penalty structure, classifying infractions into three categories ranging from minor violations to very serious violations. Minor infractions would generally consist of administrative violations, such as missing deadlines or omitting information in disclosures. Serious and very serious infractions would generally involve unlawful processing activities, with the main difference being that knowing infractions are classified as very serious. The primary penalty would be a fine of between 1 and 5,000 Monthly Tax Units (which, as of the date this publication, is approximately US$70 to US$350,000). As with the GDPR, in some cases fines could be as high as 2% to 4% of companies' annual turnover. Fine amounts would depend on the category of infraction, any mitigating or aggravating factors, and the size of the company. For repeat infractions, the agency would be authorised to impose fines three times higher than the original fine, as well as temporary or permanent suspensions of processing activities.

First published on the Global Data Review website, May 2019

Conclusion

From Colombia's Facebook decision to the new data privacy legislation adopted in Brazil and pending in Chile and Argentina, Latin American countries are launching ambitious efforts to protect their residents' personal data. Companies doing business in Latin America or processing data of Latin American residents will have to pay attention to these developments or face potentially significant consequences.

First published on the Global Data Review website, May 2019