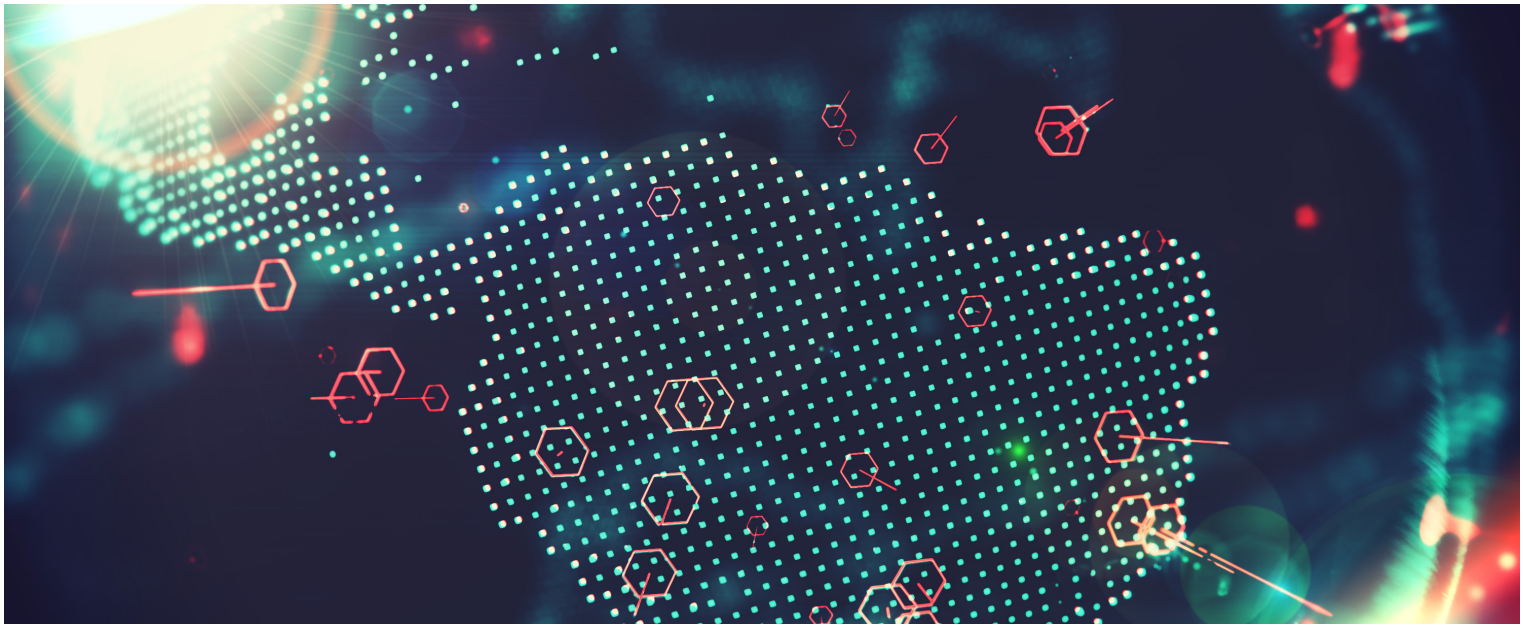
May 2019

International: The impact of the GDPR in Latin America - Part 1

Since the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect on 25 May 2018, several jurisdictions outside of Europe have proposed, and sought to harmonise their data protection laws with, the legal frameworks of the EU. In the first instalment of this two-part article, DataGuidance by OneTrust spoke with experts in Brazil, Uruguay, Peru, and Argentina, who each provide a brief overview of recent legislative developments in their jurisdictions, and discuss whether the GDPR has been a factor in the same.



blackdovfx/Essentials collection/istockphoto.com

Brazil

Driven by the GPDR's entry into force, Law No. 13.709 of 14 August 2018 Which Provides for the Protection of Personal Data and Amends the Federal Law No. 12.965 of 23 April 2014 ('LGPD') was partially approved by the President of the Republic, Michel Temer, with vetoes, on 15 August 2018. After years of debate, the LGPD will comprehensively regulate the use of personal data in Brazil, both in the private and public sector, and will significantly transform the data protection system in Brazil to move it more in line with the GDPR.

As the GDPR and the LGPD have largely similar requirements, organisations that have undertaken reasonable efforts to become compliant with the GDPR will be in a better position to proceed with the necessary measures to become compliant with the LGPD. In any case, specific adjustments are necessary, particularly regarding the lawful bases that allow the processing of per-

sonal data (e.g., the GDPR provides for six lawful bases, while the LGPD provides for ten), so as not to inadvertently violate the areas where the data protection regimes significantly differ.

Comparable to the GDPR, the LGPD is applicable to data processing activities carried out within its jurisdiction, but also has a significant exterritorial effect, reaching foreign organisations that collect personal data of individuals located in Brazil.

Another important highlight is the creation of the Brazilian data protection authority ('ANPD'). The ANPD is the first Brazilian governmental body exclusively dedicated to data protection, and has powers to oversee, issue guidelines on, and enforce data protection laws.

Temer originally vetoed the creation of the ANPD due to a flaw in the legislative process. However, on 28 December 2018, Temer enacted Provisional Measure No. 869 ('the Provisional Measure'), which amended certain provisions of LGPD and finally created the ANPD, which, at the time of publication, is not yet operational.

According to the Provisional Measure, the ANPD will be an administrative body connected to the Cabinet of the Presidency, with technical autonomy, but no financial and budgetary autonomy. The form of the ANDP's creation is raising several discussions regarding the independency of the authority, which is a particular area of importance with regard to Brazil's potential for receiving an adequacy decision from the European Commission ('the Commission').

Finally, the Provisional Measure extended the date that the LGPD will come into force. Now, the deadline for companies to become compliant with the LGPD is August 2020.

Giovanna Bruno Ventre Counsel
giovanna.ventre@mattosfilho.com.br
Mattos Filho Advogados, São Paulo

Uruguay

Since 2012, when it was recognised by the Commission as a country which granted an adequate level of data protection, Uruguay has worked hard to maintain this status, intensifying the Uruguayan data protection authority's ('URCDP') work output and improving its efficiency.

A new scenario

The GDPR's entry into force had an important impact in Uruguay, both to its companies offering their services to European clients, and to its data protection regulations, which had to be updated to keep them aligned with the new European ones.

This was achieved (at least partially), not through a specific new data protection regulation, but by Law No. 19.670 of 15 October 2018 ('Law 19.670'), which includes amendments to Law No. 18.331 on Protection of Personal Data and the Habeas Data Action 2008 ('Law No. 18.331'). Law 19.670 entered into force on 1 January 2019.

Uruguay's alignment

Articles 37 to 40 of Law 19.670 impose significant new obligations on data processors:

Territorial scope of application

Though not strictly imposing new obligations, Article 37 of Law 19.670 amends Law No. 18.331 by clarifying and extending its territorial scope of application to data processing carried out in Uruguay by a processor established in Uruguay.

That said, and mirroring the GDPR, Law No. 18.331 will apply even if the processing is not carried out in Uruguay when:

- the processing is related to the offer of goods or services to individuals located in Uruguay, or with the analysis of their behaviour;
- it is so determined by international laws or a contract; and
- processing is achieved through means located in Uruguay (except when such means are exclusively used for transit purposes and the responsible processor designates a local representative registered with the URCDP).

Security breaches

When a breach of security is detected, this (and the countermeasures adopted) will have to be notified, immediately and in detail, both to the affected data subjects and to the URCDP which, in turn, will inform the Uruguayan Incident Response Centre of Information Security ('CERTuy') and will coordinate actions.

Principle of responsibility

As of 1 January 2019, the individual responsible for a database, or those in charge of that individual, will be responsible for any and all breaches of Law No. 18.331.

Amongst others, and exercising a proactive responsibility, responsible entities must adopt appropriate technical and organisational measures in order to guarantee an adequate level of protections to data that is processed. These include but are not limited to implementing Privacy by Design principles and carrying out Data Protection Impact Assessments ('DPIAs').

Data protection officers

Under Article 40 of Law 19.670, certain entities will be required to appoint a data protection officer ('DPO') whose principal responsibilities include:

- drafting and applying data protection policies;
- supervising the entity's compliance with data privacy regulations;
- proposing measures to ensure compliance with national regulations and international standards; and
- acting as point of contact between the entity and the URCDP.

Entities required to appoint a DPO include public entities, private entities fully or partially owned by the state, and private entities whose business is in the processing of sensitive data or large amounts of personal data.

Future steps for Uruguay

Though Law 19.670 is a good first step for the harmonisation of Uruguay's data privacy regulations with the GDPR, it seems clear that Uruguay will need to enact further regulations to better align itself with European standards. This further harmonisation will probably take the form of a regulatory decree which may appear during 2019.

Guillermo Duarte Abogado
gduarte@bergsteinlaw.com
Bergstein Abogados, Montevideo

Peru

Peru's active legislation has been Law No. 29.733 on the Protection of Personal Data 2011 ('Law No. 29.733') since 3 July 2011, with Supreme Decree No. 003-2013-JUS which Approves the Regulation of Law No. 29733 following in 2013. Whilst Peru's data protection framework is highly influenced by the EU's Data Protection Directive (Directive 95/46/EC) ('the Data Protection Directive'), so far, the GDPR has not ignited any interest from the legislative authorities in terms of passing new legislation to harmonise Peru's laws with GDPR standards.

As GDPR awareness expands beyond the EU, and its impacts on the attraction of foreign investment becomes more apparent, it is likely that the Peru will soon start evaluating the convenience of adjusting to the new standards.

For the time being, regardless of lacking legislative movement, many multinationals in Peru are making efforts to adjust their policies and standards to those of the GDPR, bearing the nuances of local law. For example, some are reviewing their Binding Corporate Rules ('BCRs') to assess whether or not there are requirements that may conflict with local laws, which allows them to reach GDPR compliance whilst avoiding contingencies in light of Peru's existing data protection framework.

Iván Blume Associate
iblume@estudiorodrigo.com
Rodrigo, Elias & Medrano Abogados, Lima

Argentina

Argentina is undoubtedly going through a period of change. A couple of years ago, Argentina started a process of rethinking its current Personal Data Protection Law No. 25.326 of 2000 ('Law No. 25.326'), which has been in force for the last 20 years, inspired by the EU Data Protection Directive and the Spanish Organic Law 3/2018, of 5 December 2018, on the Protection of Personal Data and Guarantee of Digital Rights.

With that in mind, the former Argentinian data protection authority ('PDP') kicked off an open dialogue with the public and private sectors, including practicing lawyers and in-house counsels. This process ended in a draft data protection bill ('the Bill'), which was introduced in Congress in September 2018. In a nutshell, the Bill brings the following main changes:

- it broadens the territorial scope, clearly stating that Law No. 25.326 may apply when the processing of data relating to data subjects residing in Argentina is performed by data controllers not established in the country;
- it includes the obligation to appoint a DPO in the case of public agencies, the processing of sensitive data as a main activity, and big data processing;
- it provides for accountability obligations;
- it includes data breach notification requirements;
- it incorporates significant and expected clarifications regarding the handling of sensitive data; and
- it provides for the mandatory need of DPIAs in certain cases.

At the same time, there have been some important resolutions passed by the former PDP and the current Access to Public Information Agency ('AAIP'), with the aim of facilitating the processing of personal data in commerce while balancing its adequate protection. The most significant changes came in relation to the valid cross-border transfer of data.

An example of that is Rule No. 60-E/2016, which provided a whitelist of countries and jurisdictions that provide an adequate level of protection in terms of international transfers of personal data, and approved two model clauses providing companies with more tools to validly perform cross-border transfers. These standard model clauses were inspired by the EU Model Clauses.

Complementing Rule 60-E/2016, recently the AAIP also passed Resolution No. 159/2018, which brought clear guidelines regarding the use of BCRs for the international transfer of personal data. Resolution 159/2018 was designed to provide a global solution for multinational companies when it comes to privacy. For a very long time, companies were reluctant to rely on BCRs based on the lack of further regulation and clarifications. This is a clear step forward to facilitate cross-border commerce and processing.

Additionally, in December 2018 Congress approved Argentina's accession to Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ('Convention 108'), the world's only international, legally-binding data protection treaty, demonstrating its willingness to be at the forefront of privacy and data protection.

European legislation has always played an important role when regulating data protection locally, and the GDPR is no exception. One of the more tangible effects of this approach that recognises EU legislation is that it facilitated Argentina's becoming the first Latin American country to be recognised by the EU in 2003 as providing an adequate level of protection for the international transfer of data. This recognition, in turn, provided Argentina with certain competitive advantages for business opportunities in the region. With that in mind, Argentina is looking forward to passing the Bill into law with the idea of maintaining its adequacy status, and thus retaining competitive advantages for business opportunities in the region.

Argentina's plans to modernise its current data protection legislation are part of a regional trend to either introduce fresh legislation or modernise existing regulations in Latin America. Particularly in our country, this trend seems to make focus on strengthening data protection, while at the same time fostering commerce.

Diego Fernández Partner
dfer@marval.com
Marval O'Farrell Mairal, Buenos Aires

RELATED CONTENT

NEWS POST
Japan: PPC releases activity policy report

NEWS POST
Liechtenstein: Government adopts report and motion on creation of blockchain act

NEWS POST
Australia: OIAC releases notifiable data breaches report

NEWS POST
UK: Gambling Commission publishes a new version of the LCCP

OPINION
EU: How CNIL fined Google - insights on the One Stop Shop mechanism