ABA Section of International Law
Your Gateway to International Practice

Newsletter Legal Developments in Latin America—July 2018—September 2018
Compiled and edited by the Latin American and Caribbean Law Committee

ARGENTINA

FOREIGN COMPANIES IN ARGENTINA. SIGNIFICANT CHANGES IN REGISTRATION.

BRAZIL

AN OVERVIEW OF THE NEW BRAZILIAN GENERAL DATA PROTECTION LAW.

CHILE

PROGRESS MADE IN THE MPLEMENTATION OF FUNDS PASSPORTS FOR THE PACIFIC ALLIANCE.

A REFORM IS ENACTED FOR THE PURPOSE OF STRENGTHENING THE SERNAC.

AMENDMENTS MADE TO CERTAIN REGULATIONS OF CYBER-SECURITY IN THE FINANCIAL INDUSTRY IN CHILE.

CONTRIBUTING FIRMS: VITALE, MANOFF & FEILBOGEN ABOGADOS (WWW.VMF.COM.AR), MATTOS ENGELBERG ABVOGADOS (WWW.LAWME.COM.BR), CAREY Y CÍA ABOGADOS (WWW.CAREY.CL).

◊ ARGENTINA

FOREIGN COMPANIES IN ARGENTINA. SIGNIFICANT CHANGES IN REGISTRATION.

Foreign companies are especially welcome in Argentina and are fully entitled to set up and own business companies and to participate in any kind of profitable activities.

To conduct business in Argentina on a regular and permanent basis, they may either:
- Establish a branch, or
- Create a local entity or participate in an existing one.

In both cases, the foreign company must be registered with the Public Registry of Commerce.

Since August 30, 2018, the registration of foreign companies has been greatly simplified by the Superintendence of Corporations ("IGJ" for its Spanish acronym), the agency in charge of the Public Registry of Commerce in the City of Buenos Aires.

On August 29, 2018, IGJ General Resolution No. 6/2018, amending IGJ General Resolution No. 7/2015, concerning the requirements that foreign companies must fulfill to be registered to do business in Argentina, was published in the Official Gazette.

These are the most significant changes that simplified registration:

1.- Foreign companies' filing for registration with the IGJ will no longer have to provide evidence of the existence of assets or significant economic activities abroad.
2.- They will no longer have to name their members.
3.- The mandatory annual information regime has been abolished. Foreign companies that are currently registered with the IGJ will not need to submit documents and information on their assets, business activities and members on a yearly basis.

There is an exception based the Fight against Money Laundering and Financing of Terrorism: In the case of companies that are set up or incorporated in jurisdictions not considered as cooperators for the purposes of fiscal transparency, the IGJ will require proof of the existence of significant economic activities abroad, and will strictly evaluate the evidence submitted.

The above-described changes in the registration process are currently in force. Therefore, below is an updated list of documents and information to be filed with the IGJ to be registered as a foreign company to establish a branch (Section 118 of the Companies Law) or to be part of or create a local entity (subsidiary, under Section 123 of the Companies Law) in Argentina:

a.- Bylaws and articles of incorporation, their amendments and any other related document.

b.- Certificate of good standing: issued by the relevant authority stating that the company is duly organized and exists under the laws of its country of origin.

c.- Copy of the Minutes issued by the relevant corporate body approving the decision of the company to be registered in Argentina, appointing a representative and stating that the company is not under liquidation (winding up) and that there is no legal procedure pending restraining the company's assets and/or activities.

Registration in accordance with Section 123 of the Companies Law authorizes the foreign company to create or be part of other companies in any other jurisdiction within Argentina.

The documentation required must be duly authenticated in the country of origin and

must be legalized by the Argentine Consulate or the Ministry of Foreign Affairs. This legalization may be replaced by the Apostille implemented by the Convention de La Haye du 5 octobre 1961.

Contributor: Vanesa Balda, Vitale, Manoff & Feilbogen Abogados, Argentina. For further information, please send an email to vbalda@vmf.com.ar.

◊ BRAZIL

AN OVERVIEW OF THE NEW BRAZILIAN GENERAL DATA PROTECTION LAW.

The recently enacted Law 13,709/2018, the so-called Brazilian General Data Protection Law ("GDPL"), establishes a legal framework for the protection of personal data of citizens, determining how companies, organizations and public authorities should process data in their activities.

The GDPL was published on August 15, 2018 and will enter into force within 18 months after its publication. As the GDPL is highly protective of data subjects and imposes a lot of obligations on data processing agents, they must do their homework during this 18-month period so as to bring their data processing activities into compliance with the law.

The GDPL is an intricate law with many details and nuances which still need to be further detailed by rules that will probably be issued by the National Data Protection Authority ("NDPA") when it is created.

The creation of the NDPA, an independent public entity responsible for the supervision and enforcement of the law and originally contemplated in the initial bill, was vetoed by the Brazilian President on the argument that such authority should be created by the executive branch following certain specific legislative procedures. It is still not clear, though, when this will happen. Thus, data processing agents must be attentive during the next months to further developments on this matter.

So as to be compliant with the GDPL, companies should map their activities that involve the use of personal data, identify the legal basis for the processing of such data, and adopt operational, administrative and technical measures to ensure that the necessary adjustments have been made before the new law enters into force, such as the creation or updating of existing privacy and security policies, terms of use, review of contracts with third parties, among others.

1. SCOPE OF APPLICATION. The GDPL applies to all processing of personal data carried out by public or private entities and individuals, if (i) the data is collected or processed in Brazil; (ii) the purpose of the processing activity is the supply of goods or services to individuals located in the Brazilian territory; or (iii) the processing of personal data relates to individuals located in Brazil.

The GDPL defines as 'processing' any operation involving personal data (for example, collection, reproduction, use, access, distribution, evaluation, storage, transfer, etc.).

The GDPL has an extraterritorial reach and, therefore, it applies even to foreign companies that either (i) have a branch or subsidiary in Brazil; (ii) offer goods or services in the Brazilian market; or (iii) collect personal data from individuals located in the country.

2. DATA COVERED BY GDPL. Generally speaking, the GDPL covers any data that may allow the identification of a natural person, such as name, e-mail, age, marital status, address and financial situation, obtained in any format (paper, electronic, computer, sound, image or other), isolated or aggregated to another.

The law defines and provides for specific treatment for (i) **personal data**: any

information related to an identified or identifiable individual; (ii) **sensitive data**: personal data regarding racial or ethnic origin; religious beliefs; political opinions; membership of syndicates or religious, philosophical or political organizations membership; data relating to health or sexual life; and genetic or biometric data when linked to a natural person.

Personal data may also be considered any data used to develop the behavioral profile of a natural person, if identified.

Anonymized data (data which has lost the possibility of being associated to an individual) is outside the scope of application of the law, except if the anonymization process may be reversed.

3. GDPL PRINCIPLES. The GDPL sets out ten principles that must be strictly followed by all who intend to process personal data:

- Purpose limitation: all processing must be for legitimate, specific and explicit purposes duly disclosed to data subjects.
- Adequacy: compatibility of the data processing with the purposes informed to the data subject.
- Necessity: limits the processing of data to what is strictly necessary to achieve the purpose for which the data is being processed.
- Free access: guarantee, to the data subjects, of free and facilitated consultation on the form and duration of the processing.
- Data quality: provides for the accuracy, clarity, relevance and updating of the personal data.
- Transparency: guarantee, to the data subjects, of clear, precise and easily accessible information on the data processing.
- Security: adoption of technical and administrative measures to protect personal data from unauthorized access and accidental or illegal destruction, loss, alteration, communication or dissemination.
- Prevention: adoption of measures to prevent the occurrence of damages due to personal data processing.
- Non-discrimination: impossibility of data processing for unlawful or abusive discriminatory purposes.
- Accountability: adoption of effective measures capable of proving compliance with personal data protection rules.

4. LEGAL BASES FOR DATA PROCESSING. The GDPL establishes that data processing is allowed in ten cases:

- Upon consent of the data subject.
- Compliance with legal or regulatory obligations by the controller.
- Fulfillment of public policies by the public administration.
- Performance of studies by research entities.
- Performance of contract or of preliminary procedures related to a contract to which the data subject is a party.
- Regular exercise of rights in judicial, administrative or arbitration proceedings.
- Protection of data subject or third parties' life or physical safety.
- Protection of the data-subject's health, involving procedures performed by health professionals or healthcare entities.
- Legitimate interests of the controller or a third party.
- Credit protection, under the terms of the applicable legislation.

With regard to consent, it must be free, informed and unambiguous and must be provided in writing or by any other means that can demonstrate the will of data subject. Data subjects may revoke consent at any time.

5. SENSITIVE DATA. In comparison with the legal bases for processing personal data, there are more stringent provisions for the processing of sensitive data. Consent from data subject is mandatory, but the GDPL provides that consent is dismissed in some specific cases, such as, among others (i) for compliance with legal or regulatory obligation by the controller; (ii) for conducting studies by research entities; (iii) for protecting data subject or a third party's life; (iv) for ensuring prevention of fraud and safety of the data subject in the process of

identification and authentication of registration in electronic systems.

It is worth mentioning that communication or shared use of health-related sensitive personal data among controllers aimed at obtaining economic advantage is expressly prohibited, except in cases of data portability, when consented to by the data subject.

6. RIGHTS OF DATA SUBJECTS. Data subjects should have their rights guaranteed by data agents in an accessible and effective manner. Among data subject's rights, the most relevant are (i) confirmation regarding existence of data processing; (ii) access to data; (iii) correction of incomplete, inaccurate and outdated data; (iv) anonymization, blocking or elimination of unnecessary data; (v) data portability, which allows the data subject not only to request an entire copy of their data, but also to have such data provided in an interoperable format, which aims at facilitating its transfer to other services, even for competitors; (vi) withdrawal of consent; (vii) review, by a natural person, of decisions taken solely on the basis of automated processing of personal data affecting his or her interests.

When the processing of personal data is a condition for the provision of products or services - such as in cases of contracts of adhesion -, the data subject must be informed in detail about this fact and about how he or she can exercise his or her rights.

7. DATA AGENTS. We have summarized below certain obligations imposed by the GDPL that must be complied with by legal entities and individuals involved in data processing:

- **Data controllers** are responsible for making decisions regarding data processing; providing instructions to data processor; keeping records of data processing operations; appointing a data protection officer; preparing the data protection impact assessment report, if so required by the NDPA; communicating to the NDPA and data subject any security breaches which could lead to significant risk or damage.
- Data processors are responsible for carrying out data processing according to controller's instructions; keeping records of data processing operations.
- Data Protection Officer (encarregado) is the individual appointed by the controller, who is mostly responsible for being the communication channel between the controller and data subjects, the NDPA, employees and contracted parties.

8. LIABILITY. In principle, processor may be held jointly liable with controller for damages caused by breach of obligations set forth in the law or when he or she has not followed controller's lawful instructions. Controllers may also be held jointly liable whenever they are directly involved in data processing from which damages to data subject arise.

Nonetheless, the GDPL has established few exceptions to agents' liability, such as when the agents could prove that they have not performed any data processing activity; or even if they have performed such data processing activity, that it has not been done in violation of the law or, finally, when the damage arises from data subject or third party's fault.

9. PRIVACY BY DESIGN AND PRIVACY BY DEFAULT. The GDPL makes it compulsory to implement privacy and personal data protection measures as part of the creation of new services, products and business models. General principles and safety standards must therefore be observed from design to execution and offering of products and services.

10. CROSS-BORDER TRANSFERS. The GDPL also created specific rules on international data transfers, allowing it only in certain cases, such as:

- To countries or international organizations deemed by the data protection authority to provide an adequate level of data protection;
- When there is a guarantee, by the controller through contractual instruments,

that it will comply with the principles, rights and the data protection regime provided by law;
• For international legal cooperation between government agencies; or
• Based on the specific and express consent of the data subject.

The NDPA (still to be created) will assess the level of data protection of the foreign country or of the international organization.

11. PENALTIES. Non-compliance with the GDPL's requirements can result in administrative penalties, such as warnings, publication of the violation, blocking or deletion of data and fines of up to 2% of the sales of the company or group of companies in Brazil, in the last fiscal year, limited to BRL 50,000,000 per infringement. There is also the possibility of a daily fine to compel the entity to cease violation. The fine is calculated based on Brazilian revenue only, not global revenue.

Contributor: Cristiane Borges da Costa and Renata Montenegro, Mattos Engelberg Abvogados, Brazil. For further information, please send an email to contato@mattosengelberg.com.br.

◊ CHILE

PROGRESS MADE IN THE IMPLEMENTATION OF FUNDS PASSPORT FOR THE PACIFIC ALLIANCE.

On July 30, 2018, the Chilean Commission for the Financial Market (Comisión para el Mercado Financiero or "CMF") issued ruling No. 3092 (Resolución Exenta 3092), expanding the list of foreign securities exempted from registration requirements before the Registry of Foreign Securities (Registro de Valores Extranjeros) of the CMF (the "RE 3092").

Previously, under ruling No. 246 (Resolución Exenta 246) of 2014, an exemption from registration was granted in favor of the securities of issuers considered as "reporting issuers" under Canadian law, as well as the securities registered before the National Registry of Securities and Issuers of Colombia (Registro Nacional de Valores y Emisores de Colombia), the National Registry of Securities of Mexico (Registro Nacional de Valores de México), and the Public Registry of the Securities Market of Peru (Registro Público del Mercado de Valores de Perú).

In an effort to boost the implementation of the Funds Passport for the Pacific Alliance (made up of Colombia, Mexico, Peru and Chile), pursuant to RE 3092 the funds or families of collective investment funds authorized by the Financial Superintendence of Colombia (fondos o familias de fondos de inversion colectiva autorizados por la Superintendencia Financiera de Colombia) were included in the list of foreign issuers that are exempted from registration requirements before the CMF.

In line with the previous initiative, recently the Peruvian authority on securities markets (Superintendencia del Mercado de Valores), approved the so-called "Regulation for the Recognition of Foreign Funds" (Reglamento para el Reconocimiento de Fondos del Exterior) and authorized the marketing of Colombian, Chilean and Mexican funds in the Peruvian securities market. Additionally, the Financial Superintendence of Colombia (local authority on securities markets), following the same path, issued a ruling with instructions on the placement of foreign funds, including Chilean funds, in Colombia.

With these changes, progress is being made in the collaboration between the members of the Pacific Alliance for the commercialization of funds facilitating investors' access to this type of securities.

Contributors: Cristián Eyzaguirre, Francisco Guzmán and Carlos Alcalde, Carey y Cía. Ltda., Chile. For further information, please send an e-mail to ceyzaguirre@carey.cl, fguzman@carey.cl or calcaldea@carey.cl.

A REFORM IS ENACTED FOR THE PURPOSE OF STRENGTHENING THE SERNAC.

On September 13, 2018, a significant modification to the Consumer Protection Act No. 19,496 ("CPA") was enacted through Law No. 21,081 (the "Amendment").

This Amendment includes several adjustments that provide the National Consumer Service (Servicio Nacional del Consumidor or "SERNAC", as per the initials in Spanish) with more modern, expeditious and efficient tools to supervise, regulate and sanction violations of consumers' rights.

The main modifications introduced by the Amendment are the following:

(i) Further powers conferred to SERNAC to supervise compliance with and interpret the CPA and to propose new regulations;
(ii) Implementation of a substantial increase in the applicable fines in case of violations of the CPA provisions and a new system to determine the amount of the fines (penalty rating);
(iii) New benefits granted to small businesses in case of violations of the CPA;
(iv) Extension of the statute of limitations from six months to two years, since the moment the violation has ceased;
(v) Direct and automatic redress for consumers in the event of suspension, discontinuance or unjustified lack of provision of contracted basic services;
(vi) Prohibition of "tied selling" in telecommunication services;
(vii) Strengthening of consumer associations;
(viii) Introduction of a new criterion to determine competent jurisdiction of Local Courts on individual proceedings; and
(ix) Improvement of class actions, which now include injunctive measures and the right of consumers to request payment of collective moral damages –the court will determine a common minimum amount as compensation; the aggrieved party may apply for a higher compensation, in excess of such common minimum amount, by instituting a separate legal proceeding. Furthermore, the Amendment provides that the court will be vested with the authority to increase the amount of the compensation by 25% in the event any aggravating circumstances exist.

As concerns the imposition of fines, the Amendment provides that the courts may impose one fine per each consumer aggrieved, provided it is allowed by the nature of the infringement, with the following limitations: the fine cannot exceed, in the aggregate: (i) 30% of the sales of the product and/or service that is the subject-matter of the infringement, during the period in which the infringement occurred, or (ii) twice the economic profits earned as a result of the infringement, as determined by the court. The Amendment also provides that, for class actions, the imposition of fines is limited to a maximum global amount of 45,000 UTA (USD 37,5 million app.)

The Amendment will enter into force progressively, depending on the provision and the region of the country in which it is implemented.

Contributors: Cristina Busquets and Kureusa Hara, Carey y Cía. Ltda., Chile. For further information, please send an e-mail to cbusquets@carey.cl orkhara@carey.cl.

AMENDMENTS MADE TO CERTAIN REGULATIONS OF CYBER-SECURITY IN THE FINANCIAL INDUSTRY IN CHILE.

On August 31, 2018, the Superintendence of Bank and Financial Institutions ("SBIF") modified Chapters No. 20-8 and 1-13 of the SBIF's Updated Compilation of Regulations (Recopilación Actualizada de Normas- "RAN").

These amendments intended to establish the cyber-security rules applicable to the Chilean financial institutions after certain cyber-attacks suffered by this industry early this year.

The main amendments introduced by the SBIF to these chapters are the following:

I. Chapter 20-8 on Information of

operational incidents:

The modification of Chapter 20-8 of the RAN involves:

(a)Communication of operational incidents to SBIF.

A strengthening of the current obligation of banks and financial institutions to report incidents to SBIF, specifying the types of operational incidents that must be communicated and detailing opportunity, contents and communication procedures.

(b) Communication of incidents to clients or users.

An obligation to report certain types of incidents to the clients of the affected institutions, specifying the type of incident and detailing opportunity, contents and communication procedures.

(c) Communication of incidents to the banking industry.

The banks must report certain kinds of incidents to other agents of the bank industry. The purpose of this measure is to warn the industry about cyber-security threats and reducing the chances of negative impacts spreading across the national financial system.

(d)The elimination of current section No. 2 which regulated the obligation to maintain a database of cyber-security incidents.

In this regard, under Circular No. 3,640 of the SBIF dated August 31, 2018, the elements evaluated in the scope of operational risk are now incorporated into Chapter 1-13 of the RAN. On the other hand, the minimum variables to be considered in the implementation of an incident database will now be part of a file in the Information System Manual.

II. Chapter 1-13 on Classification of management and solvency.

The main amendment to this chapter is the incorporation of a new obligation for financial institutions that must keep a database of cyber-security, including the fields requested in the file of SBIF´ Information System Manual. This procedure will be regarded as evidence of good risk management.

Contributors: Paulina Silva and Carlo Benussi, Carey y Cía. Ltda., Chile. For further information, please send an e-mail to psilva@carey.cl orcbenussi@carey.cl.