Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cyber Security

Argentina
Richards, Cardinal, Tützer, Zabala & Zaefferer

chambersandpartners.com

2019

ARGENTINA

The 'Law & Practice' sections provide easily accessible information on navigating the legal system when conducting business in the jurisdiction. Leading lawyers explain local law and practice at key transactional stages and for crucial aspects of doing business.

Law and Practice

Contributed by Richards, Cardinal, Tützer, Zabala & Zaefferer

CONTENTS

Richards, Cardinal, Tützer, Zabala & Zaefferer data protection team is led by Juan Pablo M Cardinal and Lisandro Frene (partners), plus three senior lawyers, two junior lawyers and two paralegals. The team works closely with other teams within the firm in other data protection-related areas, such as TMT, IP, Compliance, Administrative - Regulatory and Corporate areas of the firm. Areas of specialisation include: database registration, audits carried out by the Data Protection Agency, data outsourcing agreements. International data transfers, cloud computing services agreement (drafting and negotiation), data protection regulation in the provision of telecommunications, OTT and IT services, data protection clauses in internal policies and compliance manuals, data protection and advertising: applicable formats and mandatory legal texts, data protection analysis for particular industries such as financial, health and agribusiness, legal review of big data applications from data protection law perspective, mandatory security and technical requirements for data hosting and processing, data security incidents management and data protection assessment in contracts with public sector.

Authors

Lisandro Frene is a partner and head of the data protection department. He also co-heads the IT department. He has published widely in industry publications, is a professor at the Universidad Austral and a data lecturer at the IAE Business School. He is also a member of the International Association of Privacy Professionals.

Juan Pablo M. Cardinal heads the TMT practice and co-heads the IT department. His practice covers TMT, IP, IT, data protection and cloud. He is a regular asistant to the IBA Technology Committee.

1. Basic National Legal Regime

1.1 Laws

Privacy and data protection are expressly acknowledged by the Argentine Constitution (including privacy and 'habeas data' Sections 19 and 43); several International Treaties executed by Argentina (with legal hierarchy superior to domestic laws); the Argentine National Civil and Commercial Code (Section 1770) and more specifically by Argentine Data Protection Act No 25,326 (PDPA); of 'public order'; and more than 60 regulations thereof derived. In broad terms, the Argentine data protection system follows the European legal regime in this matter.

Personal Data is defined in PDPA as "information of any kind referred to identified and/or identifiable individuals and/or entities." It is a very broad definition which encompasses almost any sort of information linked to a subject. In turn, data "treatment" is also widely defined as "the systematic operations or procedures, by electronic means or others, allowing storage, conservations, modifications, relationship, evaluation, lock, destruction and in general data processing of personal data, as well as assignment to third parties through communications, interconnections or transfer."

As the main data protection general principle, Argentine law requires a data subject's prior consent for any kind of data treatment (consent principle). Additionally, pursuant to the purpose principle established by PDPA, data obtained for a certain purpose cannot be used for a different one (for the latter, a new consent from a data owner would be needed).

1.2 Regulators

The Argentine data protection regulator in charge of enforcing the PDPA is the Argentine Agency of Access to Public Information (AAPI) – which pursuant to recent Decrees 746/2017 and 899/2017 – replaced the former Argentine Data Protection Authority as the PDPA enforcement authority.

AAPI is entitled to perform PDPA compliance audits. Audits are performed with a non-aggressive approach and – due to operational restrictions – only in the city of Buenos Aires and punctual cities of Buenos Aires Province (almost never in other provinces of Argentina).

Although AAPI, as the PDPA enforcement authority, may initiate ex parte investigations this rarely happens in practice and most administrative investigations are filed after a party's claim alleging a PDPA infringement.

In addition to the AAPI authority, specific regulators apply for sectoral industries, such as the Argentine Central Bank for data handled by financial institutions.

In 2017, two new regulators were created by presidential Decrees: the Big Data Observatory, an entity within the IT & Communications Bureau which aims to "study the regu-

latory framework of personal data use;" "foster and create Big Data technological platforms," and "propose new data regulations;" and the Cybersecurity Committee, within the Modernisation Ministry, in charge of "drafting and developing the National Cybersecurity Strategy," setting framework guidelines and rules for such a purpose. The specific tasks and scope of these two latter regulators have yet to be defined by rules that are still to be issued.

1.3 Administration Process

The administrative process that AAPI must follow to investigate and impose penalties is established in Sections 31 and 32 of PDPA, in Decree 1558/2001 and Decree 1160/2010.

If, after an administrative claim filed before the AAPI by anyone with a legitimate interest or an ex parte preliminary investigation filed by the AAPI, it considers there could be a possible infringement to PDPA, it should communicate so to the potential infringer, who has ten working days – which may be extended - to file its defence.

The AAPI may discretionally decide whether to receive evidence or not and then issue an administrative decision stating whether there has been a PDPA infringement; and in the former case imposing a fine for such infringement. Economic fines are currently relatively low, and may vary from ARS1,000 (circa USD55) to ARS100,000 (USD5,500).

After being notified, the infringer may file appeal remedy to such a decision, which is then analysed by judicial courts, pursuant to the regular process set forth in the Administrative Proceedings Regulation.

1.4 Multilateral and Subnational Issues

The Argentine data protection system is based on the EU system. Basic data privacy concepts are derived from EU Directive 95/46. Indeed, PDPA was taken from Spanish data protection law; and a current bill to amend the PDPA intends it to be aligned with EU general data protection regulations (GDPR).

PDPA is a law "of public order" (which means it cannot be waived by the parties of an agreement) and applicable at a federal level in the entire Argentine territory.

Although AAPI is very limited outside of Buenos Aires province; there has been judicial controversies involving personal data all throughout Argentina, particularly habeas data summary proceeding (claims from data subjects invoking the right to access, delete or update his or her data). The procedural rules of habeas data may vary from one province to the other, always respecting PDPA principles.

1.5 Major NGOs and Self-Regulatory Organisations

In Argentina there are few non-governmental organisations (NGOs) exclusively dedicated to data protection matters; and their influence is relatively low. Some of the NGOs that analyse and promote interests somehow related to privacy are the following:

- Asociación por los Derechos Civiles (Civil Rights Association) is an NGO that promotes social and civil rights in Argentina as well as in other Latin-American countries. Within this NGO there is an area called "ADC Digital" that serves as a forum for debate and critical analysis of the policies carried out by public and private actors, including topics such as big data, cybersecurity, data protection etc.
- Grooming Argentina is an NGO with awareness workshops that intends to eradicate grooming (sexual harassment through the internet).
- Argentina Cibersegura (Argentina Cyber Secure) is an NGO which develops awareness materials with the aim of promoting communication and knowledge about the personal risks derived from the use of the internet, privacy, cyber bullying, grooming, sexting etc.
- CABASE (Argentina Internet Chamber) is an NGO that looks to represent its associates' interests on the development of the internet through Argentina, and participate in the drafting of regulatory frameworks thereto related (ie such as ISPs liability bill, bill to amend the current data protection law entirely etc).

1.6 System Characteristics

Argentina was the first Latin American country to have a data protection law, in 2000, following the EU model. Indeed, PDPA was taken from Spanish data protection laws and the EU has expressly acknowledged that Argentina has "adequate data protection."

Although Argentina is still more advanced than other Latin American countries in data protection matters, its regime is much less developed than the EU one. After its enactment in 2000, technological advancements have neither been properly regulated in PDPA amendments nor addressed in AAPI regulations.

Despite a solid data protection regime, PDPA enforcement has so far been scarce in practice. AAPI fines for PDPA infringement have been few and for low amounts. Furthermore, PDPA compliance audits are performed by AAPI with a non-aggressive approach.

Recent administrative changes in the PDPA enforcement authority (the AAPI), together with legislative changes expected – particularly in the IT and telecommunications sector - may lead to a different scenario in 2018.

1.7 Key Developments

In June 2017, Regulation 11/2017 created the Big Data Observatory, an entity within the IT & Communications Bureau. Although its specific tasks are yet to be defined by further regulation, it aims to "study the regulatory framework of personal data use;" "foster and create Big Data technological platforms," "promote good Big Data practices" and "proposal for new regulations."

On 3 November 2017 the Argentina Central Bank issued Communication A 6354 which sets forth specific requirements for financial institutions intending to perform data outsourcing services, data processing and IT services.

On 6 November 2017 it was issued presidential Decree 899/2017 which – pursuant to previous Decree 746/2017 - establishes that the new AAPI shall be the enforcement authority of the PDPA, thus replacing the former Argentine Data Protection Authority (Dirección Nacional de Protección de Datos Personales) in such a capacity. The AAPI is a public autarchic entity recently created by Decree 746/2017 within the National Chief of Cabinet (the highest authority of the National Government Ministries).

Finally, in November 2017, Congress approved an Act which ratifies the Argentine accession to the Budapest Convention on Cybercrime. Such a law will have a substantial impact in Argentinian criminal law related to data cybercrime as it establishes cyber-security concepts and standards that members (in this case Argentina) shall implement through their criminal domestic legislation to be operative.

1.8 Significant Pending Changes, Hot Topics and Issues

There is currently a bill issued by the AAPI that intends to amend the PDPA entirely and which is expected to be discussed in Congress in 2018. The bill aims to cover topics not regulated by the current PDPA (ie such as data security incidents) and be aligned with EU GDPR.

AAPI also intends to update specific technical and security measures for data storage and data treatment (the current measures were set forth in 2006). In this matter, the recently created Cybersecurity Committee is also expected to draft cyber-security strategies and guidelines setting framework rules for that aim, either for the public sector, private sector or both.

Another bill already in Congress – likely to be enacted soon - related to data protection, is intended to regulate ISP liability.

In addition, several regulations to Act 27,078 (Information Technologies & Communications Act, IT&C Act, also known as the Digital Argentina Act) are expected to be issued in 2018, and are likely to have a direct impact on data processing for telecommunication providers.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Personal data protection is acknowledged in the Constitution; in the Argentine National Civil and Commercial Code (Section 1770); and regulated at a federal level by PDPA and more than 60 regulations issued by AAPI.

Other more specific data protection-related laws and sectoral regulations are also applicable, such as regulations about the right to the own image and voice (Act 11,723, Section 31; and Argentine Civil and Commercial Code, Section 53); right to intimacy (Argentine Civil and Commercial Code, Section 52); health data and consent for medical treatment (Argentine Civil and Commercial Code, Section 52); and Medical Records and Patient's Right Act 25,629, as amended by Act 26,742; financial entities' data treatment (Argentina Central Bank issued Communication A 6354) etc.

PDPA is mandatory and applicable to data treatment of Argentine residents, regardless of where such treatment is performed. PDPA rights cannot be waived by data subjects, as it is considered a public order law.

A data subject's consent is one of the key principles of PDPA. Furthermore, a data subject's right to access data and right to correct or expunge data has been a constitutional right since 1994, and the proceeding to exercise such rights is incorporated to PDPA.

As one of the exceptions to the consent principle, PDPA allows the free use of data (ie no consent required) when it is anonymous or de-identified.

Companies handling databases need to adopt internal privacy policies in compliance with PDPA, which AAPI may control in the audits it performs.

As the PDPA was enacted in 2000 concepts like "privacy by design" or "by default"; "data protection officers" or privacy impact analysis" are neither incorporated into the PDPA nor included in latter regulations. However, there is a current bill drafted by the AAPI intending to amend PDPA integrally – still to be discussed by Congress - which expressly addresses the aforementioned matters.

2.2 Sectoral Issues

Sectoral Issues - Special Categories of Data

Sensitive data is defined by the PDPA as data revealing religious, sexual, political, racial, ethnical, moral or philosophical preferences, as well as health data and criminal records.

As a general principle, sensitive data collection, processing and/or treatment is forbidden unless expressly established by law.

As it is classed as sensitive data, health data can only be treated by health professionals and health facilities/establishments (ie private and public hospitals) - in accordance with the Medical Records and Patient's Right Act 25,629 (Section 5), as amended by Act 26,742 and other applicable laws - respecting professional secret principles.

Regarding data security, PDPA and its Regulation AAPI No 11/2006 specifies the mandatory security measures for personal data storage and/or treatment. Such Regulation establishes three different security levels according to the nature of the personal data stored in the databases. Every security level lists certain security measures that must be adopted by each data controller. The highest security requirements (critical security measures) apply for health and sensitive data.

As a general principle stated above, any treatment of criminal records – also considered sensitive data - is forbidden for any private entities, as stated in PDPA and several AAAPI opinions. In other words, the collection, storage and/or assignment of criminal records (and/or of any type of sensitive information) is primarily forbidden by PDPA, unless there is an express legal requirement/allowance to do so.

Without prejudice of the aforementioned legal prohibition, in 2015 the AAPI construed – in an isolated opinion - that an employer may treat employees' criminal records' certificates and/or criminal record information as if such certificates shows that those employees have no criminal records at all.

Credit information data and data related to the fulfilment of economic content obligations can be treated without a data subject's consent, as it is expressly allowed in PDPA. In addition, personal data treated by financial institutions shall be managed in accordance with the specific regulations issued by the Argentine Central Bank (see 'infra', "International Considerations" and "Cybersecurity).

Communications Data
Save for the case of use of data for marketing and advertising purposes (please see below), the use of data through specific media such as telephones, the internet, TV, social media etc, is not specifically addressed in PDPA. Thus, general PDPA provisions are applicable in addition to the regulatory framework of each particular media.

For internet websites, privacy policies and express user-consent pursuant to a mandatory legal text (applicable also for data collection through other media) is required. However, the use of cookies, beacons or tracking technology, for instance, has never been regulated in Argentina nor particularly addressed in any AAPI opinions.

Furthermore, in spite of several bills on the matter, there is no legislation whatsoever regarding the liability of ISPs or Content Service Providers. While the right of access and deletion of incorrect data is addressed in PDPA, there are neither takedown nor counter notice/respond legal proceedings. This question - closely related to data protection rights - is currently de facto regulated pursuant to case-law precedents. During recent years, hundreds of cases have been brought to the courts against search engines and/or social media providers where plaintiffs have requested their data be erased/blocked due to 'porn revenge,' disinformation, hate speech, slander, non-authorised use of images, privacy etc. Although – in the absence of legislation - each controversy is decided on a case-by-case basis, according to Federal Supreme Court guidelines, petitioners need to indicate the specific URLs or information to be blocked.

The right to be forgotten is only expressly regulated by PDPA in relation to credit information data and has been implemented – upon a data subject's request - against banks and financial institutions (which shall delete credit information data after certain periods of time established by applicable regulations).

Children's Privacy
The PDPA has no particular provision related to minors' personal data, age for consent and/or parental disclosure; those issues shall be analysed under the general regulations of the National Civil and Commercial Code, enacted in August 2015. As a general principle, consent of a person under 18 years old shall be performed by his or her parents or representatives. However, the aforementioned Code expressly acknowledges valid consent of persons of 13 years or older (legally called adolescents) for certain specific acts. Furthermore, from 16 years onwards adolescents are considered adults for all decisions related to caring for their own body.

Educational or school data is not considered by PDPA as a special category of data, nor is it considered to be sensitive data. Thus general principles of personal data stated in PDPA apply to them.

2.3 Online Marketing
The use of data for marketing purposes is controversial in Argentina as this particular subject-matter is contradictory at present under Argentinean law.

While PDPA establishes an opt-in requirement, even when data is collected for marketing purposes (Sections 5 and 27), Decree 1558/01, which regulates PDPA, establishes that when data is collected for marketing purposes only, opt-out is allowed (ie no consent of a data owner would be required).

Some doctrines find this Decree unconstitutional on this point, as it contradicts PDPA. Other AAPI regulations (Reg 4/09) indirectly allows opt-out consent.

As a general approach, although the risk of an opt-out consent is reasonably medium/low, for a conservative risk-free system an opt-in consent would be advisable.

In addition, specific legal regulations should be considered depending on the type of marketing communications:

In telemarketing telephone calls or texts, for instance, the opt out system applies. Thus, no data-subject consent is needed to make such calls, unless the data subject is registered on the Do Not Call Registry, which telemarketing companies check on a monthly basis.

In spam e-mail, certain legal legends in the e-mail, in the Spanish language, are mandatory.

As well as this, another specific mandatory text is applicable in any form – submitted through e-mail or any other media - in which users shall fill their data, in order to ensure an adequate subject's consent pursuant to Argentine law.

The aforementioned regulations are applicable in all cases of marketing addressed to Argentine residents, irrespective of the country or jurisdiction from where the e-mail, phone call or text are submitted.

Any use of sensitive data for advertising purposes is forbidden, unless it is anonymous or de-identified.

2.4 Workplace Privacy

Workplace privacy has been an increasingly hot topic in recent years in Argentina, mainly due to the advancement of technologies and its impact on data protection. According to Argentine Employment Contract Law 20,744, an employer has the power to perform personal control of employees within certain limits to safeguard the workers' dignity and privacy (Sections 65, 70, 71 and 72). Such standards are not precisely defined and are analysed by the courts on a case-by-case basis, aligned with the rest of the labour legislation (which is very protective of an employee's rights) and with PDPA principles.

As a general rule, employees shall give their prior consent (preferably in writing) acknowledging that their data may be collected by an employer by way of monitoring their workplace communications. In practice, this is typically performed through an employer's privacy policy that (sometimes together with other policies and/or conduct guidelines) an employee signs when starting a job.

Regarding workplace video surveillance in particular, case law has established that a company must notify where cameras are located, what type of models they are, and whether they can record audio or not (it has been decided that sound or voice recording is much more intrusive and therefore has greater complications when it is used as evidence in court). Video cameras cannot be located in places that disturb an employee's privacy and/or intimacy and/or psychological integrity. Argentine labour courts consistently reject certain video recorded evidence in cases where the cameras were located in restrooms and/or places where a worker's privacy and intimacy is expected.

In addition, video surveillance is considered a data collection proceeding specifically regulated by AAPI (Regulation 10/2015). Apart from registering the video surveillance database before the National Databases Registry, as well as any other database (ie customers, employees etc), companies doing video surveillance shall have a privacy handbook containing certain mandatory information such as references to places, dates and hours in which surveillance cameras will operate; the term during which data shall be stored; security and confidentiality mechanisms; measures to grant a data owners' basic rights (block, delete, update and/or correct personal data); and reasons that justify the taking of photographs and/or video surveillance.

The collection of images in the aforementioned way shall be limited to the security reasons alleged; without interfering with privacy and/or intimacy of data owners. Letters shall be exhibited to the public/workers expressly indicating: the existence of video cameras; the purpose of video surveillance; the company responsible for the images/data treatment; its domicile; and the way in which data subjects may contact such company to exercise their basic rights.

Whistle-blower hotlines and anonymous reporting are often used by companies as part of their internal policies and/or compliance programmes for employees; still, they are not legally regulated.

2.5 Enforcement and Litigation

Despite its strict terms, the level of PDPA enforcement is fairly low in Argentina. PDPA sanctions are scarce, the amount of the few fines imposed are very low; and relatively few judicial decision granting damages for PDPA infringement are issued.

Although AAPI, as PDPA enforcement authority, may initiate ex parte investigations, this rarely happens in practice and most administrative investigations are filed after a party's claim alleging a PDPA infringement.

The AAPI has discretion to determine whether there has been a potential privacy infringement, always based on

PDPA principles. AAPI has so far had a friendly non-aggressive approach, and the fines imposed have almost always been modest. Indeed, during the last 12 months, fines imposed by AAPI almost never exceeded ARS60,000 (circa USD3,300).

This scenario might change if the bill intending to amend and replace PDPA is enacted (ie, this bill establishes more severe fines and sanctions). However, this still has not happened.

Legal actions for the infringement of data protection laws may be brought directly to court. In practice, the majority of these judicial claims are ones called habeas data claims, expressly provided for in PDPA, pursuant to which a plaintiff intends to have access to his or her data; or to have his or her data updated, modified or suppressed.

In turn, many of these habeas data claims are filed against search engine providers. Case law varies on a case-by-case basis (depending, inter alia, on the sort of data intended to be erased by a plaintiff), and many judicial decisions have considered that habeas data proceedings are not an appropriate procedural remedy against search engine providers, as they are not considered database owners.

Data protection laws are also invoked in claims against ISPs in other kinds of judicial proceedings, such as injunctions or claims for damages, particularly against search engine providers and social media providers. Without specific legislation about ISP liability, judgments are issued on a case-by-case basis based on general principles of tort law, guided by two landmark decisions issued by the Federal Supreme Court in 2014 (Belen Rodriguez v Google) and in 2017 (Gimbutas v Google). In these cases, it was decided that a search engine's liability shall be analysed under the negligence system (as opposed to strict liability); and, more punctually, that for the deletion of data from search results, a plaintiff needs to individualise the specific URLs.

Class actions are not set forth by data protection law, but they can be filed pursuant to the requirements of general rules for such actions (Consumers Protection Law, National Civil and Commercial Code, Reg. SC 90/2016 and Fed Supreme Court Reg 32/2014) and the guidelines stated by case law, mainly the Federal Supreme Court. However, they are much more often in the consumer law area than in data-protection matters.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for National Security Purposes

As a general principle, a valid court order shall be issued to authorise governmental access to data. Act 25,520 establishes in Section 5 that: "E-mail, telephone, fax or any other sort of communications as well as any other system to transfer voice, images and/or data; and any other private databases, registry, letters and/or information confidential and/or without public access, shall remain sealed and non-accessible save for judicial order". This previous judicial order requirement is applicable to the National Intelligence Agency and to any other kind of administrative and/or governmental entity. Typically, a court order presented to a database owner should include the following information:

- case name;
- name of court/authority who requests the information;
- a transcript of the court's decision that requests the information; and
- information requested.

Such a scenario would be feasible in criminal cases as a 'final resource' to procure evidence. Courts usually request the information through a formal request first and, in the case of non-compliance, a court might resort to this action.

Judicial access to data may also be ordered in civil and commercial litigation, as part of injunctions and/or discovery proceedings, with certain restrictions regarding the rights of third parties.

Court decisions ordering the disclosure of information and/or the submission of personal data can be contested through procedural remedies like an appeal and/or or revision of the court order by the same judge. As a general principle (particularly in cases of injunctions or preliminary measures), said remedies do not suspend the validity and terms set forth by such court orders. In addition, if disclosure of documents is requested by a court order within the evidentiary stage (ie civil discovery) the third party in possession of the information or documents to be disclosed may file an opposition to such disclosure alleging that the data/documents belong to him or her – if that is the case - and that its exhibition may cause him or her damages.

On an administrative level, Act 27,078 (IT&C Act), applicable only to entities considered "Telecommunications Services Provider" under such law, establishes in its Section 62.h that IT&C services provider "shall allow the IT&C controlling authority to access their facilities and provide the information requested by such authority". The IT&C controlling entity is currently the ENACOM. Pursuant to a reasonable

interpretation, this ENACOM's legal right should not be used to intercept communications or obtain a stored user's data without a previous judicial order.

Furthermore, under PDPA, the AAPI has jurisdiction to enforce certain auditing rights over servers located in Argentina for the sole purpose of verifying compliance with PDPA security measures, without accessing the data.

3.2 Key Privacy Issues, Conflicts and Public Debates

A recent concern about governmental access to personal data arose in November 2017, when the former Data Protection Agency merged with the AAPI into one same entity, as this merger might trigger conflicts of interest when individuals decide to enforce their data protection rights against the state. Furthermore, the purpose of both governmental entities (now merged into one, the AAPI) seems to be quite different. Despite these objections, and with the merger being so recent, the aforementioned concerns are, so far, more theoretical than practical.

4. International Considerations

4.1 Restrictions on International Data Issues

Argentine data protection law expressly regulates international data transfers (AAPI Regulation 60/2016), allowing it if the requirements set forth by Argentine law for such purpose are met. Said requirements vary, essentially according to the purpose of the data transfer; and to the country where data is exported. Provided said requirements (which are hereinafter explained) are met, no notification, permission or approval from the AAPI or any other authority is legally needed.

4.2 Mechanisms That Apply to International Data Transfers

As a general principle, PDPA requires a data subject's express consent for any sort of data assignment, including international data transfer. Assuming the personal data was legally collected, an exception to the consent requested for data assignment takes place when data is exported for the provision of data treatment services by the importer (ie data outsourcing, provision of cloud services, data processing etc). In these cases, a data subject's consent would not be required as long as the Argentine data exporter and the foreign data importer/data treatment service provider execute a written agreement to provide such services. The requirements of such a data transfer agreement depend on whether the legislation of the country of the data processor (data importer) provides "adequate levels of data protection" or whether it does not.

In the case of data transfer to countries whose laws do not provide "adequate data protection", such as the USA, an Argentine entity (data exporter) and the foreign data processor (data importer) shall execute a Data Transfer Agreement pursuant to the template set forth by AAPI Regulation 60/2016. This template is extremely similar to the one valid in the EU for this purpose, as set forth by EU Directive 87/2010. Among other requirements, the Data Transfer Agreement requested by the Argentine data protection law shall have:

- Argentine applicable law;
- Argentine jurisdiction for controversies;
- acknowledgment of the AAPI authority;
- both parties' joint liability toward a data subject's/third party's beneficiary for non-compliance with such agreement;
- a data importer's obligation to comply with the technical and security measures established by Argentine data protection law.

Furthermore, if the foreign data processor is obliged to disclose Argentine data pursuant to a foreign government data request, the processor shall immediately notify such circumstances to the data exporter, who may be able to terminate the agreement and request data to be transferred again to Argentina.

An identical data transfer agreement pursuant to Argentine law shall be executed by a foreign data processor and any other sub-contractor that may have access to the Argentine data.

However, if the provider renders data treatment services in countries that do provide adequate levels of protection (for example, countries of the EU), the client and the service provider are free to choose, in the services agreement, which law they will be subject to (ie either Argentine law or the data importer's law).

4.3 Data Localisation Requirements

In addition to the aforementioned data protection requirements, other industry-specific requirements are applicable for international data transfers in certain areas, such as the financial sector. In the latter, data was requested to be maintained in-country until 3 November 2017, when the Argentina Central Bank issued Communication A 6354, allowing data outsourcing abroad, as long as the many requirements therein established are complied with by both the Argentine Financial Institution and the foreign data processor.

Financial institutions intending to perform international data transfer and outsourcing activities shall do so through a communication to the Financial Institutions Bureau (Secretaría de Entidades Financieras y Cambiarias) at least 60 days before initiating such activities, including in such communication certain mandatory information and a copy of the outsourcing agreement in PDF format. The obligation

to comply with the terms of this new regulation shall be expressly indicated in the agreement between the financial institution and the foreign outsourcing services/IT provider. Furthermore, the foreign data processor providing services to Argentine financial institutions shall perform internal audits every year considering in such audits the compliance with this new regulation, and submit a copy of such audits to the External Audit Unit of the Argentine Financial Institutions Bureau, which depends on the Argentine Central Bank.

4.4 Sharing Technical Details

The aforementioned regulation does not impose software code or algorithms or similar technical detail required to be shared with the government. It does require the foreign services provider to address different "scenarios of IT services" classified according to the kind of data to be transferred to the IT provider and the risk thereof derived and imposes several "technical and operative requirements" for each scenario, that both the financial institution and the IT provider shall comply with. However, these requirements do not include specific technologies to achieve them.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

In June 2017, Regulation 11/2017 created the Big Data Observatory, an entity within the IT & Communications Bureau. Although their specific tasks have yet to be defined by further regulation, it aims to "analyse the use of Big Data to obtain technological benefits and innovation possibilities," "study the regulatory framework of personal data use;" "foster and create Big Data technological platforms," "promote good Big Data practices" and "proposal for new regulations." Regulations implementing in detail the aforementioned principles are expected to be issued during 2018.

Data collection through drones was regulated through Regulation 20/2015. However, such regulation essentially states the basic principles already stated in the PDPA, without further details or specifications.

Governmental use of biometric data for security purposes is addressed by Decree 1766/2011, which created the Federal System of Biometric Identification for Security reasons (SIBIOS) to improve scientific investigation of crimes. Biometric data, however, is not defined as a special category of data by the PDPA.

Geolocation data is slightly addressed by AAPI Regulation 18/2015 (Guide to Good Practices in Privacy for the Development of Applications) which simply states that a data owner's consent is needed to access a subject's geolocation data through a software application.

Regarding the internet of things (IoT), in April 2017 the Secretariat of Information and Communication Technology issued Regulation 7-E/2017, calling on interested parties to submit opinions, proposals and needs of different players and sectors involved in the development of the IoT, pursuant to a pre-established administrative proceeding. This regulation was issued within the framework of Regulation 8/2016, which created the "Internet Services Work group" with the purpose of "analysing and promoting public policies to develop internet services"; and in particular to "promote development of Internet of Things, specifically for the development of public policies related to security, public health and environmental matters".

More modern technological and/or data protection-related concepts such as artificial intelligence, machine learning, and facial recognition are discussed by specialised authors – there are not many in Argentina - but are neither incorporated to the PDPA nor included in latter regulations. Assessment and counselling about these topics is provided based on general principles of data protection law stated in the PDPA.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators

Cybersecurity

Legally Required Security Measures

The PDPA and its Regulation AAPI No 11/2006 specify the mandatory security measures for personal data storage and/or treatment. Such Regulation establishes three different security levels according to the nature of the personal data stored in databases: Basic Level Security Measures, Mid-Level Security Measures and Critical Level Security Measures. Every level lists certain security measures that must be adopted by each data controller.

Basic Level Security Measures are applicable to most databases and are considered standard by most industry players. Mid-Level Security Measures apply to banks and companies providing public services. The highest security requirements (Critical Security Measures) apply to health and sensitive data.

Although describing in detail the aforementioned security measures would exceed the scope of this guide, it must be noted that AAPI Regulation 11/06 focuses on the protection of data, not how to achieve it. As long as measures are complied with, the regulation does not impose any particular data storage technological method or solutions, thus allowing database owners to make their own IT solution decisions.

Under the PDPA, AAPI is empowered to apply administrative and criminal sanctions for non-compliance with the

aforementioned security measures. However, so far, no case is known of in which such sanctions or fines were applied for non-compliance with said security measures.

In addition to the aforementioned measures, several regulations issued by the Central Bank of Argentina set minimum standards (including detailed technical requirements) for the management, implementation of and risk control regarding computer technology, information systems and associated resources for financial entities. These are particularly detailed in Argentine Central Bank Communication A 6354, which establishes three different "scenarios of IT services" classified according to the kind of data to be transferred to an IT provider and the risk thereof derived; and imposes several "technical and operative requirements" for each scenario, that both the financial institution and the IT provider must comply with.

Cybercrime
In November 2017, Congress approved Act No 27.411, which ratifies the Argentine accession to the Budapest Convention on Cybercrime. Such law will be able to have a substantial impact in Argentina criminal law related to data cybercrime as all states that ratify or accede to the Convention agree to ensure that their domestic laws criminalise conducts defined therein. The main objective of the Budapest Convention on Cybercrime is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. The Convention covers three principal areas:

- substantive criminal law in the area of cybercrime (illegal access; illegal interception; system interference; misuse of device; computer-related forgery; computer-related fraud, offences related to child pornography; and offences related to infringements of copyright and related rights);
- procedural law (such as the expedited preservation of stored computer data; expedited preservation and partial disclosure of traffic data; real-time collection of traffic data; and the interception of content data); and
- rules of international judicial co-operation.

The Budapest Convention is not operational, as it expressly provides that each state party shall harmonise its national legislation so that it adapts to the different provisions of the Convention. Thus, the real impact of Argentina's accession to the Budapest Convention will be known after Argentina enacts internal regulations adapting its local legislation. Argentina should harmonise its internal rules in relation to procedural law (including its Criminal Procedural Codes) and should enact rules of international co-operation.

It must be noted that in 2008 Argentina enacted Act 26,388 (also called Cybercrime Law) which (partially) harmonises the Argentine Criminal Code with the Budapest Convention on issues related to substantive criminal law. Among the most relevant changes that the Cybercrime Law included in the Criminal Code were:

- the protection of electronic documents under criminal law;
- equal protection of e-mails and handwritten letters;
- inclusion of hacking as a crime;
- inclusion of IT fraud as a crime; and
- inclusion of the IT Damage.

It is still pending to adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with the Convention.

6.2 Data Breach Reporting and Notification
Under Argentine law there is no specific legal obligation to report data breaches to the authorities. Although an Exhibit to Regulation AAPI 11/06 mentions – among other security measures - that data controllers should have a security incidents registry, such obligation has neither been regulated, nor has it established any particular reports to the authorities or affected individuals. Furthermore, the current AAPI director has publicly declared that: "In Argentina, the obligation to inform data security incidents is not legally established".

It may be worth pointing out that currently there is a bill drafted by the AAPI that intends to amend the PDPA integrally – and is still to be discussed by Congress - which addresses in detail data breach incidents and the proceedings to be followed in case they happen. Such a bill intends to be aligned with EU GDPR in this matter. However, to date it seems to be quite far from being enacted.

In the public sector, Presidential Decree 577/2017 created the Cybersecurity Committee, within the Modernisation Ministry, composed by Members of the Modernisation Ministry, the Defence Ministry and the Security Ministry. Said committee shall be in charge of "drafting and developing the National Cybersecurity Strategy", setting framework guidelines and rules for such purpose.

Based on said Decree, in October 2017 the Federal Security Ministry issued Regulation 1107/17 which creates the "Committee to respond to Cybersecurity Incidents" to protect the Security Ministry's IT systems from cyber attacks and coordinate the responses to such attacks.

Said regulations are applicable only to public sector IT systems. However, considering the purposes stated in Decree 577, the Cybercrime Committee may soon issue cybersecurity regulations applicable also to the private sector.

6.3 Ability to Monitor Networks for Cybersecurity

Cybersecurity defensive measures must respect a user's privacy and intimacy, as expressly stated by several regulations including the IT&C Act and National Constitution.

Richards, Cardinal, Tützer, Zabala & Zaefferer
Av. Leandro N. Alem 1050, piso 13.
Buenos Aires (C1001AAS)
Argentina

Tel: +54 11 5031-1500
Fax: +54 11 5031-1500
Email: frene@rctzz.com.ar
Web: www.rctzz.com.ar