THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FOURTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE Privacy, Data Protection and Cybersecurity Law Review

Fourth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2017
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LawReviews

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

ACCOUNT MANAGERS
Pere Aspinall, Sophie Emberson,
Laura Lynas, Jack Bagnall

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Arthur Hunter

EDITORIAL COORDINATOR
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Robbie Kelly

SUBEDITOR
Caroline Fewkes

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-910813-89-8

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© 2017 Law Business Research Ltd

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC–PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

THE ISLAMIC FINANCE AND MARKETS LAW REVIEW

THE ENVIRONMENT AND CLIMATE CHANGE LAW REVIEW

THE CONSUMER FINANCE LAW REVIEW

THE INITIAL PUBLIC OFFERINGS REVIEW

THE CLASS ACTIONS LAW REVIEW

THE TRANSFER PRICING LAW REVIEW

THE BANKING LITIGATION LAW REVIEW

THE HEALTHCARE LAW REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BAKER & MCKENZIE – CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

DUCLOS, THORNE, MOLLET-VIÉVILLE & ASSOCIÉS (DTMV)

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

LEE & KO

M&M BOMCHIL

NNOVATION LLP

PERCHSTONE & GRAEYS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VDA VIEIRA DE ALMEIDA

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 4

ARGENTINA

Adrián Lucio Furman, Francisco Zappa and Catalina Malara[1]

I OVERVIEW

Data protection was introduced to the Argentine legal system following the 1994 constitutional reform, with the incorporation of the *habeas data* procedure.[2] With this constitutional reform, data protection rights in Argentina acquired constitutional protection and, thus, are considered fundamental rights that cannot be suppressed or restricted without sufficient cause.

In October 2000, Congress passed Law No. 25,326 (the Data Protection Law), which focused directly on data protection. It defined several data protection-related terms and included general principles regarding data collection and storage, outlining the data owner's rights and setting out the guidelines for the treatment of personal data. It is an omnibus law largely based on the EU Data Protection Directive[3] and the subsequent local legislation issued by the European countries (mainly Spain). Moreover, on 30 June 2003, the European Union issued a resolution establishing that Argentina had a level of protection consistent with the protection granted by the Directive with respect to personal data.

Additionally, the Data Protection Law created the enforcement authority embodied by the National Data Protection Agency (the Data Protection Agency), which is the office in charge of enforcing the data protection regulations, controlling the registration of databases, assisting individuals regarding their rights, receiving claims and carrying out inspections of companies to assess their compliance with the Data Protection Law.

In 2014, Law No. 26,951 (the Do-Not-Call Law) created the do-not-call registry and expanded the protection of data owner's rights. This regulation is enforced by the Data Protection Agency and allows the data owner to block contact from companies advertising, selling or giving away products and services. Companies offering products and services by telephonic means must register with the Data Protection Agency and consult the list of blocked numbers on a monthly basis before engaging in marketing calls.

---

1 Adrián Lucio Furman is a partner and Francisco Zappa and Catalina Malara are associates at M&M Bomchil.

2 Section 43, Paragraph 3 of the National Constitution states that, 'Any person can file this action to obtain access to any data referring to himself or herself, registered in public or private records or databases, intended to supply information; and in the case of false data or discriminatory data, to request the suppression, rectification, confidentiality or updating of the same. The secret nature of the source of journalistic information shall not be impaired'.

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

II THE YEAR IN REVIEW

During the early months of 2017, Justice 2020, a governmental initiative for the design of public policies promoted by the Ministry of Justice together with the Data Protection Agency, proposed amendments to the Data Protection Law and the Do Not Call Law. As of 15 September 2017, this draft bill (the Draft) has yet to be submitted to the legislative branch of government.

The Draft defines new data protection-related terms and clarifies other terms defined by the Data Protection Law.

One of its most relevant changes is the scope of application and jurisdiction of the law, which is not currently regulated by the Data Protection Law. If it is passed, this new law will apply in the following cases: (1) when the person responsible for the treatment is domiciled in Argentina, even if the data treatment takes place abroad; (2) when the person responsible for the data treatment is not based in Argentina but in a place where Argentine legislation applies by virtue of international law; and (3) when the data treatment of data owners that reside in Argentina is performed by an entity with responsibility for data treatment that is not based in Argentina but whose data-treatment activities are related to the offer of goods or services to data owners in Argentina, or to the monitoring of their acts, behaviour or interests.[4]

With this new wording, the Draft specifically recognises that data treatment involving Argentine residents' personal data can occur abroad and grants the same protections as if the treatment had taken place in Argentina.

The Draft also includes new valid ways for obtaining the data owners' consent for the treatment of their personal data,[5] stating that express consent may be granted in writing, orally or through electronic means or any other similar means that technology may offer.

Moreover, the concept of tacit consent[6] is introduced. Tacit consent shall be deemed granted by the data owner when (1) it emerges clearly from the context of the data treatment; (2) the conduct of the data owner is sufficient to demonstrate the existence of the relevant authorisation; (3) the data requested is necessary for the purpose of the collection; and (4) the data owner has been informed of his or her rights arising from the law.

The Draft, following the principles set out in the Data Protection Law, expressly prohibits the treatment of sensitive data, with the following exceptions: (1) the data owner has granted his or her express consent to the treatment; (2) the treatment is necessary for the fulfilment of labour and social security obligations in relation to the data treatment itself or to the data owner; (3) the treatment is necessary for the recognition, exercise or defence of rights in a judicial procedure; or (4) the treatment has a historical, statistical or scientific purpose, in which case dissociation of data must take place.

Following the recent Regulation (EU) 2016/679 of the European Parliament and of the Council, the Draft expressly addresses and regulates the consent given by children or teenagers for the treatment of their personal data.[7] The Draft establishes that such consent shall be deemed valid when it is applied to the processing of data directly linked to information services specifically designed and suitable for children or teenagers. Teenagers can grant

4 Section 4 of the Draft.

5 Section 12 of the Draft.

6 Section 12 of the Draft.

7 Section 18 of the Draft.

their consent from 13 years of age. For children less than 13 years old, the treatment of their personal data shall be considered lawful only if consent is granted by the child's parent or guardian.

Another relevant addition by the Draft is the inclusion of a procedure to be carried out by data processors in the event of data breaches. The Draft incorporates the obligation for the person responsible for the data treatment to document and report data incidents to the data owner and the enforcement authority with no delay, and preferably within 72 hours of the acknowledgment of the security breach, unless the breach is unlikely to present a risk to the data owner.[8]

With this key modification, the Draft regulates standard procedures, providing guidelines for dealing with security breaches, which the Data Protection Law does not address.

Regarding the data owner's rights,[9] the Draft extends the scope of the information to be provided to the data owner when exercising its right of access, stating that the data owner must be informed of not only the existing data, but also, *inter alia*, (1) the recipients or categories of recipients to whom the personal data has been or will be transferred; and (2) the existence of automatic decision-making processes, including profiling.

Additionally, the right to data portability is incorporated,[10] which establishes that when electronic services that comprise personal data treatment are provided, the data owner will have the right to obtain from the person responsible a copy of the personal data in a structured and commonly used format that allows its subsequent use or its direct transference from responsible entity to responsible entity when it is technically possible.

With respect to users and managers of files, records and databases, specific guidelines related to proactive responsibility are established:[11] among the technical and organisational measures to be taken, the person responsible for the treatment should include *inter alia*, internal or external audits, the adoption of a 'privacy policy' or the adherence to binding self-regulatory mechanisms to be submitted for approval by the enforcement authority. In particular, it is ordered that measures should be taken to ensure that, by default, only personal data necessary for each of the purposes of the data treatment are processed.

Another relevant addition is the requirement for the creation of a data protection officer,[12] who must be appointed when sensitive data or large-scale data treatment is carried out. The data protection officer's responsibilities include, *inter alia*, internal advice and compliance duties in connection to data protection issues.

Binding self-regulating mechanisms are encouraged, and should be filed with the enforcement authority for approval.

The Draft also excludes the possibility of legal entities registering with the do-not-call registry to block contact.[13]

8 Section 20 of the Draft.

9 Section 28 of the Draft.

10 Section 33 of the Draft.

11 Section 37 of the Draft.

12 Section 43 of the Draft.

13 Section 49 of the Draft.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

As expressed above, the Data Protection Law is an omnibus law that regulates data protection in a comprehensive manner. In contrast to other jurisdictions (particularly the United States), Argentina does not have other specific data protection regulations outside the scope of the Data Protection Law, and there is no related legislation at a subnational level.

The Data Protection Law includes principles regarding data protection, data owners' rights, the organisation of data archives and databases, and actions to protect personal data, to mention a few.

The Law's main purposes are (1) to protect personal data stored in archives, registers, databanks or other technical means of data processing; (2) to guarantee people's honour and privacy; and (3) to ensure data owners their rights to access records of their data stored and treated by third parties.

As is the case with most omnibus data protection laws around the world, the Data Protection Law contains several defined terms that are essential for interpreting the Law and determining its scope of application. Some of the main defined terms are:

a personal data: information of any kind referring to an individual or legal person, either determined or determinable;

b sensitive data: personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral convictions, union affiliation and information concerning health or sexual life;

c person responsible for the registry or database: the individual or legal entity that is the owner of a file, registry or database; and

d data owner: any individual or legal entity residing in Argentina whose data is the object of the treatment referred to in this Law.

The following are the main principles expressed by the Data Protection Law:

a due registration: data storage will be lawful if the database is duly registered with the Data Protection Agency; and

b data quality: personal data collected must be true, adequate, relevant and not excessive in relation to the scope and purpose for which the data has been obtained. The collection of personal data cannot be done by unfair or fraudulent means. Personal data subject to treatment cannot be used for purposes different from or incompatible with those leading to their collection.

The main rights for data owners contained in the Data Protection Law are the right of information, access and suppression: exercising this information right, data owners can request from the person responsible for the database their personal information that has been collected, the purpose of the collection and the identity of the person responsible for it. Additionally, personal data that is totally or partially inaccurate or incomplete should be deleted and replaced or, if necessary, completed by the file manager when the inaccuracy or incompleteness of the information is known. Data owners do not have to pay to exercise these rights. This right of access can be exercised (1) directly, through the person responsible for the database; (2) through the Data Protection Agency; or (3) through the *habeas data* procedure. To guarantee these rights, data must be stored in a way that allows the exercise of the right of access of the owner. Data must be destroyed when it is no longer necessary or relevant for the purposes for which it was collected.

ii General obligations for data handlers

The first obligation for data handlers is to obtain consent from data owners. The treatment of personal data is unlawful when the data subject has not given his or her express consent to the treatment of the data, either in writing or through any other similar means. The consent must appear in a clear and unequivocal manner. There are certain exceptional cases in which consent is not requested, such as when the personal data (1) derives from unrestricted public-access sources; (2) is collected for the performance of public duties; (3) is limited to name, identification card number, tax or social security identification, occupation, date of birth, domicile and telephone number; (4) arises from a contractual relationship and is necessary for the fulfilment of that contract; or (5) refers to the transactions performed by financial entities and arises from the information provided by their customers.

Another important obligation for database owners is the obligation for registration with the Data Protection Agency. To file the registration, the company or individual responsible for the database must provide information regarding the location of the database, its characteristics and purpose, specifications of the data provided, origin, means of collection, etc. This registration must be renewed annually. The registration process is simple and relatively inexpensive.

iii Specific regulatory areas

The Data Protection Law contains several specific regulations applicable to different areas and industries.

One of the most relevant areas is financial information provided by private registries issuing reports. In that sense, to analyse a prospective client's financial records it is common for banks and other financial entities to seek credit information through different credit information services.

The Data Protection Law specifies which information can be treated. First, it needs to be personal data of an economic nature and it must be obtained from public sources or have been given by the data owner or collected with the data owner's consent.

Additionally, information regarding the fulfilment (or not) of a party's financial obligations can be given by the creditor (or by someone acting on its behalf), since both parties are owners of the information. In this case, there is no need to obtain the other party's consent.

Information relevant for the assessment of someone's financial capacity can be stored, registered or transferred for a maximum of five years. If the debtor cancels the debt, or it expires by any means, the period shall be reduced to two years. This issue tends to generate a substantial number of claims from consumers and users of financial services.

The Data Protection Law regulates the treatment of personal data by health institutions too. Public and private hospitals and health professionals can process their patients' data relating to mental or physical health, as long as they respect professional secrecy.

These registries are very useful for scientific purposes, but it is important to note that they store sensitive data and dissociation of data is advised.

Furthermore, security and surveillance industries are also regulated and are currently the focus of most of the inspections carried out by the Data Protection Agency. Disposition 10/2015 regulates the use of closed-circuit television cameras in public spaces. The Disposition establishes that the use of these cameras is lawful when the data handler has obtained the data owner's prior and informed consent. Consent shall be deemed as granted by the data owner if the data collector includes signs indicating the existence of these cameras,

the purpose of the data collection, the person responsible for the treatment and the relevant contact information. A template of this sign is included in the Disposition. The relevant database must be registered and the data collector must implement a manual for its use.

iv Technological innovation

The Data Protection Law has not been amended recently. For that reason, several technological innovations fall outside its scope.

The use of cookies, for example, was not included in the legislation. Nevertheless, by application of the Data Protection principles, companies trying to obtain information through them must obtain the user's consent to collect information.[14]

The use of big data, on the other hand, presents a much deeper issue. Through big data, companies collect big amounts of information and its different uses are not always clearly determinable since data is often reused – so violating one of the Data Protection Law's main principles, which is specifying to the data owner the purpose of the data collection. Moreover, data treated must be accurate, true and not excessive in relation to the purpose. In many cases, it is not possible to assess that all information is accurate. Because of the large volume of information provided, some of it is bound to be inaccurate.[15] The Data Protection Law has fallen behind in regulating the use of big data. The collection of excessive amounts of information is only of benefit to the user, and regulation of big data must recognise this new and useful way of treating data and always respect the user's rights.

The Data Protection Agency has enacted several regulations aimed at reducing the technological gap generated between the enactment of the Data Protection Law and the present day. Besides the aforementioned Disposition 10/2015 on closed-circuit television cameras, a specific disposition regulating the use of drones has been enacted, setting out data privacy principles that apply to the use of these devices. Moreover, a recent disposition was enacted that contains best practice guidelines for data collection through apps.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Every nation that has specifically regulated data protection has realised that any form of planning and controlling would become useless if collected data could be automatically and unrestrictedly transferred abroad to be processed. Following the European model,[16] the Data Protection Law has prohibited international data transfer when the transfer is to countries or international or supranational organisations that do not offer 'adequate levels of protection'.[17]

With this provision, Argentina has tried to avoid data being collected and treated in its territory without regulatory controls in place or without the data owner being able to exercise its rights. Where there are no regulatory controls in place or data owners are unable to exercise their rights, international data transfers are prohibited.

It will be considered that a country or organism has an adequate level of protection when those protections derive directly from the legal order, self-regulatory measures or contractual clauses that include specific data protection provisions.

14 Osvaldo Alfredo Gozaini, *Habeas Data, Protection of Personal Data* (Rubinzal-Culzoni), p. 325.

15 Luciano Gandola, 'Conflicts between Big Data and the Data Protection Law', Infojus.

16 See footnote 3.

17 Section 12 of the Data Protection Law.

Pursuant to Regulatory Decree 1558/2001,[18] the Data Protection Agency is responsible for assessing the levels of protection granted by each country or organism, either *ex officio* or through consultation with a concerned party. If it considers that any given country or organisation does not provide adequate levels of protection, the Data Protection Agency must request the executive branch of the government to issue a declaration.

The offered levels of protection will be assessed in light of the data transfer's circumstances, the nature of the personal data involved, the duration of the treatment and the applicable law in the destination country, among other things.

Therefore, if the recipient party belongs to a country or organisation that does not comply with the Argentine legal requirements, it should adopt self-binding regulatory measures or contractual provisions covering protection for data owners.

In practice, the transferring party must assess the recipient's levels of protection and, if the recipient fails to offer protection at an adequate level legal, the transferring party must overcome this by obtaining the data owner's consent, or establishing contractual provision for an adequate level of protection.

Regulatory Decree 1558/2001 states that if the data owner has given its consent, it does not matter whether the state or organisation does not offer an adequate level of protection and, in that case, the international transfer can take place.

Additionally, consent is not necessary if the personal data is stored in a public registry legally created to provide information and that is open for public consultation or by anyone evidencing a legitimate interest.

The aforementioned prohibition will not apply in cases of (1) international judicial cooperation; (2) transfer of medical information, when the treatment of the deceased requires it, or in the case of an epidemic investigation; (3) bank or stock transfers; (4) transfers decided under international treaties to which Argentina is a party; and (5) when it takes place because of cooperation between agencies fighting organised crime, terrorism or drug trafficking.

V COMPANY POLICIES AND PRACTICES

Although it is not expressly set out in the legislation, companies are encouraged to implement a privacy policy that regulates their personal data collection, treatment and processing and security mechanisms. It is common for the Data Protection Agency to request this policy from companies upon inspections.

Additionally, Disposition 11/2006 of the Data Protection Agency requires companies to draft a security manual or report establishing the procedures and safety measures taken regarding personal data. The manual must describe the obligations of the employees regarding data treatment, the control measures implemented by the company, the applicable procedure upon information breaches or data-loss incidents, the measures for preventing malicious software, etc.

Disposition 10/2015 establishes that companies using closed-circuit television cameras must implement a policy that includes the means of data collection, a reference to the place, dates and hours of operation of the cameras, technical and confidentiality mechanisms to be used, ways of exercising the data owner's rights and, if applicable, reasons that justify obtaining a picture of the individuals entering the facilities.

18 Section 12 of Regulatory Decree 1558/2001.

Lastly, Disposition 18/2015 of the Data Protection Agency establishes 'best practice guidelines for data collection through apps'. In addition to explaining specifically how data protection principles operate in this matter, the Disposition establishes that the privacy policy should be clear and easily accessible for users. Moreover, the privacy policy for apps designed for use on phones or tablets must be shown in a useful way for users, bearing in mind the size restrictions that apply to these devices. The use of icons, pictures, distinctive colours and sounds is recommended; extra care is requested when the app is suitable for children or teenagers.

VI DISCOVERY AND DISCLOSURE

As stated above, data owners have several rights that derive from the Data Protection Law. Nevertheless, the rights of access, rectification and suppression can be denied when they could affect Argentina's national security, order or public safety, or the protection of rights or interests of third parties.

Additionally, information regarding personal data can be denied when the disclosure of information could become an obstacle to judicial or administrative proceedings regarding tax matters, pension obligations, the development of health and environmental control functions, the investigation of criminal offences or the verification of administrative infringements. The resolution denying access must be reasoned and notified to the affected party, and must relate to the reasons established above.

Since these provisions include a limitation of rights, they should be interpreted restrictively. Additionally, to safeguard the data owner's rights, this limitation must be subject to judicial review.

Despite all these provisions, the data owner must be able to access the registries if his or her defence rights rely on this action, in which case the access restriction must be lifted.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Data Protection Agency is the enforcement authority created by the Data Protection Law. Its lack of autonomy (it operates within the scope of the Ministry of Justice) has been subject to debate, and current plans involve the creation of a new autonomous entity in line with the criteria used in countries with the highest degree of personal data protection.

The agency's main functions are (1) operating as a registry of databases, keeping records of the registration and renewal of databases; (2) enforcing the Data Protection Law and the Do-Not-Call Law, carrying out inspections and imposing sanctions; and (3) creating new dispositions and regulations related to data protection matters.

In using these powers, the Data Protection Agency has issued several dispositions relating to its investigatory and auditing powers. In this context, Disposition 55/2016 regulates the Data Protection Agency's auditing procedures. The main aims of these proceedings are to control the activity of the person responsible for the database and ensure its compliance with the law.

The proceedings can be (1) *ex officio*, either scheduled annually or spontaneous; or (2) initiated upon a complaint, in which case the inspection itself will have an evidentiary nature.

After the inspection is finalised, the inspector will issue a final report with the outcome of the inspection. If the database owner has complied with the law, the proceeding is finalised. If it has not complied with the regulations, it is granted 15 days to remedy its non-fulfilment, otherwise sanctioning proceedings will begin.

ii Recent enforcement cases

The enforcement actions of the Data Protection Agency have evolved and intensified over the years. During its first years, the Agency's role was more educational than punitive, giving companies ample time to adapt to the new legislation and being proactive in responding to enquiries and explaining misconceptions. Nowadays, 17 years after the enactment of the Data Protection Law, the Agency is being more proactive in carrying out inspections and is stricter with its enforcement and punitive capabilities.

The vast majority of recent fines have been for violation of the Do-Not-Call Law, resulting in a large number of administrative proceedings and claims. Some fines have also been imposed in the recent past on companies failing to comply with their obligations under the Data Protection Law (mainly failure to register or renew registrations for their databases and failure to comply with security measures).

On a judicial level, most of the case law regarding personal data protection is connected to financial companies and the information they provide to consumer credit reporting agencies regarding their customers' debts. In most cases, the proceedings relate to financial companies' failure to update their registries once debts have been paid or the statute of limitations applied.

In this context, the Supreme Court has also stated that the 'right to be forgotten' has constitutional rank and must be respected. These cases have all been filed under the *habeas data* regime.

iii Private litigation

As stated above, the judicial remedy for private plaintiffs is the *habeas data* procedure regulated by the National Constitution and the Data Protection Law. Despite the fact that the access right of data owners can also be exercised through an administrative procedure, a judicial action is the only way for private plaintiffs to receive financial compensation.

Considering that the administrative procedure before the Data Protection Agency is a fast, free and accessible mechanism, there are not many cases brought at the judicial level.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Unlike most recent European legislation and the regulations contained in the Draft, the Data Protection Law does not specifically regulate international jurisdiction. The Data Protection Agency has no enforcement authority under the current regime regarding companies that are based abroad with no assets or registrations in Argentina, even if these companies collect and treat personal data from Argentine residents. However, foreign companies registered in or that have assets in Argentina must register with the Data Protection Agency and register their databases, to comply with the Argentine data protection regime.

Consequently, on a theoretical level, what triggers the need to comply with the Argentine regime for personal data protection is the collection or treatment of personal

data from Argentine residents. On a practical level, the need to comply with Argentine regulations is triggered by the presence of the foreign company in Argentina by way of assets or registrations in the Public Registry of Commerce.

A few months ago, a well-known technology and transport company started offering its services in Argentina, opening offices and hiring personnel. Because of the media coverage its services received, it came to the Data Protection Agency's attention that the company was operating through mobile applications that necessarily collected data, but no databases were registered. For that reason, the Data Protection Agency started an investigation and required the foreign company to register its databases with the Data Protection Agency.

IX CYBERSECURITY AND DATA BREACHES

Cybersecurity is not a highly regulated area in Argentina. The Data Protection Law does not contain specific regulations regarding data breaches. There are some regulations enacted by the National Central Bank regarding data security obligations for financial institutions, but there is no uniform or omnibus legislation that regulates the matter.

Although Resolution No. 580/2011 of the Chief of Staff created the National Programme for Critical Infrastructures for Information and Cybersecurity, there are not many companies taking part in this programme as it is not mandatory. Its main aim is to promote the creation and adoption of a specific regulatory framework for the protection of strategic infrastructures for the national public sector, inter-jurisdictional organisations and private sector organisations that require it. It seeks the collaboration of those sectors to develop adequate strategies and structures for coordinated action.

Furthermore, Decree 577/2017 has created the Cybersecurity Committee, which will mainly focus on creating a regulatory framework, educating people on the importance of cybersecurity, creating a national cybersecurity plan and creating general guidelines for security breaches. The Ministries of Modernisation, Defence and Security will take part in this initiative.

X OUTLOOK

The future landscape in Argentina regarding personal data protection includes the almost certain enactment of a new law, in line with the new technologies that have emerged since the year 2000.

It is not certain whether the Draft will be sent to Congress and finally passed, but it is the first stepping stone and is certainly one of the Data Protection Agency's objectives. We believe that a new law, in line with the European Union General Data Protection Regulation, will be enacted within the next two years.

Another probable, significant change in the near future is the creation of a new autonomous and independent enforcement agency, operating outside the scope of the Ministry of Justice. The lack of an autonomous enforcement authority has been a matter of criticism in the international community and many believe that, if it is not solved in the near future, it may lead to the loss of Argentina's status as an 'adequate' country by EU standards regarding data protection.

Appendix 1

ABOUT THE AUTHORS

M&M BOMCHIL

Suipacha 268, 12th floor
Buenos Aires 1008
Argentina
Tel: +54 11 4321 7500
Fax: +54 11 4321 7555
adrian.furman@bomchil.com
francisco.zappa@bomchil.com
catalina.malara@bomchil.com
www.bomchil.com.ar

ADRIÁN LUCIO FURMAN

M&M Bomchil

Adrián Furman is a partner in the mergers and acquisitions and entertainment law departments and in charge of M&M Bomchil's intellectual property area. He joined the firm in 2000.

He graduated as a lawyer from the University of Buenos Aires in 1998. He obtained a postgraduate degree in corporate business law at the same institution, where he is also a professor of civil and commercial contracts.

He has worked on numerous cross-border transactions and regularly advises corporate clients on various issues of a contractual nature. He also has wide experience of issues of commercial fair trade and consumer protection.

During 2005 he was international associate at the New York offices of Simpson Thacher & Bartlett.

He is a frequent speaker at chambers of commerce on his areas of expertise and at the Section of International Law of the American Bar Association seasonal meetings.

He has been and is a director and auditor of important companies such as PepsiCo, AMC Networks, Telefe and Mindray, among others.

He is co-chair of the International Commercial Transactions, Distribution and Franchise Committee of the Section of International Law of the American Bar Association.

His professional performance has been recognised by various specialised publications, including *Chambers Latin America* and *Best Lawyers*, and by the Latin American Corporate Counsel Association and Client Choice Awards.

FRANCISCO ZAPPA

M&M Bomchil

Francisco Zappa is a semi-senior lawyer in the mergers and acquisitions and entertainment law departments. He joined M&M Bomchil in 2011.

He graduated with honours from the University of Salvador, Buenos Aires and completed his masters' degree in corporate law at the University of San Andrés, Buenos Aires. His practice focuses on diverse corporate and contractual matters. He has wide experience in fair trade and consumer protection issues and specialises in data protection law.

During 2017, he was an international associate at the New York offices of Simpson Thacher & Bartlett.

He is a frequent speaker at chambers of commerce on matters in his areas of expertise.

CATALINA MALARA

M&M Bomchil

Catalina Malara is a member of the mergers and acquisitions and entertainment law departments at M&M Bomchil. She graduated with honours from the University of Buenos Aires in 2016.

Strategic Research Sponsor of the
ABA Section of International Law

Law
Business
Research

ISBN 978-1-910813-89-8