Practical Law™
MULTI-JURISDICTIONAL GUIDE 2014/15
DATA PROTECTION

Data protection in Argentina: overview

Maximiliano D'Auro and Inés de Achaval
Estudio Beccar Varela

global.practicallaw.com/3-586-5566

REGULATION

Legislation

1. What national laws regulate the collection and use of personal data?

General laws

The right to the protection of personal data is enshrined in section 43 of the Argentine National Constitution (Constitution). The current legal framework of the Argentine Data Protection Regulations (ADPR) is made up of the Constitution and the:

- Personal Data Protection Law 25,326 (PDPL).
- Regulatory Decree 1558/2001 (DP Decree).
- Provisions issued by the National Directorate for Personal Data Protection (NDPDP) (for example, Provision NDPDP 4/2009).

Additionally, National Law 26,951 was enacted, which created a "Don't Call" registry, substantially similar to the sectoral laws in the city of Buenos Aires and the province of Buenos Aires (*see below, Sectoral laws*).

Sectoral laws

Law 2,014 of the City of Buenos Aires and Law 14,326 of the Province of Buenos Aires both created "Don't Call" Registries, each within their own jurisdiction. This enabled people who did not want to receive marketing telephone calls to register. Companies using telemarketing strategies must check the registry corresponding to their jurisdiction (every 15 days in the case of the registry from the City of Buenos Aires and 60 days in the case of the Province of Buenos Aires) and refrain from contacting those listed on the register.

Scope of legislation

2. To whom do the laws apply?

The Argentine Data Protection Regulations (ADPR) apply to all persons or legal entities carrying out the treatment or processing of personal data. See *Questions 3* and *4*.

3. What data is regulated?

The Argentine Data Protection Regulations (ADPR) protects all types of personal data. Under the ADPR, personal data includes any type of information that relates to identified or identifiable individuals or legal entities.

4. What acts are regulated?

The Argentine Data Protection Regulations (ADPR) apply to the treatment or processing of personal data. The Personal Data Protection Law 25,326 (PDPL) defines the treatment or processing of data as any "systematic operations and procedures, either electronic or otherwise, that enable the collection, preservation, organisation, storage, modification, relation, evaluation, blocking, destruction, and in general, the handling of personal information, as well as its communication to third parties through reports, inquiries, interconnections or transfers".

5. What is the jurisdictional scope of the rules?

The Argentine Data Protection Regulations (ADPR) apply to any action that is considered to be treatment or processing of personal data within the Argentine territory. If a single isolated act related to personal data (for example, the collection or transfer of data) takes place in Argentina and the rest of the processing is carried out abroad, the ADPR will govern that single isolated action.

6. What are the main exemptions (if any)?

There are no main exemptions. Argentine law solely applies within the territory of Argentina. There are no exceptions or cases of extra-territorial application of the Argentine Data Protection Regulations (ADPR).

Notification

7. Is notification or registration required before processing data?

The creation of a database is only legal when the database has been duly registered before the National Directorate for Personal Data

Protection (NDPDP) (*section 3, Personal Data Protection Law 25,326* (PDPL)). The requirement to register databases is an essential condition for the legality of any processing of personal data. The NDPDP does not require disclosure of the content of the databases, but only general information about their creation and maintenance, and compliance with the principles of the PDPL. Registration is a simple process, mostly done online.

Notification is not required before data processing, but the rules on consent apply (*see Question 9*).

MAIN DATA PROTECTION RULES AND PRINCIPLES

Main obligations and processing requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

The following fundamental principles apply to data processing (*sections 4 and 10, Personal Data Protection Law 25,326* (PDPL)):

- **Purpose proportionality.** Personal data collected for processing must be relevant and not excessive in relation to the scope and purpose for which it were obtained.
- **Data accuracy.** Personal data collected for processing must be correct and accurate. It must also be updated, corrected or deleted as necessary; this is in addition to the data subjects' right to request this.
- **Purposes restriction.** Data collected for processing must not be used for any purpose other than the purpose it was collected for.
- **Confidentiality.** Those responsible or involved in any part of the data processing are bound by the duty of confidentiality.

9. Is the consent of data subjects required before processing personal data?

As a general rule, the treatment or processing of personal data is only legal when carried out with the data subject's prior and informed consent. The consent must be "in writing or by any other means that could be assimilated to writing, according to the circumstances" (*section 5, Personal Data Protection Law 25,326* (PDPL)).

In spite of the above, section 5, paragraph 2 of the Regulatory Decree 1558/2001 (DP Decree) provides that the National Directorate for Personal Data Protection (NDPDP) states the requirements for consent to be valid when provided by a means other than writing. In such cases, it is essential that the authorship and integrity of the declaration is ensured. However, to date the NDPDP has not exercised these regulating powers, and electronic consent for the treatment or processing of personal data is not expressly accepted by the applicable regulations. In any case, the method of expressing consent (other than printed writing) must produce and record enough evidence to prove that consent was actually given, in accordance with the formalities required by the Argentine Data Protection Regulations (ADPR).

With regards to consent for minors, the general dispositions from the Argentine Civil Code apply, meaning that minors do not have the legal capacity to provide their consent. Therefore, any consent involving minors must be provided by whoever is exercising the minors' legal representation (usually, the minors' parents).

10. If consent is not given, on what other grounds (if any) can processing be justified?

The Personal Data Protection Law 25,326 (PDPL) provides that consent is not necessary when the data:

- Is obtained from unrestricted sources that are accessible to the public.
- Is collected to comply with State powers or by virtue of a legal obligation.
- Is limited to basic information such as, name, ID, tax or social security numbers, occupation, date of birth and domicile.
- Derives from a scientific or professional contractual relationship and is only used in this context.
- Refers to transactions performed by financial institutions, including any information received by clients (protected by bank secrecy laws).

In addition, consent may not be necessary when the data:

- Is transferred for outsourcing purposes only, under certain conditions contained in section 25 of the PDPL and Regulatory Decree 1558/2001 (DP Decree).
- Is collected or processed for the provision of credit information services, to the extent permitted by section 26 of the PDPL and the DP Decree.
- Is collected or processed for marketing purposes, to the extent permitted by section 27 of the PDPL and the DP Decree.

Special rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

Sensitive data is defined in section 2 of the Personal Data Protection Law 25,326 (PDPL) as personal information revealing racial or ethnic origin, political views, religious beliefs, philosophical or moral stands, union affiliations or any information referring to health or sexual life.

Sensitive data is simply a sub-category of personal data that receives enhanced protection. Sensitive data must always be protected by advanced security measures, in contrast with other personal data that must be protected by basic or medium security measures.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

For consent to be valid under the Argentine Data Protection Regulations (ADPR), data subjects must be informed, in an express and clear manner, according to their cultural and social levels of education, of:

- The purpose for which the data is being processed and details of any third parties.
- The existence of a database and the identity and location of the data controller.

- The consequences of refusing to give information or providing inaccurate information.
- The data subject's right to access, update, correct and delete their data.

13. What other specific rights are granted to data subjects?

Data subjects have the right to request and obtain information on any personal data included in a database (*section 14, Personal Data Protection Law 25,326* (PDPL)). The data controller must provide this information within ten calendar days of notification. Data subjects can exercise these rights free of charge every six months or more, unless a legitimate interest is proven.

All data subjects have the right to request that their data is rectified, updated or deleted from databases. The data controller must rectify, update or delete the personal data within the five-day period following a data subject's request.

The data controller can deny the access, rectification or deletion of personal data in order to protect the country's national defense, order and public safety, or third parties' rights or interests.

14. Do data subjects have a right to request the deletion of their data?

All data subjects have the right to request the deletion of their data. *See Question 13*.

SECURITY REQUIREMENTS

15. What security requirements are imposed in relation to personal data?

The data controller must adopt technical and organisational measures to ensure the safety and confidentiality of personal data. Such measures are necessary to (*section 9, Personal Data Protection Law 25,326* (PDPL)):

- Avoid the falsification, loss, unauthorised access or treatment of the personal data.
- Enable the detection of deviations of information (intentional or unintentional), and whether caused by human action or by technical means.

It is prohibited to record personal data in archives, registers or databases that do not comply with the necessary security conditions. Provisions 11/2006 and 9/2008 of the National Directorate for Personal Data Protection (NDPDP) provide further detail on the exact security requirements needed to comply with these obligations. Provision 11/2006 of the NDPDP divides the security measures into three categories, each applicable according to the category of the data involved (basic, medium, and critical).

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

There is no requirement to notify data subjects or the National Directorate for Personal Data Protection (NDPDP) of any personal data security breaches.

REGULATOR DETAILS

National Directorate for Personal Data Protection (NDPDP) (Dirección Nacional de Protección de Datos Personales)

W www.jus.gob.ar/datos-personales.aspx

Main areas of responsibility. The NDPDP is the governmental agency, within the Ministry of Justice and Human Rights. The NDPDP is responsible for regulating the processing of personal data in Argentina. The NDPDP is empowered to take all actions necessary to enforce the provisions of the legal framework in Argentina.

However, in accordance with Provision 11/2006 of the NDPDP all owners or users of databases must implement a Data Protection Security Manual, which must contain records of any incidents related to personal data safety.

PROCESSING BY THIRD PARTIES

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

When a third party processes personal data on behalf of the data controller, they must enter into a written agreement under which the third party undertakes (*section 25, Personal Data Protection Law 25,326* (PDPL) and the *Regulatory Decree 1558/2001* (DP Decree)):

- To process the data exclusively according to the data controller's instructions.
- To comply with the security levels provided by the Argentine Data Protection Regulations (ADPR).
- To protect the confidentiality of the data.
- To implement the technical and security measures contained in section 9 of the PDPL and Provisions 11/2006 and 9/2008 of the National Directorate for Personal Data Protection (NDPDP).
- To use and apply the data solely and exclusively for the purpose set out in the services agreement.
- Not to disclose the data to any other party (even for storage purposes).
- To destroy the data once all contractual obligations have been fulfilled, unless written authorisation is obtained from the data controller to keep the data for longer where there is a reasonable possibility that there will be future requests related to the data, in which case it may be stored in safe conditions for a maximum period of two years.

ELECTRONIC COMMUNICATIONS

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

There are no specific requirements for the storage of cookies or equivalent devices on the data subject's terminal equipment, other than the requirement of consent.

The classification of IP addresses obtained through cookies as "anonymous data" or "personal data" is highly controversial. Some experts in Argentina claim that IP addresses are not personal data, as they identify a machine rather than an individual. However, the general interpretation, supported

ONLINE RESOURCES

Official website for legal information

W www.jus.gob.ar/datos-personales/documentacion-y-capacitacion/normativa/normativa-proteccion-de-datos-personales.aspx

Description. This links to the section on applicable regulations on personal data protection, within the website of the Ministry of Justice and Human Rights. It is maintained by the NDPDP, within the Ministry of Justice and Human Rights. The uploaded regulations are official and up-to-date, although not all regulations are uploaded. The website is only available in Spanish.

W www.infoleg.gov.ar

Description. This is a link to the official government website, containing all legislative and documentary information. It is controlled by the Ministry of Economy and Public Finance. The regulations provided are official and up-to-date, and all Argentine regulations on data protection (including Provisions issued by the NDPDP) are uploaded to the website. The website is only available in Spanish.

by the National Directorate for Personal Data Protection (NDPDP) is that IP addresses must be regarded as personal data under the Argentine Data Protection Regulations (ADPR). This is due to their ability to track individual behaviour and activity on the Internet, and even if the resulting data does not provide the identity or name of the individual, it allows them to be contacted, for example, for marketing purposes.

If IP addresses are regarded as personal data under the ADPR, consent is required. However, if IP addresses are classified as "anonymous data", then obtaining consent is not necessary. However, to be cautious, it is better for IP addresses to be classified as "personal data", meaning that prior consent is required for the recollection of personal data associated with an IP address via the storage of cookies.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

Electronic commercial communications can only be sent if the data is (*section 27, Personal Data Protection Law 25,326* (PDPL)):

- Accessible in public documents.
- Provided by the data subject.
- Obtained with the data subject's consent.

However, the processing of personal data for commercial or marketing purposes is allowed without the prior consent of the data subject when both (*section 27, Regulatory Decree 1558/2001* (DP Decree)):

- The data is limited to the creation of certain consumer profiles that categorise personal preferences and similar types of behaviour.
- The data subjects are solely identified by their belonging to generic groups and the individual data is strictly necessary to market or advertise to the individual.

The DP Decree and the PDPL provides that data owners may request their withdrawal or blockage from any of the databases involved.

In addition, according to Provision 4/2009 of the National Directorate for Personal Data Protection (NDPDP) all marketing communications in Argentina must include:

- Information to recipients on their right to request their exclusion from the relevant database.
- The mechanism implemented by the sender to exercise such a right.
- Two legal transcriptions (in Spanish) stating the data subject's right to request the removal or blockage of the data subject's name from the database (*section 27, PDPL* and *section 27, DP Decree*).

Additionally, under the National Directorate for Personal Data Protection's (NDPDP) Disposition no. 10/08 unsolicited or non-consented communications must evidence their marketing nature in a noticeable manner. For e-mails, their subject field must read "Advertisement" and cannot include anything else.

INTERNATIONAL TRANSFER OF DATA

Transfer of data outside the jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

Section 12 of the Personal Data Protection Law 25,326 (PDPL) prohibits the transfer of personal data to countries that do not have an adequate level of protection in place. To date, the National Directorate for Personal Data Protection (NDPDP) and the Executive Branch of the Argentina Government has not determined which countries fall within this category. Therefore, all countries should be considered as being included within this prohibition.

The general prohibition to transfer personal data to other countries is equally applicable to international data transfers between companies of the same group.

In spite of the above, the Regulatory Decree 1558/2001 (DP Decree) provides that the prohibition is not applicable when the data subject has expressly consented to the transfer.

Data transfer agreements

21. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

Data transfer agreements are not contemplated expressly in the Argentine Data Protection Regulations (ADPR). However, there have been precedents of data transfer agreements being approved by the National Directorate for Personal Data Protection (NDPDP) and there is a specific form available to request the express approval of data transfer agreements.

The NDPDP has issued (within the framework of particular cases) guidelines regarding the minimum standards that data transfer agreements must comply with. This includes the need for the data importer to be subject to the ADPR.

22. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

Data transfer agreements are sufficient to legitimise the transfer of personal data to a foreign country, but only when the data is transferred exclusively for the purposes of processing (*section 25, Personal Data Protection Law 25,326* (PDPL)). In any case, for a data transfer agreement to legitimise the transfer, it must include a provision where the transferee undertakes to comply with the Argentine Data Protection Regulations (ADPR).

If the transfer of data was carried out for any purposes other than processing (*section 25 PDPL*), then the requirement of consent would apply and a data transfer agreement would not be sufficient to legitimise the transfer.

23. Does the relevant national regulator need to approve the data transfer agreement?

It is not necessary for the National Directorate for Personal Data Protection (NDPDP) to approve the data transfer agreement, but there is an optional procedure to approve it.

ENFORCEMENT AND SANCTIONS

24. What are the enforcement powers of the national regulator?

The National Directorate for Personal Data Protection (NDPDP) is empowered to adopt all necessary measures and take all actions in order to enforce the provisions of the legal framework governing data protection.

25. What are the sanctions and remedies for non-compliance with data protection laws?

Section 31 of the Personal Data Protection Law 25,326 (PDPL) provides that the National Directorate for Personal Data Protection (NDPDP) may apply sanctions for any violations of the Argentine Data Protection Regulations (ADPR). The sanctions can include, warnings, suspensions, fines ranging from AR$1,000 to AR$100,000 and closure or cancellation of the file, register or database, without prejudice to any applicable civil or criminal liabilities. In practice, there are precedents of the NDPDP applying fines to companies who fail to comply with the ADPR, although such fines are usually low.

Section 156 of the Criminal Code, states that penalties of between AR$1,500 and AR$90,000, plus suspension from six months to three years, can be imposed on employees who gain access to confidential information (the disclosure of which could generate damages) and disclose it without authorisation and/or legal or justified cause.

Section 117 of the Criminal Code provides that any person who knowingly supplies a third party with false information contained in any given personal data record will be imprisoned for a six-month to three-year period. The sentence may be increased to half the minimum sentence and half the maximum sentence, if any person suffers damage as a result.

Section 157 of the Criminal Code provides that imprisonment of between one month and two years may be imposed on any person who:

- Knowingly and unlawfully, or by violating data confidentiality and security systems, accesses a personal database.
- Unlawfully provides or discloses to third parties information registered in a personal database that should be kept confidential by provision of law.
- Unlawfully inserts data in a database.

Penalties imposed by sections 117 and 157 of the Criminal Code will be increased if the perpetrator is a public officer.

Practical Law Contributor Profiles

Maximiliano D'Auro, Partner

Estudio Beccar Varela
T +54 11 4379 6830
F +54 11 4379 6860
E mdauro@ebv.com.ar
W www.ebv.com.ar

Professional qualifications. Solicitor, Universidad Nacional de Mar del Plata, Argentina, 1997

Areas of practice. General commercial advice to companies; M&A; banking; anti-bribery and corruption; anti-money laundering; data protection.

Non-professional qualifications. LLM, London School of Economics, 2000

Recent transactions

- Working on many cross-border projects of global clients involving multi-jurisdictional data privacy issues (including broad data protection questionnaires; international transfer of personal data, migration or centralisation of data processing; e-mail monitoring and other employees' privacy issues; Internet regulation, on-line child protection and websites' potential liability).
- Representing a large global bank, obtaining the first ever resolution from the Argentine Data Protection authority allowing the local subsidiary of the bank to transfer personal data of its client to a global processing center located abroad. The Authority resolved that the agreement entered into between transferor and transferee afforded the transfer an "adequate level of protection", which made the transfer legal.

Languages. Spanish, English

Professional associations/memberships. Buenos Aires Bar Association; International Bar Association; ABA; AIJA.

Publications:

- *Protection of personal data in financial activities", Régimen jurídico de los datos personales, Tomo II Abeledo Perrot, Buenos Aires, 2014.*
- *"The implementation of the Nacional Registry of Data Bases", Jurisprudencia Argentina 2005-III-861.*
- *"Bank secrecy and the obligation to report suspicious transactions" La Ley, 25/6/2004.*
- *"The secrecy in the bill to amend the Anti-money laundering law", El Cronista, 3/4/2006.*
- *Latin America's giant leaps in the data privacy field (Data Protection Law & Policy, printed edition, Cecile Park, September 2011), (co-authored).*
- *"The legitimacy of workplace email monitoring in Argentina" (Data Protection Law & Policy, printed edition, Cecile Park, September 2010), (co-authored).*
- *"Qué deben hacer las firmas para cumplir con el Registro No Llame?" ("What must companies do to comply with the Don't Call Registry?", Article for iProfesional.com, 2010).*
- *"Third party content. Da Cunha Virginia c/Yahoo de Argentina SRL y Otro s/Daños y perjuicios" (E-Commerce Law Reports, printed edition, 2010), (co-authored).*
- *"Argentina strengthens opt-out regime" (Marketinglaw.co.uk, OsborneClarke, 2009), (co-authored).*
- *"General Overview of Personal Data Protection in Argentina" and "Argentine Rules on Direct Marketing" (both published in the global data protection online platform powered by Data Guidance, Argentine Chapter, 2009), (co-authored).*
- *"Court judgment against Yahoo and Google in Argentina" (E-Commerce Law Reports, 2009), (co-authored).*
- *"Violation of email becomes a criminal offense in Argentina" (Data Protection Law & Policy, printed edition, Cecile Park, 2008), (co-authored).*

Inés de Achaval, Associate

Estudio Beccar Varela
T +54 11 4379 4700
F +54 11 4379 6860
E ideachaval@ebv.com.ar
W www.ebv.com.ar

Professional qualifications. Solicitor, Universidad Torcuato Di Tella, 2012

Areas of practice. General commercial advice to companies; M&A; banking; data protection.

Languages. Spanish, English, French