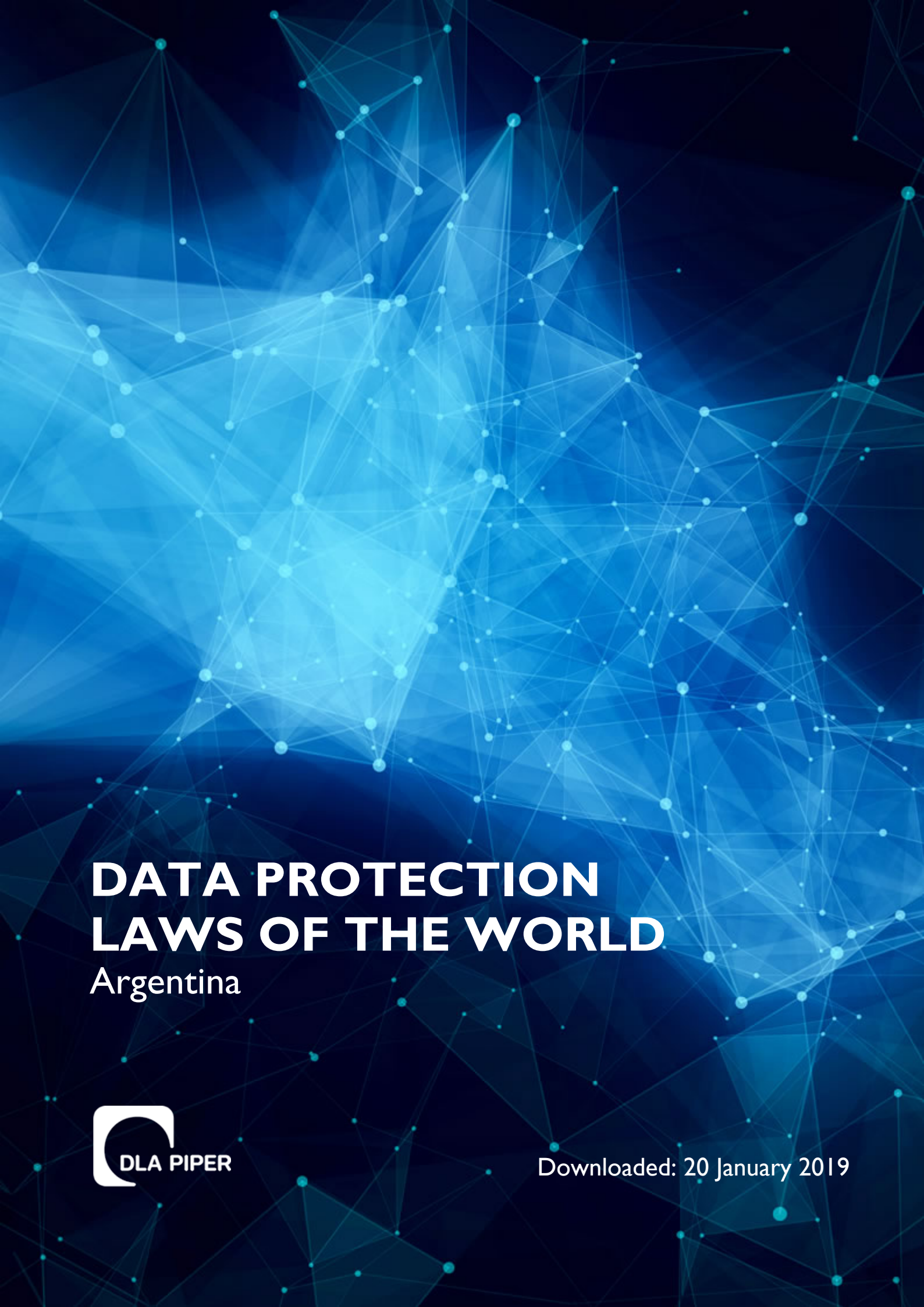

DATA PROTECTION LAWS OF THE WORLD

Argentina

DLA PIPER

ARGENTINA

Last modified 25 January 2017

LAW

Section 43 of the Federal Constitution grants citizens expeditious judicial action to gain access to information about them contained in public and private databases and to demand its amendment, updating, confidentiality, or suppression if it is incorrect.

Personal Data Protection Law Number 25,326 (the 'PDPL'), enacted in October 2000, provides much broader protection of personal data closely following Spain's data protection law. On 30 June 2003, the European Commission recognised that Argentina provides an 'adequate' level of protection of personal data, in line with the Data Protection Directive (95/46/EC).

DEFINITIONS

Definition of personal data

Personal information or data means *'any type of information related to identified or identifiable individuals or legal entities'*.

Definition of sensitive personal data

Sensitive information or data means *'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'*.

NATIONAL DATA PROTECTION AUTHORITY

Argentine Personal Data Protection Agency – in Spanish *Dirección Nacional de Protección de Datos Personales* (DNPDP)

Sarmiento 1118 – 5th Floor
Autonomous City of Buenos Aires
(C1041AAX) Argentina
T +54 11 4383 8512

http://www.jus.gov.ar/datos-personales.aspx

The DNPDP has enforcement power.

REGISTRATION

Any public or private database formed for the purpose of providing reports, any private database which is not formed exclusively for personal use, and any database formed for the purpose of transferring personal data must be registered with the DNPDP. The registration must include, at least, the following information:

- name and address of the data collector

- characteristics and purpose of the database
- nature of the data included in the database
- collection and update methods
- individuals or entities to which the data may be transferred
- methods for linking the recorded information
- methods used to ensure data security, including a detail of the people with access to information processing
- time during which the data will be stored, and
- conditions under which third parties can gain access to data related to them and the procedures performed to correct or update the data.

DATA PROTECTION OFFICERS

There is no requirement in Argentina for organizations to appoint a data protection officer.

However, a 'Head of Data Security' (*Responsible de Seguridad*) must be appointed by data controllers to which 'medium' or 'high' security requirements apply. Its duties are exclusively related to ensuring compliance with database security measures.

COLLECTION & PROCESSING

In general, data controllers may only collect and process personal data with the data subject's consent. Consent is *not required* if:

- the data is collected from a publicly accessible database, in the exercise of government duties, or as a result of a legal obligation
- the database is limited to certain basic information, such as name, ID, tax ID, job, birthdate and address
- the personal data derives from a scientific or professional contractual relationship and is used only in such context, or
- the information is provided by financial institutions, provided that they were required to do so by a court, the Central Bank or a tax authority.

When collecting personal data, the data collector shall expressly and clearly inform data subjects of:

- the purpose for which the data is being collected
- who may receive the data
- the existence of a database, the identity of the data collector and its mailing address
- the consequences of providing the data, of refusing to do so or of providing inaccurate information, and
- the data subject's access, rectification and suppression rights.

In addition, data contained in databases must be truthful, adequate, pertinent, and not excessive, be used exclusively for the purpose for which it was legally obtained and be deleted on completion of that purpose. Incomplete or partially or totally false data must be immediately amended or suppressed.

No person may be required to disclose sensitive personal data. Sensitive personal data may only be collected and processed in cases of public interest, as determined by law. Anonymised sensitive personal data may be collected for statistical or scientific

purposes, so long as the data subjects are no longer identifiable.

Data related to criminal history or background may only be collected by public authorities.

TRANSFER

The European Commission recognised Argentina as providing an adequate level of protection for personal data transferred from the European Community (Commission Decision C (2003) 1731 of 30 June 2003).

Personal data may only be transferred out of Argentina in compliance with legitimate interests of the transferring and receiving parties, and generally requires the prior consent of the data subject, which may be later revoked.

Consent to the transfer of personal data is not required when:

- the collection of the data did not require consent
- the transfer is made between government agencies in the exercise of their respective duties
- the data relates to health issues, and is used for emergencies, epidemiologic studies or other public health purposes, provided that the identity of the subject is protected, or
- the data have been de-identified such that they may no longer be linked with the corresponding subjects.

The transferee is subject to the same obligations as the transferor, and both parties are jointly and severally liable for any breach of data protection obligations.

Personal data may not be transferred to other countries or international institutions that do not provide an adequate level of protection, unless in cases of judicial or intelligence international cooperation, where Argentina has signed specific treaties with the relevant countries covering this issue, or in case of bank transfers or health issues (provided that the requirements set out above are complied with).

The adequate level of protection requirement may also be met by the parties including in the relevant agreement, data protection provisions similar to those contained in PDPL.

SECURITY

The data collector must take all technical and organisational measures necessary to ensure the security and confidentiality of the personal data, so as to avoid its alteration, loss, or unauthorised access or treatment. Such measures must permit the data collector to detect intentional and unintentional breaches of information, whether the risks arise from human action or the technical means used. It is prohibited to record personal data in databases which do not meet requirements of technical integrity and safety.

The level of security that must be provided varies in relation to the sensitivity of the personal data. Regulations distinguish between three possible levels of data security, based on the nature of the data stored in the database, and provide for minimum security requirements for each category.

BREACH NOTIFICATION

There are no requirements in the PDPL to report data security breaches or losses to the DNPDP or to data subjects. Nevertheless, all data incidents must be recorded by the data controller in a 'Security Incidents Ledger'. The DNPDP is entitled to request access to the Security Incidents Ledger when conducting an inspection. Notification may be necessary to mitigate potential violations in the event that the DNPDP starts an investigation and detects a security failure, which constitutes a violation of the data security obligations included in the PDPL.

ENFORCEMENT

The DNPDP is responsible for the enforcement of the data protection regime. Either acting ex officio or upon a complaint from a data subject, the National Ombudsman or consumer associations, the DNPDP is entitled to start an investigation when it suspects that the PDPL has been infringed. Administrative sanctions include warnings, suspension of the right to maintain a database, the imposition of monetary fines, ranging from AR$1,000 to AR$100,000 (approximately US$117 to US$11,700 as of January 2015), or the cancellation of the database.

In addition, data subjects may separately recover damages for violations of their data protection rights. The PDPL also modified the Argentine Criminal Code to include personal data crimes, such as knowingly inserting false information in a database, knowingly providing false information from a database, illegally accessing a restricted database, or revealing information contained in a database that the offender was in charge of keeping confidential. Criminal violations are subject to prison terms ranging from one month up to three years, which may be increased by 50% if any person suffers damage as a result of the crime.

ELECTRONIC MARKETING

The PDPL will apply to most digital marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be 'personal data' for the purposes of the PDPL). In all cases, the data subjects are entitled to exercise their access, amendment and deletion rights as provided in the PDPL.

In particular, the DNPDP's Disposition No. 4/2009 sets forth that:

- all promotional messages shall include the language from the PDPL's Section 27:3 and the third paragraph of Section 27 of Decree No. 1558/01 – which set forth a data subject's right to request suppression of their personal information from marketing databases
- all marketing emails not previously requested or consented to by the data subject shall include as their subject the single word *Publicidad* (promotional), and
- senders of promotional messages shall ensure that all mechanisms needed to honour the data subject's requests are in place.

On August 5, 2014, Law No. 26,951 was published in the Official Gazzette, creating the Argentine National Do Not Call Registry. The purpose of such registry is to protect telephone service users ('Users') from abuses by companies using such means to advertise, offer, sell or give non-requested goods and services ('Advertising Companies'). Users may opt to be included in the Registry for free. Advertising Companies, which will be regarded as data collectors under the PDPL and subject to their obligations, will not be allowed to call any registered User, and will need to, on a monthly basis, verify any updates of such list. The penalties for breaches and other enforcement regulations will be those provided in the PDPL. The application authority will be the DNPDP. The law must be implemented by a Decree, which should have be issued by November 3, 2014; however, as of January 6, 2014 the Decree has not yet been issued.

ONLINE PRIVACY

Argentina has not enacted specific legislation governing online privacy, nor has the PDPL issued regulations on this point.

Particularly with regard to automatic data collection programs, the current interpretation of most scholars is that information collected by 'cookies' or similar programs does not qualify as 'personal data' because such information corresponds to a device and not to the user him or herself.

KEY CONTACTS

Cordova Francos Gorbea D'Aiello Jofre ABOGADOS
www.cfgd.com.ar/

Sebastián Córdova-Moyano
Founding Partner
T +54 11 4311 3571
scordova@cfgd.com.ar

Felipe Oviedo Roscoe
Senior Associate
T +54 11 4311 3571
foviedo@cfgd.com.ar

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.