DATA PROTECTION LAWS OF THE WORLD

Argentina

DLA PIPER

ARGENTINA

Last modified 28 January 2024

LAW

Article 43 of the Federal Constitution, third paragraph, provides, in relevant part that any person may file an action to have access to personal data about such person and to information about the purpose with which they are kept, included in public data registries or banks, or in private data registries or banks, and to request the suppression, correction, confidentiality or updating of the data where inaccurate or discriminatory.

These provisions do not create an express constitutional right to privacy or data protection, but do create the basic framework for the protection of such right, as well as the foundation for the legislation, subsequently enacted, which regulates the details of that protection.

Law 25,326 - the Personal Data Protection Law (PDPL) includes the basic personal data rules. It follows international standards, and has been considered as granting adequate protection by the European Commission. Decree 1558 of 2001 includes regulations issued under the PDPL. Further regulations have been issued by the relevant agencies.

In November 2022, Argentina ratified Decision 108 of the Council of Europe, as amended, by means of Law 27,699.

DEFINITIONS

Definition of personal data

Personal data is defined as information of any type referred to individuals or legal entities, determined or which may be determined.

Definition of sensitive personal data

Sensitive data includes personal data which reveal racial or ethnic origin, political opinions, religious, philosophical or moral convictions, trade union affiliation and information related to health and sexual activities.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to Decree 746 of 2017, it is the Agency for Access to Public Information (Agencia de Acceso a la Información Pública).

REGISTRATION

All archives, registries, databases and data banks, whether public or private, having the purpose of supplying information, must be registered with the Registry organized by the national data protection authority. This registration requires the following information, to be provided to the registry:

- The name and domicile of the person responsible for the archive, registry, database or data bank
- The characteristics and purpose of the archive, registry, database or data bank
- The nature of the personal data included or to be included in the archive, registry, database or data bank
- The way in which data are collected and updated
- The destination of the data and the identity of the individuals or legal entities to whom such data may be transferred
- The way in which the recorded information is interrelated
- The means to assure the security of the data, indicating the category of persons with access to the processing of data
- The term during which the data will be preserved
- The way and conditions pursuant to which interested persons may have access to the data referring to such persons, and the procedures to be followed to rectify and update the registered data

DATA PROTECTION OFFICERS

Generally, there is no specific requirement to appoint a data protection officer. Under certain circumstances, in which special security standards apply, it may be necessary to appoint an officer in charge of data security.

COLLECTION & PROCESSING

Personal data collected for purposes of processing must be truthful, adequate, relevant and not excessive in relation with the scope and purpose for which they were obtained. The gathering of data shall not take place by unfair or fraudulent means or in an otherwise illegal manner.

Personal data may not be used for purposes different from or incompatible with those for which the personal data was initially collected. Personal data must be accurate and properly updated when necessary. Totally or partially inaccurate personal data, or those that are incomplete, shall be suppressed and substituted, or completed where relevant, by the person responsible for the archive or database, whenever such person becomes aware of the inaccurate or incomplete character of the information.

Consent from the data subject is required, which must be free, express and informed consent and in writing or in another equivalent form, unless:

- The personal data were obtained from sources open to unrestricted public access
- The personal data were obtained as part of the performance of state duties or in compliance with a legal obligation
- The personal data consists of lists whose data are limited to the name, national identity document number, tax or social security identification, occupation, date of birth and domicile
- The personal data are derived from a contractual, scientific or professional relationship and are necessary for such relationship
- The personal data result from operations conducted by financial entities with their clients or consist in the information such financial entities receive from their clients pursuant to the Financial Entities Law

When the authorization for the collection and processing of data is requested, the data subject must be informed about the purpose for which the data will be processed, as well as about the individuals or groups of individuals who will have access to the processed information. In addition, the archive, registry or data bank where the information will be kept must be identified, together with the person responsible for it. The data subject must be informed about the voluntary or compulsory nature of the

answers requested from such owner, as well as about the consequences of providing the personal data or of refusing to give such information or of providing untruthful information. The data subject must also be informed about the right to access, rectify and suppress the relevant data.

Special rules apply to sensitive data. No person may be required to disclose sensitive data. Sensitive data may only be collected and processed where necessary, and with consent, as expressly permitted by law, or for statistical or scientific purposes provided the person they refer to may not be identified.

Data related to criminal records may only be processed by the relevant public authorities.

TRANSFER

Transfers and disclosures to third parties

Personal data may only be transferred for legitimate purposes of the transferor and the transferee, and generally with the prior consent of the data subject who must be informed of the transfer’s purpose and of the transferee’s identity. This consent may be rescinded.

Consent is not required in the case of transfer of data regarding which consent was not necessary for collection. Also, it is not necessary in the case of transfer of data between state agencies, for purposes of performance of their respective activities, on in connection with health-related data, if the transfer is necessary for public health or emergency reasons, or for the performance of epidemiological studies, provided the identity of the persons to whom such data refer is reserved by means of adequate dissociation mechanism. In addition, consent is not necessary, for personal data generally, if an adequate dissociation mechanism is used in a way such that the data subjects are not identifiable.

Cross-border transfers

The cross-border transfer of personal data is prohibited to countries or international or supranational organization which do not provide adequate protection to such data, unless:

- The data subjects expressly consents to that transfer
- The transfer is necessary for international judicial cooperation
- The transfer takes place as part of certain exchanges of medical data
- Bank or stock exchange transfers, in the context banking or stock exchange transactions
- The transfer takes place as provided in the context of international treaties to which Argentina is a party
- The transfer has as its purpose the international cooperation between intelligence agencies engaged in combating organized crime, terrorism and drug traffic

SECURITY

The person responsible for a data archive, or using such archive, must adopt the technical and organizational measures to assure the security and confidentiality of personal data, so as to avoid their adulteration, loss, consultation or non-authorized processing, and to detect the misuse of information. The recording of personal data in archives, registries or data banks that do not comply with the legal requirements on integrity and security is prohibited.

BREACH NOTIFICATION

Not specifically required under data protection law.

Failure to notify a data security breach is not in itself a violation of the data protection regime, but may bear on the effects of security violation, especially if lack of such notification results in other security breaches or damages. The person responsible for the data must keep records on security breaches, and these records may be requested by the data protection authority.

Breach notification may be mandatory if the data protection authority specifically requests information about data breaches.

ENFORCEMENT

There are several enforcement mechanisms:

- The data protection authority may enforce the legal provisions and regulations on data protection, imposing fines in case of violation.
- Violation of data protection rules may constitute a crime subject to prison terms imposed by criminal courts.
- Court actions may be brought to have access to personal data and to request their correction, suppression, confidentiality or updating.

ELECTRONIC MARKETING

Electronic marketing, to the extent that it may involve processing of personal data, is subject to the general rules applicable to such data, such as valid data subject consent, adequate privacy notices as to use and disclosure of personal data and data subject rights.

ONLINE PRIVACY

Although there are no detailed regulations on online privacy, the general rules on privacy provided by the Civil and Commercial Code are applicable in this context. Nuisances from unrequested communications may be actionable. Unauthorized collection of personal data will be subject to the general rules applicable to such data.

KEY CONTACTS

Guillermo Cabanellas
Senior Partner
T +5411 41145500
g.cabanellas@dlapiper.ar

DATA PRIVACY TOOL

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