INTERNATIONAL LAWYERS NETWORK

2024 ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com

ILN Cybersecurity & Data Privacy Group and ILN Technology Media & Telecommunications Group

Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

Each contributing law firm is the owner of the copyright in its contribution. All rights reserved.

About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, and 2023 they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

Authors of this guide:

1. Cybersecurity & Data Privacy Group

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

2. Technology, Media & Telecom (TMT)

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.

www.iln.com

Argentina

In Argentina, data protection is governed by comprehensive legislation aimed at safeguarding individuals' personal data. Below you will find an outline of the key aspects including governing legislation, exploring their scope of application, requirements for data processing, rights and duties of data providers/principals, processing of children's data, regulatory authorities, and consequences of non-compliance.

Governing Data Protection Legislation

1.1. Overview of Principal Legislation

Data protection in Argentina is primarily regulated by the right to Habeas Data. This right can be found on Art. 43 of the Argentine Constitution of 1994. Although this right is enshrined in the Constitution, the implementation of protection to the personal data is regulated by the Personal Data Protection Law No. 25,326 ("Ley de Protección de Datos Personales", hereinafter "PDPL"), enacted in 2000. The PDPL is the cornerstone of Argentina's data protection regime. It aims to strike a balance between the free flow of information and individuals' right to privacy. This legislation imposes strict obligations on data controllers and data processors while affording data subjects various rights. This legislation establishes the fundamental principles and requirements for the processing of personal data in the country. It aligns with international data protection standards and provides a strong legal framework for data protection

1.2 Additional or Ancillary Regulation, Directives, or Norms

Complementing the principal legislation, several regulations and guidelines further detail data protection requirements. Notably, the Argentine Data Protection Authority ("Agencia de Acceso a la Información Pública", hereinafter "AAIP"), the regulatory body responsible for enforcing data protection laws in Argentina, issues resolutions and guidelines to clarify specific aspects of data protection, ensuring consistent compliance across various sectors and industries

Contact Us

+54 11 5278 5280

https://syls.com.ar/

jmca@syls.com.ar

Arroyo 880, 2º Piso
Buenos Aires, C1007AAB Argentina

and providing further clarity of the PDPL, especially with newer technologies. These directives help organizations understand their obligations and best practices regarding data protection.

Scope of Application

2.1 Legislative Scope

2.1.1.Definition of Personal Data

The PDPL has a broad scope of application, covering the processing of personal data within the country's borders. The PDPL discriminates on article 2 the different type of personal data that can be found and defines each one of them. Broadly, personal data is defined as encompassing any information that allows the identification of an individual or makes them identifiable. This definition includes both direct and indirect identification criteria. Some of the law's definition of personal data encompasses a wide range of information, including but not limited to names, identification numbers, addresses, and even electronic identifiers.

2.1.2 Definition of Different Categories of Personal Data

PDPL recognizes various categories of personal data, acknowledging that sensitive data, such as health records or biometric information, require special protection. Sensitive data, pertains to personal information that discloses details such as racial or ethnic origin, political beliefs, religious or

philosophical affiliations, moral convictions, union memberships, or data concerning one's health or sexual life. The terms 'file,' 'record,' 'database,' or 'data bank' are used interchangeably to describe organized sets of personal data subject to processing, whether electronically or otherwise, regardless of how they are created, stored, organized, or accessed.

2.1.3. Treatment of Data and Its Different Categories

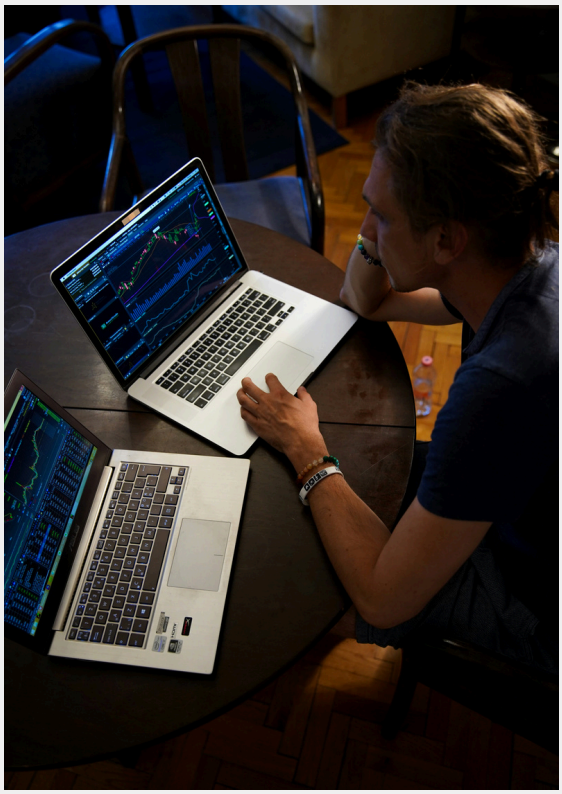
The PDPL regulates the processing of both personal and non-personal data, ensuring that the principles of data protection apply universally. Additionally, it outlines key definitions crucial for data processing, ensuring clarity and consistency. Data processing refers to systematic operations and procedures, electronic or not, involved in collecting, preserving, ordering, storing, modifying, correlating, evaluating, blocking, destroying, or generally managing personal data, including their transfer to third parties through various means. Regarding this definition, it addresses electronic and non-electronic data, adapting to evolving technological landscapes.

2.1.4. Other Key Definitions Pertaining to Data and Its Processing

The legislation provides key definitions related to data processing, such as data controller and data processor, ensuring clarity in roles and responsibilities within data processing activities. Computerized data pertains to personal information subjected to electronic or automated processing. Data disassociation involves processing personal data in a manner that renders the information obtained incapable of being linked to a specific or identifiable individual.

Statutory Exemptions

The PDPL allows for exemptions in specific situations, such as when data processing is required by law or necessary for the performance of a contract such as data processed for journalistic, artistic, or literary purposes, domestic activities or used for public security or defense. These exemptions must align with the PDPL's overarching principles and respect individuals' rights.



3.1. Territorial and Extra-Territorial Application

The PDPL applies within Argentina's territory and extends to data processing activities that have an extraterritorial impact when data controllers or processors outside Argentina process the personal data of Argentine residents.

Legislative Framework

4.1. Key Stakeholders

- **Data Controller:** Individual or legal entity, whether public or private, who is the owner of a file, record, database, or data bank.
- **Data Processor**: Entities or individuals that process data on behalf of the data controller.
- **Data Subject:** The individual to whom the personal data belongs and is being processed.

4.2 Role and Responsibilities of Key Stakeholders

The PDPL assigns specific responsibilities to each stakeholder, emphasizing the data controller's duty to inform data subjects, obtain consent, and ensure data security. Data Controllers in Argentina must ensure compliance with the PDPPL, obtain explicit consent for data processing, and protect data subjects' rights. They are responsible for notifying data subjects about the purpose and scope of data processing. Moreover, they must register with the AAIP as data controllers as well as any database containing personal data, whether public or private.

https://syls.com.ar/

Data Processors are required to process data strictly in accordance with the instructions provided by the Data Controller. They must also implement robust data security measures to protect the data they handle.

Data subjects in Argentina have various rights, including the right to access their data, rectify inaccuracies, and request data erasure when necessary.

Requirements for Data Processing

5.1. Grounds for Collection and Processing

Data processing must be based on lawful grounds, including consent, contractual necessity, legal obligations, vital interests, or legitimate interests pursued by the data controller. Data processing often requires the explicit and informed consent of the data subject. Consent notices should clearly outline the purpose of data processing, and data subjects have the right to withdraw their consent at any time. Consent is a fundamental requirement, and individuals have the right to withdraw it at any time.

5.2. Data Storage and Retention Timelines

The PDPL requires data controllers to establish retention periods that align with the purpose of data processing. Data storage and retention timelines are defined in accordance with the purpose for which the data was

collected. Argentina's regulations specify maximum periods for data retention and the conditions under which data can be retained.

5.3. Data Correction, Completion, Update, or Erasure of Data

Individuals have the right to request corrections or erasure of inaccurate or outdated data concerning them. Data controllers are obligated to respond to such requests promptly.

5.4. Data Protection and Security Practices and Procedures

Data protection and security practices are of paramount importance. Data controllers and processors are required to implement security measures to protect personal data from unauthorized access, disclosure, alteration, or destruction. Some examples of these security measures are encryption, access controls, and regular audits to protect personal data from breaches. These measures must be commensurate with the sensitivity of the data being processed.

5.5 Disclosure, Sharing, and Transfer of Data

Transfers of personal data to third parties require data subject consent or a legal basis.

Cross-border data transfers

must adhere to data protection regulations and, in certain cases, require authorization from the AAIP, as further discussed below.

5.6. Cross-Border Transfer of Data

Cross-border data transfers are subject to specific rules and safeguards, which are in line with international data protection standards.

On January 15, 2024, the European Commission ("Commission") published its findings regarding the first review of adequacy decisions made under Article 25(6) of Directive 95/46/EC ("Directive") in 1995. In these decisions, the Commission had determined that eleven countries or territories, including Argentina, ensured an adequate level of personal data protection, allowing for the free transfer of data from the European Union (EU) to these countries or territories. With the entry into force of the EU General Data Protection Regulation (GDPR) in 2018, it was established that adequacy decisions made under the Directive would remain in effect but would be subject to review every four years. In this first review, the Commission found that the data protection frameworks in the countries and territories under review had evolved, including through legislative reforms and regulations by data protection authorities

Regarding Argentina, the Commission emphasized the importance of the independence of the AAIP as the supervisory authority and the ratification of Convention 108+ in 2023. Additionally, it noted that a draft Data Protection Bill introduced in Congress and still subject to review could further strengthen the data protection framework in the country. As a result of its findings, the European Commission concluded that personal data transferred from the European Union to Argentina benefits from adequate protection guarantees. Consequently, such data can continue to flow freely from the EU to Argentina, maintaining the country's position at the forefront of personal data protection and facilitating greater efficiency and security in international operations.

5.7. Grievance Redressal

The PDPL mandates the establishment of grievance redressal mechanisms, enabling data subjects to exercise their rights and seek remedies in cases of non-compliance.

Rights and Duties of Data Providers/Principals

6.1. Rights and Remedies

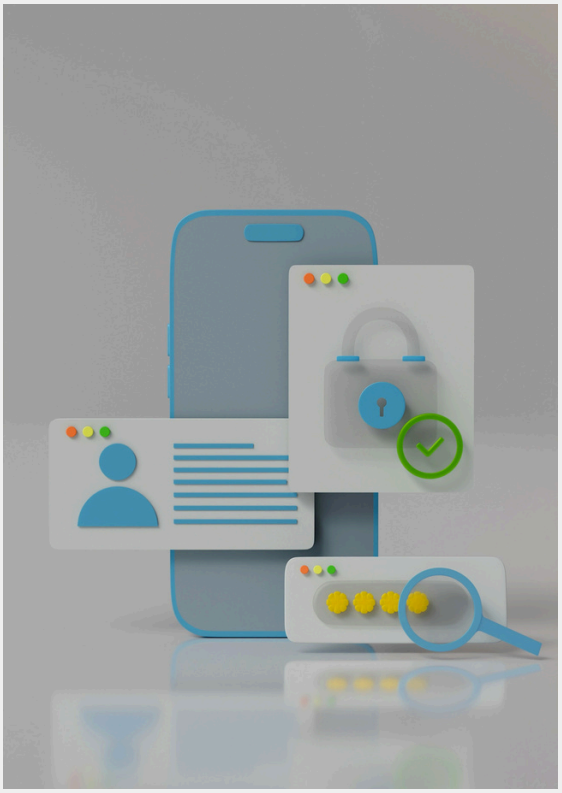
- **Right to Withdraw Consent**: Individuals have the right to withdraw their consent for data processing at any time.
- **Right to Grievance Redressal and Appeal:** Data subjects can file complaints with the Data Protection Authority and seek judicial remedies.

- **Right to Access Information (Habeas Data):** Art. 43 of the Argentine Constitution grants individuals the right to access, update, or delete personal data held about them.

- **Right to Nominate:** Individuals can nominate a representative to exercise their data protection rights.

6.2. Duties

Data controllers and processors are duty-bound to provide accurate information, report changes and respect the rights and privacy of others in accordance with Argentina's data protection regulations.



Processing of Children or Minors' Data

The PDPL places special emphasis on protecting the data of children and minors, requiring parental consent for data processing activities involving minors.

Regulatory Authorities

8.1. Overview of Relevant Statutory Authorities

The AAIP is the regulatory authority responsible for enforcing the PDPL, and has the power to issue resolutions and guidelines to clarify specific aspects of data protection and keep the data protection regulation updated to upcoming technologies.

8.2. Role, Functions, and Powers of Authorities

The AAIP plays a crucial role in overseeing compliance with data protection regulations. It is tasked with monitoring compliance, investigating data breaches, and issuing penalties for violations.

8.3. Role, Functions, and Powers of Civil/Criminal Courts in the Field of Data Regulation

Civil and criminal courts can be involved in data protection cases, particularly when individuals seek

legal remedies for data breaches or non-compliance with data protection laws.

Consequences of Non-Compliance

9.1. Consequences and Penalties for Data Breach

Data controllers and processors in Argentina face significant penalties and consequences for data breaches, including fines and mandatory notifications to affected data subjects. Non-compliance with data protection laws, including data breaches, can result in severe penalties, including fines, suspension of data processing activities, or data controller disqualification. The PDPL modifies some of Argentina's criminal laws (article 117 bis and 157 bis of National Penal Code) to include cases in which data controllers and processors are punished for Data breaches and Non-Compliance.

9.2. Consequences and Penalties for Other Violations and Non-Compliance

Violations of other provisions of data protection laws may also lead to penalties, depending on the severity of the violation.

Contact Us

+54 11 5278 5280

https://syls.com.ar/

jmca@syls.com.ar

Arroyo 880, 2º Piso
Buenos Aires, C1007AAB Argentina