Global Data and Cyber Handbook - Argentina

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What's new?

## Recently Updated Topics

This chapter was reviewed and updated on 2 December 2024.

There have been no material developments in data privacy and cybersecurity in Argentina. The Personal Data Protection Bill of Law introduced in Congress by the former National Executive Branch has not been approved.

We highlight the following points:

In January 2024, the European Commission published its conclusions from the first review of the adequacy decisions adopted in 1995, determining that Argentina, among others, guarantees an adequate level of protection.

Several discussions on artificial intelligence are taking place at both public and private levels, with certain non-binding regulations enacted during 2023 and 2024.

# Key Data & Cyber Contacts

# Key Data & Cybersecurity Laws

## How are data and cybersecurity laws/regulations implemented?

*Last reviewed: 2 December 2024*

☒     omnibus – all personal data

☒     sector-specific — e.g., financial institutions, governmental bodies

☒     constitutional

## What are the key data privacy laws and regulations?

*Last reviewed: 2 December 2024*

[Personal Data Protection Law No. 25,326](http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm)

[Personal Data Protection Regulatory Decree No. 1558/2001](http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/texact.htm)

[Access to Public Information Law No. 27,275](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=265949)

[Access to Public Information Regulatory Decree No. 206/2017](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=273023)

[International Personal Data Transfer Disposition No. 60-E/2016](http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm)

[Resolution 159/2018 on Binding Corporate Rules](http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/317228/norma.htm)

[Resolution No. 47/2018, which sets forth the recommended security measures for the processing and retention of personal data in computerized and non-computerized media](http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/312662/norma.htm)

[Resolution No. 4/2019, which provides interpretation guidelines of Personal Data Protection Law No. 25,326](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=318874)

[Resolution No. 332/2020, which approves legal and technical guidelines related to audits conducted by the Data Protection Authority](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=345895)

[Resolution No. 126/2024, which contemplates a new classification of infringements and sanctions regime applicable to breaches of Laws 25,326 (data protection) and 26,951 (do not call registry)](https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=399750)

[Convention 108+ on the Protection of Individuals with regard to Automatic Processing of Personal Data (approved by Law No. 27,699)](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=375738)

[Resolution No. 255/2022 on Genetic Data](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=376740)

[Law 26,951 on National Do Not Call Registry](http://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/233066/texact.htm)

[Resolution No. 198/2023 on New Standard Contractual Clauses for International Personal Data Transfers of the Ibero-American Data Protection Network](http://servicios.infoleg.gob.ar/infolegInternet/anexos/390000-394999/391538/norma.htm)

## What are the key cybersecurity laws and regulations?

*Last reviewed: 2 December 2024*

[Personal Data Protection Law No. 25,326](http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm)

[Personal Data Protection Regulatory Decree No. 1558/2001](http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/texact.htm)

[Disposition No. 47/2018](http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/312662/norma.htm)

[Resolution No. 332/2020](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=345895)

[Law No. 26,904 (Grooming).](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=223586)

[Law No. 24,766 (Confidential Information)](http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41094/norma.htm)

[Law No. 26,388 (Criminal penalties for unauthorized access to information)](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do;jsessionid=00D701C14EA856A456AABA9DCA283A29?id=141790)

[Executive Order No. 577/2017 (creates the Cybersecurity Committee)](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=277518)

[Resolution No. E-1107/2017 (creates the Response to Security Incidents Committee)](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=281854)

[Resolution No. 829/2019 (approves the National Cybersecurity Strategy)](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=323594)

[Decision No. 641/2021 (approves the "Minimum Information Security Requirements for National Public Sector Organizations")](https://www.boletinoficial.gob.ar/detalleAviso/primera/246104/20210628)

[Disposition No. 7/2021 (creates the Registry of Focal Points in Cybersecurity of the National Public Sector)](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=353181)

[Disposition No. 8/2021 (approves the "Introductory Guide to Security for the Development of Web Applications)](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=356582)

[Law No. 25,506 on Digital Signatures](https://www.argentina.gob.ar/normativa/nacional/ley-25506-70749)

[Digital Signatures Regulatory Decree No. 2628/2002](https://www.argentina.gob.ar/normativa/nacional/decreto-2628-2002-80733)

[Resolution No. 141/2019 (Presidency of the Cybersecurity Committee)](https://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/323038/norma.htm)

[Resolution No. 44/2023 (Second National Cybersecurity Strategy)](https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904)

[Communication A 7724 of the Argentine Central Bank](https://www.bcra.gob.ar/Pdfs/comytexord/A7724.pdf)

[Executive Order No. 614/2024, which creates the federal cybersecurity agency within the state intelligence secretariat](https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=401512)

## What are the key laws and regulations relating to non-personal data?

*Last review date: 2 December 2024*

[Resolution No. 4/2019, which provides interpretation guidelines of Personal Data Protection Law No. 25,326](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=318874) (which defines when personal data is no longer considered as such, among others)

[Law No. 24,766 (Confidential Information)](http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41094/norma.htm)

[Access to Public Information Law No. 27,275](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=265949)

[Access to Public Information Regulatory Decree No. 206/2017](http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=273023)

## Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last reviewed: 2 December 2024*

**No**

The National Executive Branch introduced the Personal Data Protection Bill of Law in Congress. It proposes significant amendments to the current regime and introduces mandatory provisions that are novel to Argentine legislation. The Bill of Law includes references to its extraterritorial application in certain cases, an expanded definition of sensitive data, mandatory reporting obligations of certain security incidents, and will recognize legitimate interest as a legal basis for the processing of personal data, among other changes to the current regime  However, there are no expectations for this Bill to be approved.

Although the legislative process to incorporate Convention 108+ (on the Protection of Individuals with regard to Automatic Processing of Personal Data) into local legislation has been completed, the Convention is not yet in force.

# Regulators, Enforcement Priorities and Penalties

## Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last reviewed: 2 December 2024*

The main local regulator is the Agency for Access to Public Information (*Agencia de Acceso a la Información Pública*), which is the current DPA. The other regulator is the Federal Cybersecurity Agency.

## How active is each of the regulator(s)?

*Last reviewed: 2 December 2024*

☒ Moderately active

## What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last reviewed: 2 December 2024*

The DPA approved the Strategic Plan for the period 2022-2026 ("**Plan**") via Resolution No. 94/2023, which sets forth these main objectives:

Promote and strengthen the exercise of the right to the protection of personal data and access to public information.

Expand regulatory and management powers (seeking to update and strengthen regulations and improve information management capacities).

Promote transparency in public management and citizen participation by bringing the state closer to its citizens.

Expand and strengthen the institutional powers of the DPA.

The Plan will undergo an annual review to evaluate its progress and make any necessary adjustments.

It is anticipated that the DPA will continue in its efforts to extend its jurisdiction and enforce Argentine law on foreign entities processing personal data of data subjects residing in Argentina.

## What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: 2 December 2024*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

☒         Staying the same

Class actions/group actions under data or cyber regulation are:

☒         Rare

## What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last reviewed: 2 December 2024*

There are:

☒       administrative remedies /civil penalties applied by regulators and law enforcement

The administrative remedies for damages arising from non-compliance with key data privacy and cybersecurity laws include warnings, suspensions, fines from ARS 1,000 to ARS 100,000, and closure or cancellation of the files, registers or database.

DPA’s Resolution No. 126/2024 unifies the sanctions regime of Personal Data Protection Law No. 25,326 and National Do Not Call Registry Law No. 26,951. It seeks to systematize, in a single rule, the diverse regulations in the various dispositions and resolutions that constitute the sanctions regime.

In this sense, the Resolution raised the maximum limits for applicable fines when a condemnatory administrative act includes more than one pecuniary sanction for an identical punishable action within each of the levels of the "graduation of sanctions." It provides a maximum limit for the total amount of the fine for such conduct equivalent to the maximum of the scale according to the seriousness of the infringements committed, multiplied by 500.

☒       criminal penalties from regulators and law enforcement

Pursuant to Personal Data Protection Law No. 25,326, certain data protection infringements are considered criminal offenses:

Knowingly providing to a third-party false data stored in a database (punished by a six-month to three-year imprisonment).

When a person is harmed as a result of the offense, the minimum and maximum punishments specified above will be increased by 50% (e.g., where a person is harmed by an offender knowingly providing to a third-party false data stored in a database, the offender will be punished by imprisonment for three months to 1.5 years).

When the infringer is a public officer in the exercise of their duties, an accessory penalty consisting of disqualification to serve as a public officer will be applied. The penalty will be doubled if the public officer:

Knowingly and unlawfully, or violating data confidentiality and data security systems, accesses, in any way, a personal database (punishable by a one-month to two-year imprisonment).

Discloses to a third party any information registered in a database that should be kept secret by law (punishable by a one-month to two-year imprisonment).

Unlawfully introduces or modifies data in a database (punished by a one-month to two-year imprisonment).

In the event that the infringer is a public officer, an accessory penalty resulting in a special disqualification for one to four years will be imposed.

☒       private remedies

Individual personal action (*i.e.*, a claim). In any event, damages must be evidenced.

## If data subjects have private remedies, what form can these remedies take?

*Last reviewed: 2 December 2024*

☒       individual personal actions

☒       representative actions (e.g., brought by a consumer / data privacy body or the supervisory authority)

☒       class actions

# Key Definitions

## Personal data

*Last reviewed: 2 December 2024*

Personal data is defined as information of any kind relating to an identified or identifiable individual or legal entity.

## Sensitive/special personal data (including personal data subject to additional protections/ restrictions/breach notification obligations)

*Last reviewed: 2 December 2024*

Sensitive data includes:

☒       personal data revealing racial or ethnic origin
☒       personal data revealing political opinions
☒       personal data revealing religious or philosophical belief
☒       personal data revealing trade / professional union or association membership
☒       data concerning health/medical information
☒       data concerning a natural person's sex life or sexual orientation
☒       personal data regarding an individual's criminal convictions or record
☒       other

Under DPA Resolution No. 4/2019, biometric data identifying an individual will be considered sensitive data only when it can reveal additional information on the data subject that may result in the discrimination of the data subject (*e.g.*, data revealing ethnic origin). The same approach is followed for genetic data (Resolution No. 255/2022).

## Controller vs Processor

*Last reviewed: 2 December 2024*

**Do the privacy laws distinguish between controllers/owners and processors/agents? Whereby:**

The controller/owner is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

The processor/agent is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

**Yes**

Although not expressly defined as in the GDPR, Personal Data Protection Law No. 25,326 includes provisions related to data processing services and distinguishes between "one having responsibility of the database" and the "user of the data."

# Territorial Scope

## What is the territorial reach of the data privacy and cybersecurity laws?

*Last reviewed: 2 December 2024*

☒       applies to organizations located in the jurisdiction
☒       other

Despite the wording of Personal Data Protection Law No. 25,326, which in general appears to limit its application within Argentina, in practice the DPA issued regulations aiming to expand its jurisdiction and application to foreign entities processing personal data of data subjects residing in Argentina.

In addition, the DPA has issued an online registration form to enable foreign individuals and legal entities that are not established in Argentina but that process personal data of Argentine residents to register themselves as "responsible for databases."

# Legal Bases for Processing of Personal Data

## Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last reviewed: 2 December 2024*

**Yes**

The following are potential legal bases for processing personal data:

☒       the data subject has provided consent to the processing for the identified purposes
☒       the personal data is necessary to perform a contract with the data subject
☒       the personal data is necessary to comply with a legal obligation
☒       other

Personal data is obtained from unrestricted public access sources

Personal data is collected for the performance of the duties inherent to the powers of the State

Personal data is limited to the name, ID number, tax or social security ID number, profession, date of birth and domicile

Personal data is collected by financial entities in connection with transactions performed by customers of the referred entities

## Is an identified legal basis required in order to collect or process sensitive personal data?

*Last reviewed: 2 December 2024*

Yes

The following are potential legal bases for processing special categories of personal data:

☒       the data subject has given consent to the processing, where consent is measured to the same standard as non-sensitive personal data
☒       processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
☒       processing is necessary for reasons of substantial public interest
☒       processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
☒       processing is necessary for reasons of public interest in the area of public health
☒       processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
☒       other

If the processing is for statistic or scientific purposes and data subjects cannot be identified

## Are there special requirements that apply to the collection or processing of personal data from minors?

*Last reviewed: 2 December 2024*

**Yes**

Under local regulations, a *minor* is a person below the age of 18. However, the "*progressive capacity theory*" included in the Civil and Commercial Code considers that minors are more prepared to make legal decisions based on their age and level of maturity (which must be analyzed on a case-by-case basis). Additionally, DPA's Resolution No. 4/2019 contemplates that it would be reasonable to conclude, in principle, that minors between 13 and 17 years old may provide their consent for the processing of their personal data.

## In what circumstances do these special requirements apply?

*Last reviewed: 2 December 2024*

☒       generally

## What are the special requirements that apply to collecting or processing personal data from minors?

*Last reviewed: 2 December 2024*

☒       consent must be given or authorized by the holder of parental responsibility over the child
☒       additional data security requirements apply

When consent is granted by the parent/guardian of the minor, the individual or entity responsible for the database must perform reasonable efforts to verify that consent was actually granted by the parent/guardian of the minor.

☒       other

DPA's Disposition No. 18/2015 sets forth certain recommendations when processing minors' personal data, such as: limiting to the maximum extent possible the type and amount of information collected about them, implementing robust security measures on the collected information, and avoiding sharing minors' personal information with third parties.

Further, DPA's Resolution No. 332/2020 provides that during an inspection, the DPA will consider whether the individual or entity responsible for the database has obtained minors' consent with the authorization of their parents and/or legal guardians or if such consent has been obtained taking into account the minor’s progressive capacity.

# Information Requirements, Data Subject Rights, Accountability and Governance

## What information needs to be included in a privacy notice to data subjects?

*Last reviewed: 2 December 2024*

☒       the identity and the contact details of the controller and, where applicable, of the controller's representative
☒       the purposes of the processing for which the personal data is intended
☒       the recipients or categories of recipients of the personal data, if any
☒       the existence of data subjects' rights, such as the right to access, rectification, erasure, data portability, etc.
☒       the right to lodge a complaint with a supervisory authority
☒       whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
☒       other

The existence of any relevant file, record, electronic database or database of any other kind and the identity and domicile of the individual or entity having responsibility over the database

The procedure for data subjects to exercise their rights

Consequences for providing inaccurate personal data

Moreover, DPA's Disposition No. 18/2015, which approves the "Guidelines on good privacy practices for the development of applications," recommends, among other things, clearly indicating the data protection principles applicable to the data processing, any transfer of personal data, any data processing service and any information related to the Data Protection Officer.

Although not expressly envisaged by Personal Data Protection Law No. 25,326, it is best practice (and a clear expectation of the DPA) to inform data subjects of the categories of personal data that will be collected/processed and to provide information on assignments and cross-border data transfers.

## Do data subjects have specific privacy rights that must be operationalized?

*Last reviewed: 2 December 2024*

**☒ Yes**

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

☒       right to access the data subject's own personal data
☒       right to rectify/correct the data subject's own personal data where inaccurate or incomplete
☒       right to erasure of personal data
☒       right to withdraw consent
☒       other

Right to information, defined as the ability of the data subject to request information from the DPA on the existence of databases, their purposes and the identity of those having responsibility over the databases

Right to access, rectify or erase personal data collected through video surveillance systems

Right to request an explanation of an automated-decision making

Right to opt out from marketing communications

## Are there accountability and governance requirements?

*Last reviewed: 2 December 2024*

There are accountability and governance requirements to:

☒       maintain a record of processing activities
☒       implement appropriate measures to comply with data privacy and cybersecurity
☒       demonstrate compliance with data privacy and cybersecurity

The remaining requirements (*e.g.*, privacy by default and design, DPIAs, appointing local representatives in the jurisdiction) are included under certain guidelines, resolutions or dispositions of the DPA and the Draft Bill.

# DPOs and Notification Requirements

## Is the concept of data protection officer (DPO) recognized in the jurisdiction?

*Last reviewed: 2 December 2024*

**No**

However, there are certain non-mandatory guidelines that refer to this matter. Based on such guidelines, it would be reasonable to conclude that appointing a DPO would be considered as good practice by the DPA, and thus doing so is highly recommended (although the concept of DPO is not expressly recognized and its appointment is not mandatory). That said, the  Personal Data Protection Bill of Law introduced in Congress contemplates such figure or a similar one.

## Are there circumstances in which it is mandatory to appoint a DPO or similar position?

*Last reviewed: 2 December 2024*

**No**

If yes, under what circumstances?

N/A

## Where a DPO is appointed, does the DPO have to meet specific requirements?

*Last reviewed: 2 December 2024*

If yes, what are these requirements?

The Personal Data Protection Bill of Law introduced in Congress provides that the DPO or a similar position must meet the following requirements: suitability, capacity, and specific knowledge for the performance of their duties. The DPO or a similar role may be filled by an employee or a third party.

## Are there obligations to notify, submit filings to, register with or obtain approval from local data protection authorities to collect and/or process personal data generally?

*Last reviewed: 2 December 2024*

**Yes**

The DPA issued Resolution No. 132/2018, which sets forth a mechanism for the registration of those responsible for databases and the existence of their databases before the National Registry of Databases created by the DPA. Such registration requires no annual renewal. However, any significant changes should be reported to the DPA.

Moreover, the DPA has issued an online registration form to enable foreign individuals and legal entities – not established in Argentina but that process personal data of Argentine citizens – to register themselves as "responsible for databases." However, such form is not yet available at this point.

# Data Processors

## Are there obligations for controllers to establish controls with respect to data processors?

*Last reviewed: 2 December 2024*

The obligations are as follows:

 ☒       controllers must only use processors subject to a written agreement that complies with specific requirements

## Are there any direct regulatory or statutory requirements on processors?

*Last reviewed: 2 December 2024*

**Yes**

Personal Data Protection Law No. 25,326 sets forth, among other things, these obligations for data processors:

Adopt all technical and organizational measures necessary to ensure the security and confidentiality of personal data, preventing such data from being modified, lost, probed or processed without authorization, and enabling the detection of any information deviation, whether intentional or not, whether risks arise from a human act or from the technical means in use

Comply with the professional secrecy duty regarding the personal data (such duty must subsist even after the termination of the relationship between the parties)

To act only upon the instructions of the data controller

# International Data Transfer

## Are there restrictions on the transfer of personal data to third countries?

*Last reviewed: 2 December 2024*

**Yes**

A third country means a jurisdiction different from Argentina.

Transfers of personal data to third countries are only permissible if there is a legal basis for the processing/transfer and one of the following applies:

☒       approved adequate/whitelisted jurisdictions
☒       approved standard contractual clauses
☒       binding corporate rules
☒       derogations, such as consent, contract performance, necessity to establish, exercise or defend legal claims
☒       other solutions

***Please see separate question for information on data localization provisions that are not restricted to personal data.***

For instance, Data Transfer Agreements differ from the controller-to-controller and controller-to-processor models issued by the DPA and do not observe the principles, guarantees and content of such models. In such cases, these should be filed with the DPA for approval. The same approach should be followed when using corporate rules that do not comply with the guidelines and principles issued by the DPA.

# Cookies, Online Tracking and Direct Marketing

## Are there specific requirements for the use of cookies and other online tracking technologies?

*Last reviewed: 2 December 2024*

**Yes**

Under Personal Data Protection Law No. 25,326, the personal data required to establish certain profiles for promotion, business or advertising purposes can only be obtained if it is included in documents available to the public, provided by data subjects or obtained with their consent. However, Decree No. 1558/2001 sets forth that personal data may be collected, processed and transferred for advertising purposes without the data subject's consent when it is intended for the formation of specific profiles, which categorize similar preferences and behaviors of the data subjects, provided that data subjects are only identified by their belonging to generic groups.

It has been said that these particular provisions of the Decree, which alter the spirit of Law No. 25,326, have been passed as a result of a strong lobby conducted by marketers developing activities in Argentina. There is visible uncertainty under local data protection regulations as to whether companies are required to obtain express consent from data subjects before sending them direct marketing communications. While some scholars are of the opinion that express consent is required, others take the view that such consent can be avoided.

Additionally, DPA's Disposition No. 4/2009 related to advertising expressly sets forth that any communications for direct advertising purposes may be performed provided that certain mandatory information is granted to data subjects, i.e., a notice of the opt-out right from the database and the mechanism for its exercise, including certain mandatory wording of local data protection regulations.

Further, communications must indicate in a clear manner that the material is a marketing document when it has not been expressly required/consented by the data subject.

## Are there specific requirements related to the use of personal data for direct marketing activities?

*Last reviewed: 2 December 2024*

**Yes**

**☒**  **email marketing**

☒       opt-out or implied consent

**☒**  **telephone marketing**

☒       opt-out or implied consent

**☒** **SMS/text message marketing**

☒       opt-out or implied consent

**☒**  **postal marketing**

☒       opt-out or implied consent

**☒**  **online behavioral advertising targeting/social media targeting/ad personalization marketing**

☒       opt-out or implied consent

# Data Processing in the Employment Context

## Is an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

*Last reviewed: 2 December 2024*

**Yes**

**The potential legal bases for data processing in the employment context are:**

The processing of personal data or sensitive personal data in the employment context can be carried out without obtaining employees' consent, provided the data arises from the employment relationship and is necessary for its development and/or compliance.

Otherwise, one of the legal bases identified above must be established in order to collect or process personal data or sensitive data.

## Can consent be validly obtained in the employment context?

*Last reviewed: 2 December 2024*

☒       Yes, but this consent is typically more difficult to establish in an employment context (specify details below)

Consent obtained from data subjects must be prior, informed, expressly given in writing or through any other similar means (e.g., electronically), considering the circumstances involved.

Prior to or while securing consent, certain mandatory information must be provided to data subjects (please refer to the section on "*Information Requirements*").

Due to the nature of an employment relationship, consent granted by employees could eventually be challenged by them with a certain level of success (alleging, for instance, that they had no other alternative than granting consent).

## Has the data privacy regulator issued guidance on use of artificial intelligence, automated decision making or profiling in an employment context – for example, relating to use in employee monitoring or hiring?

*Last reviewed: 2 December 2024*

No

While the DPA and other regulators have issued some non-binding regulations and recommendations regarding the use of AI, none of them are specifically targeted to an employment context. There is no express regulation addressing AI technology. Consequently, from a privacy standpoint, there would be no additional binding legal obligations beyond those indirectly resulting from the data protection regulatory framework.

# Artificial Intelligence, Profiling and Automated Decision Making

## Are there any restrictions or requirements related to creating profiles of data subjects or utilizing automated decision-making for decisions related to data subjects, including with respect to artificial intelligence?

*Last reviewed: 2 December 2024*

**Yes**

The restrictions or requirements are as follows:

☒       right to information / transparency requirement

☒       other

Under Convention 108+ (which refers to the Automatic Processing of Personal Data), the processing of genetic data, personal data relating to offenses, criminal proceedings and convictions, biometric data uniquely identifying a person, and other sensitive personal data (*e.g.*, information revealing racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life), will only be allowed where appropriate safeguards are enshrined in law, complementing those of Convention 108+. Moreover, under Convention 108+, data subjects are entitled to (i) obtain knowledge of the reasoning underlying the data processing, which is important in terms of profiling of individuals; and (ii) not to be subject to a harmful decision and which is made solely on automated processing, without considering the data subject's views.

Also, DPA's Resolution No. 4/2019 sets forth that data subjects have the right to request from the entity responsible for the database an explanation of the logic applied when the decisions are based solely on the automated processing of personal data and cause harmful effects or affect data subjects in a significant and negative way.

On artificial intelligence specifically:

Disposition No. 2/2023 of the Undersecretariat of Information Technologies of the Cabinet Chief approved the "Recommendations for a Reliable Artificial Intelligence." These Recommendations aim to guide and encourage the ethical and responsible use of AI and establish guidelines that cover the key stages of the development cycle of AI projects. The Recommendations are based on the "Recommendation on the Ethics of Artificial Intelligence" issued by UNESCO in November 2021, adopted by several countries, including Argentina. Their main objective is to provide guidance to the public sector in the management of AI projects. Following UNESCO's approach, the Recommendations consider the ethical aspects at each stage of the AI cycle, such as data design and modelling, verification and validation, implementation, and operation and maintenance. Although included guidelines and principles are non-binding and highly abstract, the importance of these Recommendations relies on the fact that they may constitute the basis for future and more specific regulations on AI.

Within the framework of the National Program for Transparency and Protection of Personal Data in the Use of AI, the DPA published the preliminary version of the "Guide for Public and Private Entities on Transparency and Protection of Personal Data for Responsible Artificial Intelligence" in September 2024. The main purpose of the Guide is to provide non-mandatory guidelines addressed to entities from the public and private sectors to incorporate transparency and protection of personal data in technological development projects that implement AI systems, ensuring the effective exercise of the rights of data subjects.

## If such restrictions or requirements exist, are they subject to any exceptions?

*Last reviewed: 2 December 2024*

**Yes**

It is the responsibility of databases/controllers to demonstrate compelling legitimate grounds for the processing that override data subjects' interests or rights and fundamental freedoms.

## Has the data privacy regulator issued guidance on data privacy and artificial intelligence, automated decision-making or profiling?

*Last reviewed: 2 December 2024*

**Yes**

The DPA has issued Resolution No. 161/2023, establishing the "Program for Transparency and Protection of Personal Data in the Use of Artificial Intelligence." The Program was created in consideration of the OECD's "Principles on Artificial Intelligence," the UNESCO's "Recommendations on the Ethics of Artificial Intelligence," and the Recommendations mentioned above (those approved by the Undersecretariat of Information Technologies of the Cabinet Chief). The general purpose of the program is to promote analysis, regulation and the strengthening of state capacities necessary to support the development and use of AI, guaranteeing the effective exercise of the rights of citizens in the transparency and protection of personal data. The program identifies specific objectives, such as investigating the implications of AI development from various perspectives (e.g., social, economic, and labor), generating knowledge to identify good practices, lessons learned, and recommendations in AI use, and promoting participatory processes for creating AI regulatory proposals.

Link to the Resolution [here](https://servicios.infoleg.gob.ar/infolegInternet/anexos/385000-389999/389231/norma.htm).

Further within the framework of the National Program for Transparency and Protection of Personal Data in the use of AI, the DPA published the preliminary version of the "Guide for Public and Private Entities on Transparency and Protection of Personal Data for Responsible Artificial Intelligence" in September 2024. The main purpose of the Guide is to provide non-mandatory guidelines addressed to entities from the public and private sectors to incorporate transparency and protection of personal data in technological development projects that implement AI systems, ensuring the effective exercise of the rights of data subjects.

Link to the preliminary version of the Guide [here](https://www.argentina.gob.ar/sites/default/files/aaip-argentina-guia_para_usar_la_ia_de_manera_responsable.pdf).

## Has the data privacy regulator taken enforcement action in relation to artificial intelligence, including automated decision-making or profiling?

*Last review date: 2 December 2024*

**☒**         No enforcement activity to date

## Do other (non-personal data or cybersecurity) laws or regulations impose restrictions on use of artificial intelligence, automated decision-making or profiling?

*Last reviewed: 2 December 2024*

☒       Draft legislation in progress

☒      Non-binding guidance or principles issued or in progress

Disposition No. 2/2023 of the Undersecretariat of Information Technologies of the Cabinet Chief approved the "Recommendations for a Reliable Artificial Intelligence." These Recommendations aim to guide and encourage the ethical and responsible use of AI and establish guidelines that cover the key stages of the development cycle of AI projects. The Recommendations are based on the "Recommendation on the Ethics of Artificial Intelligence" issued by UNESCO in November 2021, adopted by several countries, including Argentina. Their main objective is to provide guidance to the public sector in the management of AI projects. Following UNESCO's approach, the Recommendations consider ethical aspects at each stage of the AI cycle, such as data design and modelling, verification and validation, implementation, and operation and maintenance. Although the guidelines and principles are non-binding and highly abstract, the importance of these Recommendations relies on the fact that they may constitute the basis for future and more specific regulations on AI.

Link to the Disposition [here](https://www.boletinoficial.gob.ar/detalleAviso/primera/287679/20230602)

Further within the framework of the referred National Program for Transparency and Protection of Personal Data in the use of AI, the DPA published the preliminary version of the "Guide for Public and Private Entities on Transparency and Protection of Personal Data for Responsible Artificial Intelligence" on September 2024. The main purpose of the Guide is to set forth non-mandatory guidelines addressed to entities from the public and private sector to incorporate transparency and protection of personal data in those technological development projects that implement AI systems, ensuring the effective exercise of the rights of data subjects.

Link to the preliminary version of the Guide [here](https://www.argentina.gob.ar/sites/default/files/aaip-argentina-guia_para_usar_la_ia_de_manera_responsable.pdf).

# Data privacy and cybersecurity in a transactional context

## Has the data privacy authority issued any guidance on data privacy compliance in the context of transactional activity (including, but not limited to, share sales, asset sales, reorganizations or spinouts)?

*Last reviewed: 2 December 2024*

No

## In the context of an asset sale (the sale of a separate business unit as a going concern), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the assets that are the subject of the asset sale)?

*Last reviewed: 2 December 2024*

It depends (for example, on the way the asset sale is structured, and/or the assets being acquired)

## If so, how would any regulatory fines be calculated?

*Last reviewed: 2 December 2024*

☒        Based on a metric other than those outlined above

## In the context of a share sale (where the acquiring entity acquires 100% of the shares of a target company), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the target company)?

*Last reviewed: 2 December 2024*

☒       It depends (for example, on the way the share sale is structured)

## If so, how would any regulatory fines be calculated?

*Last review date: 2 December 2024*

☒        Based on a metric other than those outlined above

# Security Requirements and Breach Notification

## Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last reviewed: 2 December 2024*

Yes.

☒       general obligation to take appropriate / reasonable technical, physical and/or organizational security measures
☒       other

DPA Resolution No. 47/2018 provides the recommended security measures for the processing and conservation of personal data in computerized and non-computerized media, such as the necessary confidentiality measures to guarantee effective control of access, backups and recovery systems and detection of possible security breaches, among others.

## Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last reviewed: 2 December 2024*

☒       public company obligations (e.g., duties to maintain sufficient information security measures or ensure operational resilience to cyberattacks)

☒       financial services requirements

☒       telecommunication requirements

☒       providers of critical infrastructure

Resolution No. 580/2011 creates the National Program on Information and Cybersecurity Critical Infrastructure and Resolution No. 1523/2019 defines Critical Infrastructure.

The National Communications Entity issued the "Regulation for the Collection of Personal Data and Identity Validation of Users of Mobile Services that Hold a Mobile Number" that requires mobile services providers to adjust their existing protocols for the registration of new mobile numbers and for changes of certain conditions in which the services are provided. This means implementing new guidelines for the collection of personal data and identity validation of users to mitigate risks of fraud and impersonation.

The Argentine Central Bank issued Communication 'A' 7724, which updated the technology and information security risk standards to strengthen the cyber resilience of financial institutions. Generally, the Argentine Central Bank aims for regulated financial institutions to develop and implement governance programs that include, among other things: (i) risk identification and management; (ii) design of internal policies and procedures; (iii) continuous evaluation and audit of policies to identify and correct errors; (iv) internal awareness and training; and (v) proper documentation and backup of data and information, as well as of any security incident or event.

## Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

*Last reviewed: 2 December 2024*

☒  Data privacy

☒  Securities or public company

☒  health

☒  financial services

☒  telecommunications

## Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last reviewed: 2 December 2024*

**No**

However, DPA's Resolution No. 47/2018, which sets forth the "Recommended security measures for the processing and retention of personal data in computerized and non-computerized media," refers to security incidents and recommends the preparation of a report including, at least, the following information: (i) nature of the incident; (ii) category of personal data affected; (iii) identification of affected users; (iv) measures adopted to mitigate the breach, and (v) measures adopted to prevent future incidents. It also recommends notifying the DPA of the security incident and attaching the aforementioned report. *There is no timeframe provided to send the mentioned notice to the DPA.*

Also, DPA's Resolution No. 332/2020 includes legal and technical guidelines to be considered by inspectors when carrying out the inspection of personal data processing activities. The implementation of an incident notification notice to the DPA and the data subjects will be considered when conducting an inspection. It will also be considered if the individual or entity responsible for the database implements, among others, *an incident notification system* to the DPA and data subjects.

The Personal Data Protection Bill of Law introduced in Congress includes the obligation to report to data subjects and the DPA certain security incidents within 72 hours of acquiring effective knowledge. A similar approach is followed under other Bills of Law being discussed in Congress.

## Controllers/Owners have to notify:

*Last reviewed: 2 December 2024*

N/A

## Processors/Agents have to notify:

*Last reviewed: 29 December 2023*

N/A

## Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last reviewed: 2 December 2024*

**☒ Yes**

☒      public company obligations (e.g., to notify security incidents that may materially affect an investor's decision)
☒       financial services requirements
☒      other

**If so, please provide brief details of the relevant law / guidance and indicate which body/bodies must be notified of the breach.**

Some sector-specific regulations are not explicitly clear as to the obligation to report a data security breach.

Although the National Securities Commission (*Comisión Nacional de Valores*, or CNV) regulations do not define or refer to "security breach," they establish that every act or situation that, due to its importance, is able to substantially affect the placement of negotiable securities, the course of their negotiation, or the development of the activity of who suffered the event, must be reported to the investors and the CNV (Title XII, Chapter I, Section II of the CNV framework). There is no specific timeframe established to inform investors and the CNV. The regulations only provide that the notification should be done immediately upon acknowledgment of such breach.

Moreover, the Argentine Central Bank issued Communication "B" No. 11847 related to technology and systems incidents, which sets forth that financial entities must report to the External Systems Audit Management (*Gerencia de Auditoria Externa de Sistemas)* when financial information or customer personal data is compromised.

In addition, Communication "A" No. 7266 of the Argentine Central Bank establishes that financial entities, payments service providers, and financial market infrastructures must report relevant information on cyber incidents to the authorities as required and in accordance with the timeframes established by applicable laws.

Communication "A" No. 7724 of the Argentine Central Bank establishes that financial institutions must implement effective control and management practices in accordance with the complexity of the financial services offered and the technology used. In this sense, among other obligations, they must develop cyber incident management policies, including roles and responsibilities of the areas involved in their response, and keep a complete record of the cyber incidents suffered in such a way that allows the identification, traceability and evidence of the actions taken until their closure. In terms of communication and notification, they should establish effective procedures for a timely and planned response, as well as designate a point of contact for reporting cyber incidents and mitigating the impact in a timely manner.

# Data localization and regulation of non-personal data

## Are there data localization/data residency or other types of laws that may require the retention and storage of data in the local jurisdiction, or prohibit the transfer of data out of the jurisdiction?

*Last reviewed: 2 December 2024*

Under the Personal Data Protection Law No. 25,326, no. However, other regulations do provide data localization requirements:

☒       Data localization / data residency laws that mandate retention of personal data or a copy thereof in the local jurisdiction (include whether copies or the original data may also be stored outside of the jurisdiction):

Corporate and accounting books and related documents have to be stored in the companies' legal domicile. Also, said books that may contain personal data (*e.g.*, tax receipts) should be stored for a term of ten years.

Communication "A" 6354 issued by the Argentine Central Bank ("**BCRA**") allows financial entities to outsource Information Technology Services (ITS) (*e.g.*, cloud migration), provided that they do not contain information on clients and/or the general public. The Communication provides that certain documentation must be stored within Argentina (*e.g.*, original copies of accounting books and records and debtors' profiles according to credit management regulations).

☒       Other laws that may require the retention and storage of personal data (including, for example, where such data is part of another type of record or dataset) in the local jurisdiction or otherwise prohibit the transfer or disclosure of the personal data outside of the local jurisdiction:

☒       employment laws

## Does law or regulation impose mandatory requirements to share or make accessible non-personal data?

*Last review date: 2 December 2024*

☒         Obligation for public sector organizations to share or make accessible non-personal data\

***If so, please provide brief details of the relevant law or regulation.***

Access to Public Information Law No. 27,275 aims to guarantee the effective exercise of the right to access public information, promote citizen participation, and ensure transparency in public administration. It mandates that various public entities, including the national public administration, legislative and judicial branches, and state-owned companies, provide public information as stipulated by the law.

## What specific obligations do these data-sharing rules impose on private organizations?

*Last review date: 2 December 2024*

☒         Obligation to share data on request

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.