Employee Data Privacy – Argentina

Employee Consent

Do I have to obtain employees' consent in order to collect their personal data?

The processing of any personal data may impose obligations to the individuals the data is related to, the data subjects. Some jurisdictions only recognize processing personal data as lawful if the data subject has provided express consent. Other jurisdictions require a legal obligation to process the data and may not require consent. The processing of HR personal data has raised questions and court decisions in a few countries, and interpretations may vary based on data privacy and labor law requirements.

Free, express and informed consent is generally required prior to processing an individual's personal data in Argentina. The consent must be given in writing or via another means that allows it to be "equated" depending on the circumstances (Protection of Personal Data Law, 2000, No. 25326, Art. 5). Consent of the individual is also generally required to transfer personal data.

Consent to collect, process and transfer personal information is not required in certain circumstances. The circumstances that are most likely to apply to employers include when:

- data is obtained from an unrestricted public source;
- data is collected for functions of the government or by virtue of a legal obligation (ex., when collecting an employee's data to comply with a government regulation);
- data is being used as part of a list, when this data is limited to name, national identity documents, tax/social security identification, occupation, date of birth and address; or, when
- data is collected through a contractual, scientific or professional relationship with the owner of the data (i.e., the employee) and is necessary to develop or fulfill the relationship (such as when collecting an employee's bank account information in order to pay them under the terms of the employment contract).

In addition to the above, employers do not need to obtain consent from the individual to transfer personal data, when (Art. 11):

- allowed by law;
- the data is personal health data and the information is necessary for public health, an emergency or, to carry out epidemiological studies as long as the individual has been

deidentified via an appropriate method; or, when
- an information deidentification method is used so that the individual is unidentifiable.

Informing Individuals

When personal data is collected, employees (and other data owners) should be clearly and expressly informed by the employer in advance of:

- the purpose of the processing and the potential recipients or class of recipients of the data;
- the existence of the file, registry, database, etc. in question along with the identity and address of the data manager;
- whether the request for the personal data is required or optional, especially if the data is considered sensitive;
- the consequences of the individual providing or refusing to provide their personal data or providing inaccurate data; and,
- how they can exercise their rights to access, rectification and deletion of data (Protection of Personal Data Law, 2000, No. 25326, Art. 6).

The above information must be displayed in a visible place so that employees (and any other data owners) are aware of their rights prior to any data collection (AAIP Resolution 14/2018). This can be done through an online notification.

Sensitive Personal Data

Under the Protection of Personal Data Law, there are additional restriction relating to processing and collecting sensitive personal data. Sensitive personal data includes data that reveals: racial and ethnic origin; political opinions; religious, philosophical or moral convictions; union affiliation; or, information regarding health or sexual life.

Individuals cannot be forced to provide sensitive data, and this data can only be collected and processed when there are reasons of general interest authorized by law. Sensitive data can also be processed for statistical or scientific purposes when the owners of the data cannot be identified

(ex., such as when sensitive data has been anonymized). In addition, forming files, banks or registers that store information that reveals sensitive data (directly or indirectly) is generally not permitted. Data relating to criminal or infringement records can only be processed as legally permitted by the relevant public authorities.

Last updated October 2022.