AGENCY FOR ACCESS TO PUBLIC INFORMATION

Resolution 86/2019

RESOL-2019-86-APN-AAIP

City of Buenos Aires, 05/31/2019

Considering the electronic file EX-2019-36666622- -APN-DNPDP # AAIP, the laws N ° 25,326 of Protection of Personal Data and N ° 27,275 of the Right of Access to Public Information, the Decrees N ° 1558 of November 29, 2001 and N ° 746 of September 26, 2017 Y;

CONSIDERING:

That Law 25,326 established the general principles relating to data protection, defining the scope of exercise of the rights of data holders, the scope of responsibility of users and those responsible for files, records and databases, control of the use of data and the basic scheme of sanctions applicable to its transgression.

That by Decree No. 1558 of November 29, 2001, regulating the aforementioned Law, the NATIONAL DIRECTORATE OF PERSONAL DATA PROTECTION was created, within the orbit of the SECRETARIAT OF JUSTICE AND LEGISLATIVE AFFAIRS of the MINISTRY OF JUSTICE AND HUMAN RIGHTS, as a matter control body.

That Law No. 27,275 created the AGENCY FOR ACCESS TO PUBLIC INFORMATION (AAIP) as an autarkic entity with functional autonomy within the scope of the HEAD OF MINISTERS 'CABINET, in order to "ensure compliance with the principles and procedures established in Law [N ° 27,275], guarantee the effective exercise of the right of access to public information and promote active transparency measures ".

That Decree No. 746 of September 25, 2017, attributed to the AAIP the power to act as the Enforcement Authority of Law No. 25,326, and assigned it the competence of "[f] overseeing the comprehensive protection of personal data recorded in files, records, databases, or other technical means of data processing, whether public or private, destined to give reports, to guarantee the right to honor and privacy of people, as well as access to the information that is registered about them ".

That, on the other hand, in a democratic state, communication between political organizations and voters is essential and that proselytizing activities are especially protected by the principle of freedom of expression, enshrined in article 14 of the Constitution. National, article 13 of the American Convention on Human Rights, article 19 of the Universal Declaration of Human Rights and article 19 of the International Covenant on Civil and Political Rights.

That, along these lines, Article 4 of the Inter-American Democratic Charter stipulates that freedom of expression and of the press is one of the "fundamental components for the exercise of democracy."

That, in a consistent manner, Article 2 of Law No. 23,298, Organic Law of Political Parties, establishes that "parties are necessary instruments for the formulation and implementation of national politics."

That, likewise, as the National Electoral Chamber has expressed in its Extraordinary Agreement No. 66/2018 "in relation to the information and dissemination of ideas of political groups in electoral contests, the impact and the new challenges which represents the rise of digital platforms and environments, which became a new communication circuit ".

That, in this context of technological development and the search for greater transparency, some methods of political propaganda, such as disclosure on social networks and the automated sending of messages by email, involve the processing of personal data.

That, in this sense, all data processing is regulated by Law No. 25,326 and Convention 108, for the Protection of People with respect to the Automated Processing of Personal Data, approved by Law No. 27,483.

That Law No. 25,326 aims at "the comprehensive protection of personal data recorded in files, registers, data banks, or other technical means of data processing, be they public or private for reporting purposes" and that the Convention 108, in turn, is applies to anyone who performs automated data processing; so this legal regime reaches political organizations and groups.

That by virtue of the need to establish guidelines that help provide more clarity on a subject as sensitive as personal data and communication between political organizations and voters in a democratic state, there are several control authorities for the protection of personal data in the world that, recently, have published guides, regulations or opinions on the processing of personal data for electoral purposes.

That in this sense, the works prepared by the Commission Nationale de l'Informatique et des Libertés in France (2016), the Information Commissioner's Office in the United Kingdom (2018), the Data Protection Commission in Ireland (2018), the Urzad Ochrony Danych Osobowych in Poland (2018), the Spanish Data Protection Agency in Spain (2019), the Gegevenbeschermingsautoriteit in Belgium (2019) and the European Data Protection Board (2019).

That in all cases, the objective was "to underline the key points that must be respected by political parties when they process personal data in the course of electoral activities" (JEPD [2019], Statement 2/2019).

That, for the aforementioned reasons and with the deep conviction that communication with voters and proselytizing activities are absolutely necessary and indispensable for democracy, the AGENCY FOR ACCESS TO PUBLIC INFORMATION deems it appropriate prepare a guide on the processing of personal data for electoral purposes, aimed mainly at groups, political organizations, candidates, think tanks, consultants and anyone who processes personal data in order to carry out or contribute to an electoral campaign.

That the objective of the Guide is to ensure the integrity and protection of the personal data of the participating citizens during the election process, establishing a series of basic guidelines to achieve that end, adapting to current regulations.

That the NATIONAL DIRECTORATE OF PERSONAL DATA PROTECTION and the COORDINATION OF LEGAL AFFAIRS of the AGENCY OF ACCESS TO PUBLIC INFORMATION have taken the intervention of their competence.

That this measure is issued in use of the powers conferred by art. 29, inc. 1, section b) of Law No. 25,326, art. 19 of Law No. 27,275 and article 29 of Decree 1558/2001.

Thus,

THE DIRECTOR OF THE PUBLIC INFORMATION ACCESS AGENCY

RESOLVES:

ARTICLE 1. - Approve the Guide on the Processing of Personal Data for Electoral Purposes, which as Annex I (IF-2019-51061931-APN-AAIP) forms an integral part of this Resolution.

ARTICLE 2. - Communicate, publish, give it to the NATIONAL ADDRESS OF THE OFFICIAL REGISTRY and, in due course, file it. Eduardo Andrés Bertoni

NOTE: The Annex / s that make up this Resolution are published on the BORA web edition -www.boletinoficial.gob.ar-

and. 06/05/2019 N ° 39216/19 v. 06/05/2019

*(**Note Infoleg:** The annexes referenced in this standard have been extracted from the web edition of the Official Gazette)*

Guide on the processing of personal data for electoral purposes

1. Fundamental principles of personal data protection

Purpose The data must be treated according to the purpose that has been declared at the time of obtaining them. The data may be used for other purposes that are compatible with the main purpose, if and only if these could have been reasonably foreseen by the owner of data (art. 4, inc. 1 and 3 of Law No. 25,326).

Proportionality The data collected must be proportional and not excessive in relation to the purpose declared for obtaining it (art. 4, inc. 1 of Law No. 25,326).

Accuracy and updating. The data must be exact and will have to be updated, completed or deleted in case of error, imprecision or impairment of another right of the owner thereof. Those who carry out any treatment should periodically examine their database data and, when appropriate, make the necessary corrections (art. 4, inc. 1, 4 and 5 of Law No. 25,326).

Loyalty and good faith. Data collection cannot be done by means that are unfair, fraudulent or that in any way violate the law (art. 4, inc. 2 of Law No. 25,326).

Accessibility. The data must be stored in such a way as to allow access by the owner (art. 4, inc. 6 of Law No. 25,326).

Minimization. The data must be destroyed when they are no longer necessary or relevant for the purposes for which they were collected (art. 4, inc. 7 of Law No. 25,326).

2. Registration

Any database that is not registered in the National Registry of Personal Data Bases is illegal (art. 3 of Law No. 25,326 and Resolution 132/2018). Those who process personal data and are not yet registered, must register. Registration is a guarantee essential for citizens to exercise their rights of access, updating, rectification and deletion of their data.

3. Rights of data holders

Access . The owner of the data, after proof of their identity, has the right to request and obtain information on their personal data that have been stored or registered. The requested information must be provided within ten calendar days of being requested. (art. 14 of Law No. 25,326).

Update and rectification . When there is an error or any affectation to the data owner, he has the right to request the updating or rectification of his personal data. The person responsible for the database or registration that has been required must reply to the owner within five days. working days of receipt of the claim or noticed the error or falsehood (art. 16 of Law No. 25,326).

Suppression . The owner of the data has the right to request the deletion or confidentiality of their personal data. The deadline to answer the claim is the same as in the case of updating or correction. However, the deletion does not proceed when it could cause damage to legitimate rights or interests of third parties, or when there is a legal obligation to keep the data (art. 16 of Law No. 25,326).

4. Consent

When transferring your personal data, the consent of the owner must be free, express and informed (art. 5 of Law No. 25,326). Therefore, when data is collected through surveys, questionnaires, subscriptions or other internet services, it is mandatory to provide the respondent or subscriber the terms and conditions that:

to. they are clear, simple and written in a language understandable to the general public;

b. identify the person responsible for the treatment and their address;

c. express the purpose of the treatment;

d. In the event that the data is collected through questionnaires, forms or surveys, they differentiate between the optional or mandatory nature of the responses;

and. explain the consequences of providing the data;

F. inform all the rights that can be exercised by any interested party as the owner of personal data.

5. Political opinions

Personal data that reveal political opinions are considered sensitive data (art. 2 of Law No. 25,326). As a general criterion, the processing of sensitive data is prohibited (art. 7, inc. 3 of Law No. 25,326). This kind of data can only be processed when There is consent regarding the publication of the data, when the treatment has statistical purposes and its holders cannot be identified, or when, legally foreseen reasons of general interest, justify it (arts. 5 and 7 of Law No. 25,326).

6. Affiliation to a political organization

The affiliation and the consequent delivery of sensitive data to a political organization is perfectly legal and valid (art. 7, inc. 3 of Law No. 25,326), as long as consent is provided.

7. Public data on social networks, forums and web platforms

The personal data published in social networks, forums or web platforms of easy access or unrestricted access, are also covered by the fundamental principles of Law No. 25,326, so they must comply with the principles defined in section (1).

Therefore, those who process this type of public data must inform, at least through a global notification or an online publication, the purpose of the treatment, who is responsible, what their address and what are the rights that the holders of the data in question (art. 6 of Law No. 25,326).

8. Electoral propaganda on social networks, messaging platforms and other web services

The personal data that will be used to send electoral propaganda such as email, the account of a social network, an instant messaging service or other similar must have been obtained lawfully, protected in any of the bases legal provisions contained in arts. 5 or 7 of Law No. 25,326.

9. Basic data

The consent of the owner of the data will not be necessary, in the case of lists whose data is limited to name, national identity document, tax or social security identification, occupation, date of birth and address (art. 5, inc. C of the Law No. 25,326).

10. Provision of computerized services

When a third party is hired to process personal data, the data may not be used for a purpose other than that stated in the service contract, nor may the data be transferred to other people, not even for conservation (art. 25, inc. 1 of Law No. 25,326). For For example, if a political party hired a consultant or advisor to carry out a survey based on a registry of its members, this would have to conform to the purpose of the service contract and could not exceed it.

Once the performance of the contract has been fulfilled, the personal data processed must be destroyed, unless expressly authorized and the possibility of further orders is reasonably presumed. In that case, the data may be stored with the proper conditions of security for a period of up to two years (art. 25, inc. 2 of Law No. 25,326).

11. Security and confidentiality

It is mandatory to adopt the appropriate technical and organizational measures to guarantee the security and confidentiality of personal data, in order to avoid its adulteration, loss, consultation or unauthorized treatment (art. 9 of Law No. 25,326).

The people who intervene in any phase of the processing of personal data are also bound by a duty of confidentiality. Such obligation will subsist even after the contractual relationship has ended (art. 10 of Law No. 25,326).

In order to comply with these obligations, it is convenient to incorporate the Recommended Security Measures for the Treatment and Conservation of Personal Data, contained in Resolution 47/2018 (https://www.boletinoficial.gob.ar/#!DetalleNorma/anexos/188654/20180725).

12. Interpretation

This guide must be interpreted and complemented with the full reading of Law No. 25,326, Decree 1558/2001, Agreement for the Protection of People with respect to the Automated Processing of Personal Data and the regulations issued by the Agency for Access to Public Information, available on the web (https://www.argentina.gob.ar/aaip/buscador-normativa).