AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA

Resolución 86/2019

RESOL-2019-86-APN-AAIP

Ciudad de Buenos Aires, 31/05/2019

Visto el expediente electrónico EX-2019-36666622- -APN-DNPDP#AAIP, las leyes N° 25.326 de Protección de Datos Personales y N° 27.275 de Derecho de Acceso a la Información Pública, los Decretos N° 1558 del 29 de noviembre de 2001 y N° 746 del 26 de septiembre de 2017 y;

CONSIDERANDO:

Que la Ley 25.326 estableció los principios generales relativos a la protección de datos, definiéndose el ámbito de ejercicio de los derechos de los titulares de datos, el alcance la responsabilidad de los usuarios y responsables de archivos, registros y bancos de datos, el control del uso de datos y el esquema básico de sanciones aplicables a su transgresión.

Que mediante el Decreto N° 1558 del 29 de noviembre de 2001, reglamentario de la Ley citada, se creó la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, en la órbita de la SECRETARÍA DE JUSTICIA Y ASUNTOS LEGISLATIVOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, como órgano de control de la materia.

Que la Ley N° 27.275 creó la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA (AAIP) como ente autárquico con autonomía funcional en el ámbito de la JEFATURA DE GABINETE DE MINISTROS, con el objeto de "velar por el cumplimiento de los principios y procedimientos establecidos en la Ley [N° 27.275], garantizar el efectivo ejercicio del derecho de acceso a la información pública y promover medidas de transparencia activa".

Que el Decreto N° 746 del 25 de septiembre de 2017, atribuyó a la AAIP la facultad de actuar como Autoridad de Aplicación de la Ley N° 25.326, y le asignó la competencia de "[f]iscalizar la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre".

Que, por otra parte, en un estado democrático la comunicación entre las organizaciones políticas y los votantes es fundamental y que las actividades de proselitismo están especialmente protegidas por el principio de libertad de expresión, consagrado en el artículo 14 de la Constitución Nacional, el artículo 13 de la Convención Americana de Derechos Humanos, el artículo 19 de la Declaración Universal de Derechos Humanos y el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos.

Que, en esta línea, el artículo 4 de la Carta Democrática Interamericana preceptúa que la libertad de expresión y de prensa es uno de los "componentes fundamentales para el ejercicio de la democracia".

Que, de manera concordante, el artículo 2 de Ley N° 23.298, Ley Orgánica de los Partidos Políticos, establece que "los partidos son instrumentos necesarios para la formulación y realización de la política nacional".

Que, asimismo, tal como ha expresado la Cámara Nacional Electoral en su Acordada Extraordinaria Nro. 66/2018 "en relación con la información y difusión de ideas de las agrupaciones políticas en las contiendas electorales, no puede dejar de advertirse el impacto y los nuevos desafíos que representa el auge de las plataformas y entornos digitales, que se constituyeron en un novedoso circuito de comunicación".

Que, en este contexto de desarrollo tecnológico y búsqueda de mayor transparencia, algunos métodos de propaganda política, como por ejemplo, la divulgación en redes sociales y el envío automatizado de mensajes por correo electrónico, involucran el tratamiento de datos personales.

Que, en este sentido, todo tratamiento de datos está regulado por la Ley N° 25.326 y el Convenio 108, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal , aprobado por la Ley N° 27.483.

Que la Ley N° 25.326 tiene por objeto "la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes" y que el Convenio 108, a su turno, se aplica a todo aquel que realice tratamiento automatizado de datos; por lo que este régimen legal alcanza a las organizaciones y agrupaciones políticas.

Que en virtud de la necesidad de establecer pautas que ayuden a brindar más claridad en un tema tan sensible como los datos personales y la comunicación entre las organizaciones políticas y los votantes en un estado democrático, son varias las autoridades de control de protección de datos personales en el mundo que, recientemente, han publicado guías, reglamentos u opiniones sobre el tratamiento de datos personales con fines electorales.

Que en este sentido, pueden citarse los trabajos elaborados por la Commission Nationale de l'Informatique et des Libertés en Francia (2016), la Information Commissioner's Office en Reino Unido (2018), la Data Protection Commission en Irlanda (2018), la Urzad Ochrony Danych Osobowych en Polonia (2018), la Agencia Española de Protección de Datos en España (2019), la Gegevenbeschermingsautoriteit en Bélgica (2019) y la Junta Europea de Protección de Datos (2019).

Que en todos los casos, el objetivo fue "subrayar los puntos clave que deben ser respetados por los partidos políticos cuando tratan datos personales en el curso de actividades electorales" (JEPD [2019], Statement 2/2019).

Que, por las razones expuestas y con la profunda convicción de que la comunicación con los votantes y las actividades de proselitismo son absolutamente necesarias e indispensables para la democracia, la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA estima oportuno elaborar una guía sobre tratamiento de datos personales con fines electorales, destinada principalmente a las agrupaciones, organizaciones políticas, candidatos, think tanks, consultores y todo aquel que trate datos personales con el fin de realizar o contribuir en una campaña electoral.

Que el objetivo de la Guía es asegurar la integridad y la protección de los datos personales de los ciudadanos participantes con motivo del proceso eleccionario, sentando una serie de lineamientos básicos para alcanzar ese fin, adecuándose a la normativa vigente.

Que la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES y la COORDINACIÓN DE ASUNTOS JURÍDICOS de la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA han tomado la intervención de su competencia.

Que la presente medida se dicta en uso de las facultades conferidas por el art. 29, inc. 1, apartado b) de la Ley N° 25.326, el art. 19 de la Ley N° 27.275 y el artículo 29 del Decreto 1558/2001.

Por ello,

EL DIRECTOR DE LA AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA

RESUELVE:

ARTÍCULO 1°. – Apruébese la Guía sobre Tratamiento de Datos Personales con Fines Electorales, que como Anexo I (IF-2019-51061931-APN-AAIP) forma parte integrante de la presente Resolución.

ARTÍCULO 2°. - Comuníquese, publíquese, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y, oportunamente, archívese. Eduardo Andrés Bertoni

NOTA: El/los Anexo/s que integra/n este(a) Resolución se publican en la edición web del BORA -www.boletinoficial.gob.ar-

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

(***Nota Infoleg:*** *Los anexos referenciados en la presente norma han sido extraídos de la edición web de Boletín Oficial)*

República Argentina - Poder Ejecutivo Nacional
2019 - Año de la Exportación

Anexo

Número: IF-2019-51061931-APN-AAIP

CIUDAD DE BUENOS AIRES
Viernes 31 de Mayo de 2019

Referencia: Guía sobre tratamiento de datos personales con fines electorales.

Guía sobre tratamiento de datos personales con fines electorales

1. Principios fundamentales de protección de datos personales

Finalidad. Los datos deben ser tratados conforme a la finalidad que se haya declarado al momento de obtenerlos. Se podrán emplear los datos para otros fines que sean compatibles con la finalidad principal, si y sólo si estos pudieran haber sido razonablemente previstos por el titular de datos (art. 4, inc. 1 y 3 de la Ley N° 25.326).

Proporcionalidad. Los datos recolectados deben ser proporcionales y no excesivos en relación con la finalidad que se hubiese declarado para su obtención (art. 4, inc. 1 de la Ley N° 25.326).

Exactitud y actualización. Los datos deben ser exactos y tendrán que actualizarse, completarse o suprimirse en caso de mediar error, imprecisión o afectación de otro derecho del titular de los mismos . Quienes realicen algún tratamiento deberán examinar periódicamente su base de datos y, cuando corresponda, hacer las correcciones que resulten necesarias (art. 4, inc. 1, 4 y 5 de la Ley N° 25.326).

Lealtad y buena fe. La recolección de datos no puede hacerse por medios desleales, fraudulentos o que de alguna manera contraríen la ley (art. 4, inc. 2 de la Ley N° 25.326).

Accesibilidad. Los datos deben ser almacenados de modo que permitan su acceso por parte del titular (art. 4, inc. 6 de la Ley N° 25.326).

Minimización. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes para los fines por los que hubiesen sido recolectados (art. 4, inc. 7 de la Ley N° 25.326).

2. Inscripción

Toda base de datos que no esté inscripta en el Registro Nacional de Bases de Datos Personales es ilícita (art. 3 de la Ley N° 25.326 y Resolución 132/2018). Quienes hagan tratamiento de datos personales y aún no estén registrados, deberán inscribirse. El registro es una garantía fundamental para que los ciudadanos puedan ejercer sus derechos de acceso, actualización, rectificación y supresión de sus datos.

3. Derechos de los titulares de datos

Acceso. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales que hayan sido almacenados o registrados. Se debe proporcionar la información solicitada dentro de los diez días corridos de haber sido requerida (art. 14 de la Ley N° 25.326).

Actualización y rectificación. Cuando exista error o alguna afectación al titular de datos, este tiene derecho a requerir la actualización o rectificación de sus datos personales. El responsable de la base o registro que hubiera sido requerido, debe contestar al titular en el plazo de cinco días hábiles de recibido el reclamo o advertido el error o falsedad (art. 16 de la Ley N° 25.326).

Supresión. El titular de los datos, tiene derecho a solicitar la supresión o confidencialidad de sus datos personales. El plazo para contestar el reclamo es el mismo que en el caso de actualización o corrección. Sin embargo, la supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos (art. 16 de la Ley N° 25.326).

4. Consentimiento

Al ceder sus datos personales, el consentimiento del titular debe ser libre, expreso e informado (art. 5 de la Ley N° 25.326). Por lo tanto, cuando se recaben datos por medio de encuestas, cuestionarios, suscripciones u otros servicios de internet, es obligatorio proveerle al encuestado o suscriptor los términos y condiciones que:

a. sean claros, sencillos y estén redactados en un lenguaje comprensible para el público general;

b. identifiquen al responsable del tratamiento y su domicilio;

c. expresen la finalidad del tratamiento;

d. en el caso en que los datos se recolecten por medio de cuestionarios, formularios o encuestas, diferencien entre el carácter opcional u obligatorio de las respuestas;

e. expliquen las consecuencias de proporcionar los datos;

f. informen todos los derechos que puede ejercer cualquier interesado en calidad de titular de datos personales.

5. Opiniones políticas

Los datos personales que revelan opiniones políticas son considerados datos de carácter sensible (art. 2 de la Ley N° 25.326). Como criterio general, el tratamiento de datos sensibles está prohibido (art. 7, inc. 3 de la Ley N° 25.326). Esta clase de datos solo podrá tratarse cuando medie consentimiento respecto de la publicación del dato, cuando el tratamiento tenga fines estadísticos y no puedan ser identificados sus titulares, o bien cuando, razones de interés general, previstas legalmente, lo justifiquen (arts. 5 y 7 dela Ley N° 25.326).

6. Afiliación a una organización política

La afiliación y la consecuente entrega de datos sensibles a una organización política es perfectamente legal y válida (art. 7, inc. 3 de la Ley N° 25.326), siempre y cuando medie consentimiento.

7. Datos públicos en redes sociales, foros y plataformas web

Los datos personales publicados en redes sociales, foros o plataformas web de fácil acceso o acceso irrestricto, también están alcanzados por los principios fundamentales de la Ley N° 25.326, por lo que deben adecuarse a los principios definidos en el apartado (1).

Por lo tanto, quienes traten éste tipo de datos públicos deberán informar, al menos a través de una notificación global o una publicación en internet, la finalidad del tratamiento, quién es el responsable, cuál su domicilio y cuáles son los derechos que pueden ejercer los titulares de los datos en cuestión (art. 6 de la Ley N° 25.326).

8. Propaganda electoral en redes sociales, plataformas de mensajería y otros servicios web

Los datos personales que vayan a ser utilizados para el envío de propaganda electoral tales como, el correo electrónico, la cuenta de una red social, de un servicio de mensajería instantánea u otros similares deberán haber sido obtenidos lícitamente, amparados en alguna de las bases legales contenidas en los arts. 5 o 7 de la Ley N° 25.326.

9. Datos básicos

No será necesario el consentimiento del titular de los datos, cuando se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio (art. 5, inc. c de la Ley N° 25.326).

10. Prestación de servicios informatizados

Cuando se contrate a un tercero para que haga tratamiento de datos personales, los datos no podrán utilizarse con un fin distinto al que figure en el contrato de servicios, ni se podrán ceder los datos a otras personas, ni aun para su conservación (art. 25, inc. 1 de la Ley N° 25.326). Por ejemplo, si un partido político contratara a un consultor o un asesor para que elabore una encuesta en base a un registro de sus afiliados, este tendrá que ajustarse a la finalidad del contrato de servicios y no podrá excederlo.

Una vez cumplida la prestación del contrato, los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa y razonablemente se presuma la posibilidad de ulteriores encargos. En ese caso, se podrán almacenar los datos con las debidas condiciones de seguridad por un período de hasta dos años (art. 25, inc. 2 de la Ley N° 25.326).

11. Seguridad y confidencialidad

Es obligatorio adoptar las medidas técnicas y organizativas que resulten adecuadas para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado (art. 9 de la Ley N° 25.326).

Las personas que intervengan en cualquier fase del tratamiento de datos personales están obligadas, además, por un deber de confidencialidad. Tal obligación subsistirá aun después de finalizada la relación contractual (art. 10 de la Ley N° 25.326).

A los fines del cumplir con estas obligaciones, resulta conveniente incorporar las Medidas de Seguridad Recomendadas para el Tratamiento y Conservación de los Datos Personales, contenidas en la Resolución 47/2018 (https://www.boletinoficial.gob.ar/#!DetalleNorma/anexos/188654/20180725).

12. Interpretación

Esta guía debe ser interpretada y complementada con la lectura íntegra de la Ley N° 25.326, el Decreto 1558/2001, Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y los reglamentos emitidos por la Agencia de Acceso a la Información Pública, disponibles en la web (https://www.argentina.gob.ar/aaip/buscador-normativa).

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=SECRETARIA DE GOBIERNO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30716117564
Date: 2019.05.31 13:58:48 -03'00'

Eduardo Andrés Bertoni
Director
Agencia de Acceso a la Información Pública