Subprocuraduría de Asuntos Jurídicos

LEY DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO

PAOT

PROCURADURÍA AMBIENTAL Y DEL ORDENAMIENTO TERRITORIAL DE LA CDMX

Medellín número 202, 2° Piso, Col. Roma, Delegación Cuauhtémoc, C.P. 06700, Ciudad de México, Teléfono: 52.65.07.80 Ext. 15000

El 10 de abril se publicó en la Gaceta Oficial de la Ciudad de México, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, la cual entró en vigor al día siguiente de su publicación.

Objeto: Establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona al tratamiento lícito de sus datos personales, a la protección de los mismos, así como al ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición de sus datos personales en posesión de *sujetos obligados* (cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, partidos políticos, fideicomisos y fondos públicos).

Antecedentes:

- El 03 de octubre de 2008, se publicó la **Ley de Protección de Datos Personales para el Distrito Federal**, la cual fue reformada el 18 de diciembre de 2014.

- El 26 de enero de 2017, se publicó la **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**, la cual tenía como objetivo distribuir competencias entre los Organismos garantes de la Federación y las Entidades Federativas, en materia de protección de datos personales en posesión de sujetos obligados.

- El 10 de abril se publicó en la Gaceta Oficial de la Ciudad de México, la **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México**; **sin embargo, esta Ley no abroga expresamente la publicada en 2008.**

Temas relevantes

1. Definiciones
2. Principios y Deberes
3. Aviso de privacidad
4. Medidas de seguridad
5. Documentos de Seguridad

Temas relevantes

6 Sistemas de Datos Personales

7 Derechos ARCO

8 Unidades Responsables

9 Transferencia de datos

10 Tratamiento intensivo o relevante

11 Recurso, verificación y medidas de apremio

1. Definiciones

Dentro de las definiciones incorporadas en la Ley, se destacan las siguientes:

Aviso de privacidad: Documento a disposición del titular de los datos personales, generado por el responsable, de forma física, electrónica o en cualquier formato, previo a la recabación y tratamiento de sus datos, con el objeto de informarle sobre la finalidad del tratamiento, los datos recabados, así como la posibilidad de acceder, rectificar, oponerse o cancelar el tratamiento de los mismos;

Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;

Responsable: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, que decida y determine finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales;

Usuario: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

2. Principios y Deberes

- Calidad
- Confidencialidad
- Consentimiento
- Finalidad
- Información
- Lealtad
- Licitud
- Proporcionalidad
- Transparencia
- Temporalidad

Consentimiento

El responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse en forma:

1. Libre
2. Específica
3. Informada
4. Inequívoca

El silencio o la inacción no pueden considerarse por ningún motivo consentimiento por parte del titular.

El titular de los datos personales podrá revocar el consentimiento en cualquier momento, en ese caso, el tratamiento cesará y no podrá tener efectos retroactivos.

Deberes de los responsables:

•Destinar Recursos autorizados para la instrumentación de programas y políticas.

•Elaborar políticas y programas de protección de datos personales.

•Poner en práctica un programa de capacitación y actualización del personal.

•Revisar periódicamente las políticas y programas de seguridad de datos personales.

•Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorias.

•Garantizar a las personas, el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición.

Deberes de los responsables:

- Diseñar, desarrollar e implementar políticas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales.

- Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas o cualquier otra plataforma cumpla con la protección de datos personales.

- Cumplir con políticas y lineamientos.

- Adoptar las medidas de seguridad necesarias para la protección de datos.

- Elaborar y presentar al Instituto un Informe correspondiente sobre las obligaciones previstas en la Ley.

Deberes de los responsables:

- Registrar ante el Instituto los Sistemas de Datos Personales, así como la modificación o suspensión de los mismos.

- Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales.

- Coordinar y supervisar la adopción de **medidas de seguridad** (conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de datos personales) a que se encuentren sometidos los sistemas de datos personales.

3. Aviso de Privacidad

El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento previo a que sus datos personales sean sometidos a tratamiento, a fin de que pueda tomar decisiones informadas al respecto.

Por regla general, el aviso de privacidad deberá ser puesto a disposición del titular previo a la obtención y recabación de los datos personales y difundido por los medios electrónicos y físicos con que cuente el responsable.

Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara, sencilla y comprensible.

Cuando resulte imposible dar a conocer al titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios establecidos para tal efecto.

El aviso de privacidad deberá contener la siguiente información:

- La identificación del responsable y la ubicación de su domicilio;
- El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
- Los datos personales que serán sometidos a tratamiento, así como de la existencia de un sistema de datos personales;
- Las finalidades del tratamiento para las cuales se recaban los datos personales, el ciclo de vida de los mismos, la revocación del consentimiento y los derechos del titular sobre éstos;
- Los mecanismos, medios y procedimientos disponibles para ejercer los derechos Acceso, Rectificación, Cancelación y Oposición; y
- El domicilio de la Unidad de Transparencia.

4. Medidas de seguridad

Con independencia del tipo de sistema de datos personales en el que se encuentren los datos o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las **medidas de seguridad** de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Niveles de seguridad

Básico: relativas a las medidas generales de seguridad cuya aplicación será obligatoria para el tratamiento y protección de todos los sujetos obligados.

Medio: se refiere a las medidas de seguridad requeridas para aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como los sistemas que contengan datos con los que se permita obtener evaluación de personalidad o perfiles de cualquier tipo en el presente pasado o futuro.

Alto: corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a ideología, religión, creencia, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados por fines policiales, de seguridad, prevención, investigación y persecución de delitos.

5. Documentos de seguridad

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión denominado **documento de seguridad**.

El responsable deberá elaborar el documento de seguridad que contendrá, al menos, lo siguiente:

I. El inventario de datos personales en los sistemas de datos;

II. Las funciones y obligaciones de las personas que intervengan en el tratamiento datos personales, usuarios y encargados, en el caso de que los hubiera;

III. Registro de incidencias;

IV. Identificación y autentificación;

V. Control de acceso; gestión de soportes y copias de respaldo y recuperación;

VI. El análisis de riesgos;

VII. El análisis de brecha;

VIII. Responsable de seguridad;

IX. Registro de acceso y telecomunicaciones;

X. Los mecanismos de monitoreo y revisión de las medidas de seguridad;

XI. El plan de trabajo; y

XII. El programa general de capacitación.

6. Sistemas de Datos Personales

Los **sistemas de datos personales** son un conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los sujetos obligados, tienen como finalidad cumplir con la transparencia, responsabilidad y licitud en su tratamiento.

El Instituto habilitará un registro de sistemas de datos personales, donde los sujetos obligados inscribirán los sistemas bajo su custodia y protección.

El registro debe contemplar como mínimo lo siguiente:

- Nombre y cargo del titular del sujeto obligado como responsable del tratamiento y los usuarios.
- Finalidad del tratamiento.
- Naturaleza de los datos personales contenidos en cada sistema.
- Forma de recabación, pertinencia, proporcionalidad y calidad de los datos.
- Las posibles transferencias.
- Modo de interrelacionar la información registrada.
- Ciclo de vida de los datos personales y tiempos de conservación.
- Medidas de seguridad.

7. Derechos de Acceso, Rectificación, Cancelación y Oposición

Toda persona por sí o a través de su representante, podrá ejercer los derechos de Acceso, Rectificación, Cancelación y/u Oposición al tratamiento de sus datos personales en posesión de los sujetos obligados, siendo derechos independientes, de tal forma que no pueda entenderse que el ejercicio de alguno de ellos sea requisito previo o impida el ejercicio de otro.

ARCO

Ejercicio de los derechos ARCO:

- Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular y en su caso, la identidad y personalidad con la que actúe el representante.

- El ejercicio de los derechos ARCO deberá ser gratuito.

- Se deberán establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO.

- Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del sujeto obligado, que el titular considere competente, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al afectado establezca el Instituto en el ámbito de sus respectivas competencias.

8. Unidades Responsables

Los responsables en materia de protección de datos personales en posesión de los sujetos obligados son:

- Comité de Transparencia
- Unidad de Transparencia

Atribuciones del Comité de Trasparencia:

- Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales.

- Instituir procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.

- Confirmar, modificar o revocar las solicitudes de derechos ARCO en las que se declare la inexistencia de los datos personales.

- Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la Ley.

- Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.

- Establecer programas de capacitación y actualización para los servidores públicos .

- Dar vista al órgano interno de control en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales.

Comité de Transparencia

Atribuciones de la Unidad de Transparencia:

- Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales.
- Gestionar las solicitudes para el ejercicio de los derechos ARCO.
- Establecer mecanismos para asegurar que los datos personales sólo se entreguen a su titular o su representante debidamente acreditados.
- Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;
- Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;

- Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO;

- Asesorar a las áreas del sujeto obligado en materia de protección de datos personales;

- Registrar ante el Instituto los sistemas de datos personales, así como su modificación y supresión; y

- Hacer las gestiones necesarias para el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales en posesión del responsable.

NUBE:

El responsable podrá utilizar servicios, aplicaciones e infraestructura de cómputo en la nube (modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente), de aquellos servicios en los que el proveedor:

I. Cumpla, al menos, con lo siguiente:

a) Aplique políticas de protección de datos personales con base en los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable;

b) Transparente y limite las subcontrataciones que involucren el tratamiento de datos personales;

c) Se abstenga de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y

d) Guarde confidencialidad respecto de los datos personales sobre los que se preste el servicio.

II. Cuente con mecanismos, al menos, para:

a) Dar a conocer cambios en sus políticas de protección de datos personales, privacidad o condiciones del servicio que presta;

b) Permita al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;

c) Establezca y mantenga medidas de seguridad adecuadas y verificables para la protección de los datos personales sobre los que se preste el servicio;

d) Garantice la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, e

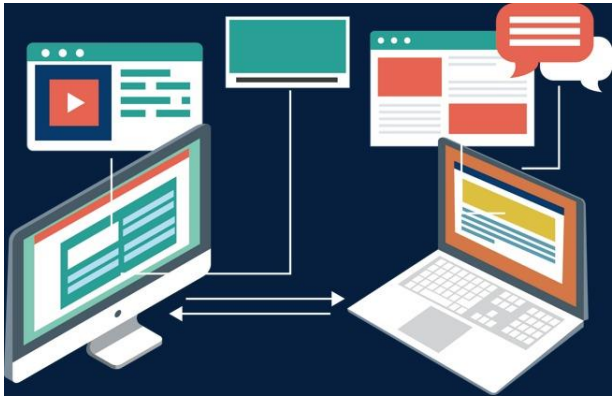
e) Impida el acceso a los datos personales a personas ajenas, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

9. Transferencia de Datos

Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en la Ley.

Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

En toda transferencia de datos personales, el responsable deberá comunicar al receptor de los datos personales las finalidades conforme a las cuales se tratan los datos personales frente al titular.



10. Tratamiento Intensivo o relevante

Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con la Ley impliquen el tratamiento intensivo o relevante de datos personales, deberá presentar ante el Instituto una evaluación de impacto en la protección de datos personales, para que éste emita recomendaciones especializadas, cuyo contenido tendrá como guía las disposiciones que para tal efecto emita el Sistema Nacional.

SISTEMA NACIONAL DE TRANSPARENCIA
ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES

Para efectos de la Ley se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales, el cual amerite una manifestación de impacto a la protección de datos personales, en función de los siguientes factores:

I. El número de titulares;

II. El público objetivo;

III. El desarrollo de la tecnología utilizada;

IV. La relevancia del tratamiento de datos personales en atención al impacto social o, económico del mismo, o bien, del interés público que se persigue;

V. Existan riesgos inherentes a los datos personales a tratar;

VI. Se traten de datos personales sensibles;

VII. Se traten de datos personales de forma masiva y continua; o

VIII. Se efectúen o pretenda hacer transferencias de datos.

11. Recurso, Verificación y Multas

Recurso de revisión: el recurso de revisión podrá interponerse, de manera directa, por correo certificado o por medios electrónicos, ante el Instituto, o ante la Unidad de Transparencia del sujeto obligado que haya dado respuesta a la solicitud de acceso, rectificación, cancelación u oposición a datos personales.

Verificación: el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, tiene la atribución de vigilar y verificar el cumplimiento de los principios y las disposiciones contenidas en la Ley.

La verificación podrá iniciarse:

- De oficio cuando el Instituto cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes.

- Por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la presente Ley y demás normativa aplicable.

- Por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia.

- Para verificar el cumplimiento de los principios, el tratamiento de los datos personales y la gestión de los sistemas de datos personales en posesión del responsable, para tal efecto el Instituto presentará un programa anual de verificación.

Medidas de Apremio:

El Instituto podrá imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:

I. La amonestación pública; o

II. La **multa**, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.

El incumplimiento de los sujetos obligados será difundido en los portales de obligaciones de transparencia del Instituto y considerados en las evaluaciones que realicen.

En caso de que el incumplimiento de las determinaciones del Instituto implique la presunta comisión de un delito o una de las conductas señaladas en la presente Ley, deberán denunciar los hechos ante la autoridad competente. Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos**.**

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, puede ser consultada en el siguiente link:

http://www.paot.org.mx/centro/leyes/df/pdf/2018/Ley_Protec_Datos_Pers_Posesion_Sujetos_Ob_10_04_2018.pdf

PAOT

PROCURADURÍA AMBIENTAL
Y DEL ORDENAMIENTO
TERRITORIAL DE LA CDMX