AGRICULTURA

SECRETARÍA DE AGRICULTURA Y DESARROLLO RURAL

SEGALMEX

SEGURIDAD ALIMENTARIA MEXICANA

LICONSA

POLÍTICA INTERNA DE GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES.

UNIDAD DE TRANSPARENCIA

Gerencia Jurídico Institucional
Dirección de Asuntos Jurídicos

ÍNDICE

I. INTRODUCCIÓN

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal.

En cumplimiento a lo dispuesto con el artículo 33, fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el responsable tiene el deber de establecer y mantener medidas de seguridad para la protección de los datos personales que reciba en ejercicio de sus facultades, para lo cual debe crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

Asimismo, de conformidad con el artículo 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, el responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, el cumplimiento de todos los principios, deberes, derechos y demás obligaciones que establece la normatividad en materia de protección de datos personales.

2. OBJETIVO

Establecer los principios generales que deberán observar los servidores públicos en el ejercicio de las funciones para el tratamiento de los datos personales, de conformidad con lo establecido en el artículo 7 de los Lineamientos Generales de Protección de Datos Personales para el Sector Publico.

Establecer las obligaciones y atribuciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para el correcto cumplimiento en el tratamiento de los datos personales.

Fortalecer los conocimientos para la correcta observancia de los principios y deberes que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Publico.

Cumplir con las disposiciones que emanan de la Ley de la materia y demás normatividad aplicable, para garantizar el correcto tratamiento de los datos personales.

Establecer mecanismos que coadyuven a comprobar que la Política interna de gestión de Protección de Datos Personales, se ejecuten de conformidad con la normatividad en materia de protección de datos personales, así como demás disposiciones aplicables.

3. MARCO JURÍDICO

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Acuerdo mediante el cual se aprueban los Instrumentos Técnicos que refiere el Titulo Decimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Demás leyes aplicables en materia de protección de datos personales.
- Demás leyes aplicables en materia de protección de datos personales.

4. GLOSARIO

Instituto: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados.

Sujeto obligado: LICONSA, S.A. DE C.V.

Titular: La persona física a quien corresponden los datos personales.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

5. PRINCIPIOS GENERALES DE PROTECCIÓN DE DATOS GENERALES.

El artículo 7 de los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, establece que en todo tratamiento de datos personales se deberá observar los principios rectores de la protección de datos personales:

- Licitud.
- Finalidad.
- Lealtad.
- Consentimiento.
- Calidad.
- Proporcionalidad.
- Información.
- Responsabilidad.

En observancia al correcto tratamiento de los datos personales en posesión de este Sujeto Obligado, la aplicación de los Principios Generales de Protección de Datos Personales, se formalizan como sigue:

Principio de Licitud.

- Llevar a cabo el tratamiento de los datos personales de conformidad con las atribuciones o facultades que establecen las leyes en materia de protección de datos personales, respetando los derechos y libertades de los titulares.

Principio de Finalidad.

a) Verificar que los tratamientos de datos personales que se realicen atiendan los fines específicos o determinados (concretas, licitas, explicitas y legitimas) y que sean acordes a las atribuciones o facultades de este Sujeto Obligado.

b) Verificar que las finalidades para el tratamiento de los datos personales estén relacionadas con las atribuciones normativas de esta Dependencia.

c) Identificar las finalidades que no fueron informadas en los avisos de privacidad, verificando que estas se encuentren dentro de las atribuciones legales para el tratamiento de los datos personales y recabar el consentimiento del titular al momento de obtener sus datos personales.

Principio de Lealtad.

a) Garantizar que los datos personales recabados por este sujeto obligado, no se obtengan a través de medios engañosos o fraudulentos.

b) Garantizar que los tratamientos de datos personales que lleva a cabo esta dependencia no den lugar a la discriminación, trato injusto o arbitrario en contra del titular.

c) Supervisar que los datos personales, sean tratados conforme a lo señalado en el aviso de privacidad y las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y sus Lineamientos.

Principio de Consentimiento.

a) Garantizar que previo a la obtención de los datos personales de los titulares y después de haberles puesto a disposición los avisos de privacidad, se cuente con su consentimiento (tácito o expreso) para el tratamiento de datos personales que lleva a cabo este Sujeto Obligado (salvo las causales de excepción señaladas en el artículo 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados).

b) Verificar que el consentimiento que se obtenga de los titulares sea libre, específico e informado.

c) Cuando los datos personales se recaben directamente del titular y se requiera el consentimiento, éste deberá solicitarse previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad.

d) Cuando los datos personales se recaben indirectamente del titular y se requiera el consentimiento, no se podrán tratar los datos personales hasta que se cuente con la manifestación libre, específica e informada del titular, en la que autorice el tratamiento de sus datos personales de manera tácita o expresa según corresponda.

e) Atender las solicitudes de revocación del consentimiento, mismas que podrán ser representadas por el titular en cualquier momento del tratamiento.

Principio de Calidad.

a) Adoptar las medidas necesarias, para mantener exactos, completos, correctos y actualizados los datos personales que son tratados por esta Dependencia.

b) Establecer los plazos de conservación de los datos personales, de conformidad con los instrumentos de clasificación archivística.

c) Establecer y documentar los procedimientos para la conservación y supresión de los datos personales que son tratados en este sujeto obligado.

Principio de Proporcionalidad.

a) Garantizar que los datos personales que se recaben sean los adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento.

b) Garantizar que los datos personales recabados contengan los datos mínimos necesarios en relación a las finalidades que justifican su tratamiento.

Principio de Información.

a) Poner a disposición del titular los avisos de privacidad que correspondan (Simplificados e Integrales), antes y después de la obtención de los datos personales.

b) Implementar mecanismos para que el titular pueda manifestar su negativa para el tratamiento de datos personales para finalidades o transferencias que requieran su consentimiento.

c) Difundir los avisos de privacidad por medios electrónicos y físicos.

d) Ubicar los avisos de privacidad en lugares visibles que faciliten la consulta del titular.

e) Verificar que los avisos de privacidad integrales se encuentren de manera permanente en el portal de internet de este sujeto obligado.

f) Poner a disposición del titular los nuevos avisos de privacidad cuando se actualicen los siguientes supuestos.

I. Cambie la identidad de este Sujeto Obligado.
II. Se requiera recabar datos personales sensibles.
III. Cambien las finalidades señaladas en el aviso de privacidad.
IV. Se modifiquen las condiciones de las transferencias de datos personales o se pretendan realizar transferencias no previstas inicialmente y el consentimiento del titular sea necesario.

Principio de Responsabilidad.

a) Elaborar políticas y programas de protección de datos personales, tomando en cuenta el desarrollo tecnológico y las técnicas existentes.

b) Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y deberes en materia de protección de datos personales.

c) Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

d) Establecer un sistema de supervisión y vigilancia interna y/o externa, para comprobar el cumplimiento de las políticas de protección de datos personales.

e) Cuando se requiera poner en práctica el procedimiento para atender dudas y quejas de los titulares.

f) Garantizar que las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la ley general de protección de datos personales en posesión de sujetos obligados.

g) Implementar mecanismos para evidenciar el cumplimiento de los principios, deberes y obligaciones ante los Titulares y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

POLÍTICAS DE GESTIÓN Y TRATAMIENTOS DE DATOS PERSONALES

TRATAMIENTO DE DATOS PERSONALES

El tratamiento de datos personales que realicen las unidades administrativas deberá cumplir con los principios, deberes y obligaciones que prevé la LGPDPPSO.

Para ello los servidores públicos del Sujeto Obligado identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las unidades administrativas, de acuerdo con lo que establece la LGPDPPSO y los Lineamientos Generales, y según el ciclo de vida de los datos personales.

La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados.

- Obtención de Datos Personales.

Es importante destacar que los datos personales que obtiene el Sujeto Obligado son básicamente para formar expedientes de personas físicas o morales para que con base en las Reglas de Operación de los Programas de Subsidio se otorguen los apoyos al campo mexicano.

- USO de Datos Personales.

CONSERVACIÓN Y CICLO DE VIDA DE LOS DATOS PERSONALES.

El plazo de conservación de los datos personales no debe exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, ni aquél que se requiera para cumplir con:

Las disposiciones legales establecidas en la Ley General de Archivos.

Las disposiciones aplicables en la materia de que se trate.

Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

- El periodo de bloqueo.

Es importante señalar que, en particular, el artículo 24 la Ley General, establece que se deben documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales respecto de cada tratamiento que se efectúe por las unidades administrativas.

- Conclusión del plazo de conservación

Una vez concluido el plazo de conservación, y siempre que no exista disposición legal o reglamentaria que establezca lo contrario, las unidades administrativas deben proceder a la supresión de los datos personales. En este caso, deberán de informarlo a la Unidad de Transparencia, quien lo hará del conocimiento del Comité de Transparencia, a efecto de que determine lo conducente.

Es importante recordar que el plazo de conservación debe incluir un periodo de bloqueo, ya que los datos personales deben ser bloqueados antes de que sean eliminados o suprimidos.

Además, en cuanto a los datos personales sensibles, el responsable debe realizar esfuerzo razonable para limitar el periodo de tratamiento al mínimo indispensable.

BLOQUEO DE LOS DATOS PERSONALES.

El bloqueo se define como la acción que tiene por objeto impedir el tratamiento de los datos personales para cualquier finalidad, con excepción de su almacenamiento y acceso para determinar posibles responsabilidades, hasta el plazo de prescripción correspondiente.

Las personas servidoras públicas están obligadas:

Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales. Concluido dicho periodo se deberá proceder a su supresión.

El Sujeto Obligado tendría que bloquear los datos personales después de transcurridos los 15 años del tratamiento (10 años en que el titular tuvo una relación con estos más 5 años que establecía la norma).

El tiempo en que los datos personales deberán estar bloqueados depende de los plazos legales que establezca la legislación de índole archivística para determinar posibles responsabilidades en relación con el tratamiento de los datos personales, lo cual dependerá, a su vez, de la materia de que se trate. Concluido el periodo de bloqueo, el responsable deberá suprimir los datos personales.

El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales.

DURANTE LA ETAPA DE MONITOREO.

La Unidad de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, la elaboración de un reporte, en el que deberá precisarse, lo siguiente:

1) Si se elaboraron los avisos de privacidad.

2) Si se ha definido y establecido medidas de seguridad administrativas, técnicas y físicas.

3) Si se ha revisado el marco normativo que regula el tratamiento de datos personales.

4) Si se contemplan medidas de seguridad específicas o adicionales.

5) Si se han definido las funciones, obligaciones de cada servidor público que trata datos personales.

6) Si se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando durante el tratamiento de datos personales.

7) Si se ha elaborado el inventario de datos; el análisis de riesgo; así como el análisis de brecha.

8) Si se monitorean y revisan de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones.

DURANTE LA ETAPA DE SUPERVISIÓN.

La Unidad de Transparencia analizará los reportes de las áreas administrativas, verificando aquellos puntos en los que se hubiera reportado “No” como respuesta y se emitirá un dictamen o ficha técnica en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.

El Sujeto Obligado, siempre ha cumplido con toda la normatividad aplicable, en la materia de protección de datos personales. En tal sentido, la Unidad de Transparencia se ha ocupado de sensibilizar y llevar a cabo capacitaciones a las diversas unidades administrativas por conducto del INAI y sus labores cotidianas realizan actividades vinculadas al tratamiento de datos personales y deban elaborar avisos de privacidad, y/o atender solicitudes de ejercicio de derechos ARCO.

Para lograr la ejecución de esta línea estratégica el área de Tecnologías de la información, realizará de manera constante al interior del Sujeto Obligado, campañas de promoción y difusión de diversos materiales sobre la protección de datos personales a través del correo electrónico institucional.

LAS SANCIONES.

Cuando la Unidad de Transparencia, tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá informarlo al Comité de Transparencia del Sujeto Obligado para que éste realice a la unidad administrativa correspondiente un exhorto para que lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo para los datos personales.

De manera adicional, es importante que las personas servidoras públicas que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 163 de la LGPDPPSO serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, mismas que son las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

II. Incumplir los plazos de atención previstos en la LGPDPPSO para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la LGPDPPSO, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales; VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la LGPDPPSO; VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;

VII. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la LGPDPPSO;

EL PROCESO DE ATENCIÓN DE LOS DERECHOS ARCO

Del Procedimiento para el Acceso, Rectificación, Cancelación y Oposición de los Datos Personales en Posesión del Sujeto Obligado.

La Unidad de Transparencia, las y los titulares de las áreas atenderán las solicitudes de acceso, rectificación, cancelación u oposición de datos personales, conforme a lo dispuesto en la Ley Federal de Transparencia y Acceso a la Información Pública.

Las solicitudes de acceso, rectificación, cancelación u oposición de datos personales podrán recibirse por cualquiera de los siguientes medios:

1) Por escrito material o en los formatos específicos que para el efecto apruebe el INAI presentada personalmente en la UT, a través de correo ordinario, correo certificado o servicio de mensajería;

2) De manera verbal, en forma presencial en la UT por el interesado o su representante legal;

3) Por correo electrónico; y

4) Por la Plataforma Nacional de Transparencia; En el caso de solicitudes de acceso, rectificación, cancelación y oposición de datos personales, presentadas mediante

escrito material, la UT las capturará y registrará en la PNT, a más tardar al día hábil siguiente de que tenga conocimiento de estas. Tanto los formatos de solicitudes de acceso, rectificación, cancelación u oposición de datos personales aprobados por el INAI, como los vínculos a la Plataforma Nacional de Transparencia deberán estar disponibles en la Página Web del Sujeto Obligado.

Para dar respuesta a las solicitudes de acceso, rectificación, cancelación u oposición de datos personales se deberá observar lo siguiente:

I. Si la solicitud de acceso, rectificación, cancelación u oposición de datos personales es procedente, el área responsable remitirá el oficio de respuesta debidamente fundado y motivado; la UT lo notificará a la persona interesada en un plazo que no excederá de quince días hábiles contados a partir de la recepción de la solicitud;

II. En caso de que la solicitud de datos personales implique un costo por reproducción de la información que exceda de veintiún hojas simples, en el oficio de notificación de respuesta se hará del conocimiento de la persona solicitante los costos por conceptos de reproducción de la información;

III. Si la respuesta de la Unidad Administrativa responsable considera improcedente la solicitud de acceso, rectificación, cancelación u oposición de datos personales, deberá fundar y motivar las razones por las cuales no procedió la solicitud en los términos de la Ley Reglamentaria del Artículo 6° Constitucional, debiendo ser notificado por la UT a la persona interesada;

IV. Si la solicitud de acceso, rectificación, cancelación u oposición de datos personales no es clara ni precisa, el área responsable remitirá a la UT el oficio de prevención fundado y motivado para que aclare o complete su solicitud; la UT notificará la prevención a la persona solicitante, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación;

V. Cuando así lo justifiquen las circunstancias del caso, la Unidad Administrativa mediante oficio debidamente fundado y motivado podrá notificar a la persona solicitante, a través de la UT, la ampliación del plazo hasta por quince días hábiles

más, para dar respuesta a la solicitud de acceso, rectificación, cancelación u oposición de datos personales;

VI. Si en la solicitud de acceso, rectificación, cancelación u oposición de datos personales, los datos respecto de los cuales se ejerciten estos derechos no son localizados en los sistemas de datos personales del Sujeto Obligado, se hará del conocimiento de la persona solicitante mediante oficio.

Cuando una solicitud de acceso, rectificación, cancelación u oposición de datos personales sea presentada ante cualquier Unidad Administrativa del Sujeto Obligado diferente a la UT, la persona servidora pública que la reciba, deberá indicar al particular la ubicación física de la UT o, en su caso, turnar la solicitud a la UT, a más tardar en el término de veinticuatro horas hábiles siguientes a la recepción de la solicitud.

Las y los titulares de las Unidades Administrativas del Sujeto Obligado deberán observar los plazos para la atención interna de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales que reciban de la UT, conforme a lo siguiente:

1) Dentro de los cuatro días hábiles siguientes a que reciban una solicitud de acceso, rectificación, cancelación u oposición de datos personales, enviarán, mediante oficio, a la UT, la respuesta a la misma;

2) Dentro de las 24 horas siguientes a que reciban una solicitud de acceso, rectificación, cancelación u oposición de datos personales pedirán, mediante oficio, a la UT prevenga a la persona solicitante para que complete o aclare su solicitud;

3) Dentro de los cinco días hábiles siguientes a que reciban una solicitud de acceso, rectificación, cancelación u oposición de datos personales harán del conocimiento mediante oficio fundado y motivado a la UT, que la solicitud es improcedente, exponiendo las razones de dicha circunstancia, y

4) Dentro de los cinco días hábiles siguientes a que reciban una solicitud de acceso, rectificación, cancelación u oposición de datos personales harán del

conocimiento, mediante oficio fundado y motivado a la UT, que los datos personales de los cuales se ejerciten los derechos ARCO no son localizados en los Sistemas de Datos Personales del Sujeto Obligado

La Unidad de Transparencia, tomará en cuenta la oferta que brinda el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), para difundir a los servidores públicos la calendarización sobre los diversos temas de capacitación en materia de protección de datos personales, con la finalidad de que los servidores públicos estén debidamente capacitados en la normatividad de referencia. Bajo ese contexto, los servidores públicos que participen y se involucren en los temas de capacitación que engloba la LGPDPPSO, podrán contar con información certera sobre el cumplimiento y atención de sus obligaciones en materia de protección de datos personales, dando cumplimiento a los deberes y principios previstos en la normatividad, dado que el tema de protección de datos personales es competencia de todos los servidores públicos que participen y se involucren en la protección de la información confidencial que obre en los archivos del sujeto obligado.


LICONSA