PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES DE IMPRESORA Y ENCUADERNADORA PROGRESO, S.A. DE C.V.

1.- Presentación

El concepto de protección de datos personales, encuentra su fundamento en el segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidad Mexicanos, otorgando a la población el derecho de libre decisión sobre el uso de sus datos personales, estableciendo como límite a la seguridad nacional, las disposiciones de orden público, la seguridad y salud públicas y la protección de los derechos de terceros.

Tras la publicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en el Diario Oficial de la Federación (DOF) el 11 de junio de 2002 (abrogada en el año 2016), México da inicio a la regulación de la protección de datos personales, y es precisamente la reforma al artículo 16 del año 2009, la que otorga el derecho a la protección de datos personales, dando paso a la creación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares en 2010, pero es en el año 2014 cuando se da inicio al estudio de la creación de una Ley General en la materia, pero de la información en posesión del sector público.

Es en el mes de enero del año 2017, cuando se publica la **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)**, en la cual se establecen las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de sujetos obligados (Artículo 1, cuarto párrafo de la LGPDPPSO), y en el año 2018 es cuando se realiza la publicación de **los Lineamientos Generales de Protección de Datos Personales para el Sector Publico (Lineamientos Generales)**, los cuales enlistan las obligaciones en el tratamiento de datos personales y el ejercicio de los derechos ARCO, además de delimitar los principios rectores de la materia que son, licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

2.- Objetivo

El objetivo primordial de este documento, es establecer el marco de trabajo para que **Impresora y Encuadernadora Progreso, S.A. de C.V. (IEPSA)**, de cabal cumplimiento a lo estipulado en la LGPDPPSO y en los Lineamientos Generales, estableciendo un **sistema de gestión**, entendido como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales. (Artículo 34 de la LGPDPPSO y artículo 65 de los Lineamientos Generales).

De acuerdo a la *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales* del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) actualizada en el mes de junio del año 2015, la importancia de los sistemas de gestión de datos personales, es garantizar a las personas la privacidad y su autodeterminación informativa; el INAI propone un sistema denominado **"Planificar-Hacer-Verificar-Actuar"**, configurando así las 4 fases de dicho sistema de gestión, que ayudan a los Sujetos Obligados a la implementación de Programas de protección de datos; las fases de tal sistema se definen según lo siguiente:

- ✓ ***Planificar:*** identificar políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por el responsable o encargado.
- ✓ ***Hacer****:* implementar y operar las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
- ✓ ***Verificar****:* evaluar y medir los resultados de lo implementado, a fin de verificar el adecuado funcionamiento del sistema de gestión y el logro de la mejora esperada.
- ✓ ***Actuar:*** adoptar medidas correctivas y preventivas en función de los resultados de la revisión realizada, o de otra información relevante, para lograr la mejora continua.
- ✓

Derivado de lo anterior, este programa tiene el **objetivo** de establecer las dinámicas internas de trabajo necesarias para brindar la debida protección a los datos personales que se encuentren en posesión de IEPSA, así como garantizar la constante revisión y actualización de los parámetros de protección que esta Entidad haya establecido en su Documento de Seguridad para la Protección de Datos Personales.

3.- Alcance

El contenido del presente documento, es de aplicación y observancia general y de carácter obligatorio para todas las personas servidoras públicas de IEPSA, que lleven a cabo el tratamiento de datos personales, por lo que dichas personas servidoras públicas deberán de cumplir con todas las obligaciones previstas en la LGPDPPSO, así como la aplicación de todos los principios que establece la norma, además de las personas prestadoras de servicios profesionales (en su caso), y personal externo a la Entidad, entre los que están los encargados.

4.- Responsables

De acuerdo en lo estipulado en el artículo 84 de la LGPDPPSO, el Comité de Transparencia es la autoridad máxima en materia de protección de datos, por lo que le corresponderá, entre otros, el coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de datos personales que estén en posesión de IEPSA, y también será el propio Comité quien proponga los cambios y mejoras que considere pertinentes, tales actividades deberán ser cumplidas por las personas servidoras publicas adscritas a las Unidades Administrativas que realizan el tratamiento de datos personales.

5.- Inventario de tratamiento de Datos Personales

En primera instancia, las Unidades Administrativas deberán de realizar un análisis del tratamiento de datos personales que lleven a cabo, esto será realizado mediante la elaboración de un Inventario de Datos Personales; entendiéndose que el inventario es el control de los tratamientos que se realizan en la Entidad a través de las Unidades Administrativas, en el cual se identificarán lo siguientes aspectos:

a) Identificación de los procesos en los que se realiza el tratamiento de datos personales.
b) Realizar la definición de las Unidades Administrativas a cargo de los procesos enlistados en el punto anterior.
c) De acuerdo al ciclo de vida de los datos personales (figura 1), se deberá de determinar lo siguiente:

c.1) Fuente de obtención de los datos personales:

Del titular:

- De manera física por parte del titular o bien, por su representante.
- Vía telefónica.
- Por correo electrónico.
- Por internet o un sistema informático.
- Por medio de un escrito presentado en las oficinas del sujeto obligado.
- Por medio de un escrito enviado por mensajería.

Mediante una transferencia.

- Por quien transfiere los datos personales y para qué fines.
- Medios por los que se realiza la transferencia.

De una fuente de acceso público

c.2) Verificar qué tipo de datos personales se tratan y si estos son sensibles.

c.3) Lugar en el que se almacenan y realiza el tratamiento de datos personales.

- Sección, serie y subserie (en su caso) de archivos.
- Formato en que se encuentran los datos personales (físico y/o electrónico)
- Ubicación de la base de datos.

c.4) Determinar la finalidad de la utilización de los datos personales.

- La finalidad se determina como “acciones más específicas de los procesos de los que derivan los tratamientos de datos personales”; se deberá de determinar si es requerido o no el consentimiento del titular (tácito o expreso y por escrito), o si es que no se requiere,

definir los supuestos se actualizan de acuerdo a lo estipulado en el artículo 22 de la LGPDPPSO, indicando por último, el marco jurídico aplicable.

c.5) Definir a las personas servidoras públicas que tienen acceso a los datos personales y con qué finalidad.

c.6) Identificar si existen encargados en el tratamiento de datos personales, así como el número de contrato, pedido o convenio que corresponda.

c.7) Identificar a los terceros externos a la Entidad a quienes se comunican los datos personales y los fines de las transferencias, en el caso de que se realicen, así como señalar si es necesario el consentimiento del titular para la transferencia.

c.8) En caso de que suceda, indicar si los datos personales se difunden.

c.9) El plazo de conservación deberá de estar contenido en los instrumentos de clasificación archivística, por lo que es importante tener bien definida la serie documental,

Figura 1.- *Ciclo de vida de los datos personales.*
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2021). Programa de Protección de Datos Personales. https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/DocumentoOrientadorPPDP.docx [Fecha de consulta: 15 de enero de 2024]

6. Obligaciones

6.1 Obligaciones transversales.

Las presentes versan sobre los deberes de seguridad y confidencialidad, las cuales deben de observarse en cualquier etapa del ciclo de vida de los datos personales, desde su obtención, hasta su eliminación.

a) Medidas de Seguridad.

El deber de seguridad consiste en la implementación de medidas físicas, técnicas y administrativas para proteger los datos personales contra el daño, pérdida, alteración, destrucción, su uso, acceso o tratamiento no automatizado, y garantizar la confidencialidad, integridad y disponibilidad.

Esto se traduce a las medidas de seguridad que son todas aquellas acciones que permiten la protección de los datos personales y que son de carácter administrativo, técnico y físico. Las medidas de seguridad administrativas van desde los procedimientos institucionales para la gestión de la información hasta la sensibilización y capacitación del personal en materia de protección de datos personales.

Por otro lado, las medidas de seguridad físicas son los mecanismos que protegen el entorno físico de los datos personales, se puede entender lo anterior, por ejemplo, como la verificación y control de los accesos a las instalaciones e información, la prevención del deterioro de las instalaciones físicas o áreas donde se encuentre la información, brindar protección a los recursos móviles, cuando salgan de la Entidad y/o proporcionar mantenimiento eficaz a los equipos que contienen datos personales, entre otros.

Por último, en este rubro, las medidas de seguridad técnicas se describen como las acciones que tengan que ver con hardware y software y que conlleven proteger el entorno digital de los datos personales, podría hablarse por ejemplo de la protección de bases de datos al ser utilizadas únicamente por usuarios identificados, realizar configuraciones de seguridad para la adquisición, desarrollo y mantenimiento, por mencionar algunas.

b) Documento de Seguridad

El responsable deberá de elaborar un Documento de Seguridad, el cual incluirá los siguientes rubros: el inventario de datos personales, la denominación de la Unidad Administrativa, nombre del sistema o inventario que contenga los datos personales, la finalidad u objetivo del sistema, fundamento legal, listado de los datos personales que contiene el sistema, denominación del cargo del responsable del manejo de los datos, funciones específicas al tratamiento de datos personales, obligaciones, denominación del

cargo del administrador del sistema, funciones y obligaciones, denominación del cargo de los usuarios del sistema, funciones y obligaciones, además de la descripción de la estructura del sistema que contiene los datos personales.

Deberá de incluir además, el análisis de riesgos, el análisis de brecha, el plan de trabajo, mecanismos de monitoreo y el programa general de capacitación.

c) Vulneraciones

Sin afectación de las vulneraciones señaladas en la normatividad aplicable, serán consideradas vulneraciones de seguridad la pérdida o destrucción no autorizada, robo, extravío o copia no autorizada, el uso, acceso o tratamiento no autorizado y/o daño, alteración o modificación no autorizada.

d) Confidencialidad

En necesario considerar y establecer todos aquellos controles dirigidos a las personas servidoras públicas que intervengan en los procedimientos de tratamiento de datos personales, para que guarden confidencialidad sobre éstos, obligación que se mantendrá vigente aun si la relación con los datos personales se da por concluida, es importante destacar que la capacitación es necesaria para generar conciencia sobre el tema; dentro de las actividades que se deben observar, se encuentra el establecer cláusulas en los contratos que se celebren con los encargados, que los obliguen a guardar confidencialidad respecto de los datos personales. Estos controles deben de ser incluidos en las medidas de seguridad.

6.2 Obligaciones de la etapa de Obtención de los datos personales.

a) Licitud

El tratamiento de datos personales, deberá de realizarse en apego a las facultades y atribuciones normativas que le han sido conferidas a cada Unidad Administrativa, de acuerdo a lo establecido en la LGPDPPSO, los Lineamientos Generales y el Manual de Operación de Impresora y Encuadernadora Progreso, S.A. de C.V., y los demás instrumentos jurídicos que resulten aplicables, siempre respetando los derechos y libertades de las personas titulares.

Es necesario realizar un análisis respecto de las atribuciones de cada Unidad Administrativa, en específico en el Manual de Organización de IEPSA, para establecer claramente la necesidad que surge, para cada una de ellas, de recabar datos personales y que la justificación de esto, esté directamente ligado a sus actividades.

b) Lealtad

El tratamiento y obtención de datos personales nunca podrá realizarse en contraposición de lo que avale la normatividad aplicable, por lo que siempre deberá de procurarse la protección de los intereses del titular y la expectativa razonable de privacidad, que es la confianza que el titular ha depositado en el sujeto obligado respecto a que sus datos personales serán tratados conforme a lo señalado en el Aviso de Privacidad y en cumplimiento de las disposiciones previstas en la LGPDPPSO y los Lineamientos Generales.

Los datos personales no deben de obtenerse o tratarse a través de medios engañosos o fraudulentos, lo cual se entiende como aquellos que se utilicen para tatar los datos personales con dolo, mala fe o negligencia (Artículo 11 de los Lineamientos Generales). Por lo tanto, de acuerdo a las facultades establecidas para cada Unidad Administrativa que trate datos personales, se debe garantizar que las actividades por las cuales se obtengan los datos personales no deben de corresponder a las características en listadas con anterioridad (dolo, mala fe o negligencia).

Derivado de lo anterior, se deberán de realizar Avisos de Privacidad en apego a los establecido para ello en la LGPDPPSO, con la información suficiente respecto del tratamiento de que se le da a los datos personales, incluyendo en cada uno la finalidad de los tratamientos que prevé, la redacción del aviso deberá de ser clara y concreta, sin que permita que haya lugar a alguna confusión.

Si bien es cierto que esta obligación inicia con la obtención de los datos personales, deberá de mantenerse vigente hasta la conclusión de la relación con ellos.

c) Información

Los titulares deben de conocer completamente el tratamiento que se les dará a sus datos personales, quien es la persona responsable del tratamiento, la finalizad de la utilización de sus datos, con quien serán compartidos y como ejercer los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) y la portabilidad.

Es al Aviso de Privacidad el documento por el cual se cumple con la obligación de información, ya que es a través de éste que se establecen públicamente las características del tratamiento de datos personales que realiza la Entidad, en este entendido cada Unidad Administrativa deberá de realizar un Aviso de Privacidad, atendiendo lo siguiente:

1.- Realizar un Aviso de Privacidad por cada tratamiento que se realice.
2.-Respetar la estructura de los modelos de Aviso de Privacidad de la herramienta “Generador de Avisos de Privacidad” (https://generador-avisos-privacidad.inai.org.mx/)

3.- Realizar cada Aviso de Privacidad en sus dos modalidades: simplificada y general.
4.- Los Avisos de Privacidad deberán difundirse por medios electrónicos, en sus dos modalidades, en el portal de internet de IEPSA, sin menos cabo de que éstos deberán estar disponibles para su consulta física en la Entidad.
5.- El Aviso de Privacidad simplificado deberá de estar puesto a disposición de manera permanente.

d) Medidas compensatorias

IEPSA deberá de aplicar medidas compensatorias, que son los mecanismos alternos por los que se da conocer el Aviso de Privacidad Simplificado, cuando resulte imposible para la Entidad darlo a conocer directamente al titular o que conlleve esfuerzos desproporcionados, esto se podrá realizar a través de medios de comunicación masiva o cualquier medio de amplio alcance como lo es el Diario Oficial de la Federación o diarios de circulación nacional.

Resultan esfuerzos desproporcionados cuando el número de titulares impida el poner a disposición de cada uno el Aviso de Privacidad directamente, implicando para el responsable un costo excesivo de acuerdo a su suficiencia presupuestaria.

La imposibilidad de dar a conocer al titular el Aviso de Privacidad de manera directa, se materializa cuando el responsable no tiene los datos personales necesarios para establecer contacto con el titular, ya sea porque no obran en sus expedientes o sistemas o bien por que éstos no están actualizados.

Cuando el supuesto de la aplicación de medidas compensatorias aplique, IEPSA debe determinar si es necesario tener la autorización del Instituto, según lo estipulen los Criterios Generales para la Implementación de Medidas Compensatorias en el Sector Público del Orden Federal, Estatal y Municipal, e implementar dichas medidas de acuerdo también a la normatividad mencionada.

e) Consentimiento

Para el tratamiento de datos personales, el responsable debe de tener el consentimiento de su titular, a excepción de lo considerado en el artículo 22 de la LGPDPPSO, que a la letra dice:

> **"Artículo 22.** El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:
>
> **I.** Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;

II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;

IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;

V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;

VIII. Cuando los datos personales figuren en fuentes de acceso público;

IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o

X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia."

En su caso, el consentimiento del titular debe ser obtenido de **manera libre** (sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de la voluntad del titular), **especifica** (referida a finalidades concretas, lícitas, explicitas y legítimas que justifiquen el tratamiento) e **informada** (que el titular tenga el conocimiento del Aviso de Privacidad previo al tratamiento a que serán sometidos sus datos personales) (artículo 20 de la LGPDPPSO).

Para tal efecto, IEPSA debe de dar a conocer al titular el Aviso de Privacidad que corresponda, para posteriormente realizar una solicitud de consentimiento redactada de manera clara, siempre acorde del perfil de titular.

Ahora bien, el consentimiento del titular puede ser manifestado de manera **expresa**, de forma verbal, por escrito mediante firma autógrafa, o de manera electrónica, por cualquier medio de autenticación, esta manera de manifestar el consentimiento se aplica por exigencia de una ley o disposiciones en la materia, no habiéndose actualizado los supuestos antes enlistados del artículo 22 de la LGPDPPSO, en todos los demás casos, el consentimiento se expresa de manera **tácita**.
En el caso del consentimiento y acreditación de la identidad de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada por la ley, IEPSA deberá observar lo dispuesto en los artículos 78, 78, 80 y 81 de los Lineamientos Generales, identificando primeramente los tratamientos que corresponden a las

personalidades mencionadas, una vez hecho esto se debe de poner a disposición de los padres , tutores o representantes legales el Aviso de Privacidad e implementar actividades que permitan tener certeza de que la persona que otorga el consentimiento cuenta con las facultades legal suficientes para hacerlo.

En este orden de ideas, las personas servidoras públicas de IEPSA que sean partícipes del tratamiento de datos personales de menores de edad deberán conocer la Ley General de Niñas, Niños y Adolescentes, con el objetivo de conocer los derechos de este sector poblacional, para así privilegiar el interés superior del menor.

f) Datos sensibles

Los datos sensibles únicamente se pueden tratar si se cuenta con el consentimiento expreso del titular, Existen datos personales que puedan causar discriminación para sus titulares dado el origen étnico, estado de salud, información genética, opiniones políticas, por su creencia religiosa, su moral y su preferencia sexual.

IEPSA debe de verificar la legalidad del tratamiento de los datos sensibles con el objetivo de que cumpla con la finalidad de mismo, buscando así que se justifique debidamente y evitar en todo momento qué el tratamiento no tenga como consecuencia la discriminación.

g) Proporcionalidad

Los datos personales que sean recabados deberán de ser solo aquellos que resulten necesarios, adecuados y relevantes para el cumplimiento de las atribuciones que le son conferidas a cada Unidad Administrativa.

Las unidades administrativas de IEPSA que realicen el tratamiento de datos personales, deberán de identificar claramente los datos que requieren para cada una de las finalidades, además se debe revisar que únicamente sean solicitados aquellos que resultan indispensables, requiriendo el mínimo posible de datos personales.

6.3 Obligaciones de la etapa de Uso de los datos personales.

a) Finalidad

La finalidad del tratamiento de los datos personales, es la justificación del mismo, y que se puede conceptualizar como:

Concretas: la finalidad del tratamiento es la consecución de fines específicos o determinados, en los que no se admiten errores, distintas interpretaciones, incertidumbre, dudas o confusión en el titular.

Explícitas: las finalidades se expresan de manera clara en el Aviso de Privacidad.

Lícitas: las finalidades que justifican el tratamiento de los datos personales son acordes con las facultades del responsable.

Legítimas: las finalidades del tratamiento se encuentran habilitadas por el consentimiento del titular.

IEPSA deberá verificar que las finalidades de cada tratamiento que realiza esta directamente ligado a las facultades que tenga conferida cada unidad administrativa de la que se trate, dentro de la misma verificación, se debe incluir la revisión al Aviso de Privacidad para constatar que dichas finalidades sean enlistadas en el de manera clara, sin olvidar identificar cuales finalidades requieren consentimiento.

En el caso de que el tratamiento de los datos personales, tenga una finalidad distinta a las indicadas en el Aviso de Privacidad, será necesario contar con atribuciones legales para el caso y el consentimiento del titular, a menos que se trate de una persona desaparecida.

b) Calidad

Esta obligación se refiere a que los datos personales deben de mantenerse exactos, completos, correctos y actualizados, en especial si fueron obtenidos de manera indirecta del titular.

Los datos personales son exactos y correctos cuando no presentan errores, se consideraran completos cuando permiten el cumplimiento de las finalidades para las que fueron recabados y se entenderá que están actualizados cuando se someten totalmente a la situación actual del titular.

Para que los datos personas mantengan las características antes mencionadas es necesario que las Unidades Administrativas de la Entidad, implementen medidas para que todas las bases de datos se corrijan o completen de manera constante e inmediata, una vez que se tanga conocimiento de la actualización o corrección.

Además, se deberán establecer plazos de conservación de los datos personales, que no deberán exceder los plazos contemplados para las finalidades respectivas y que debe de ser congruentes con los plazos de conservación archivística.

Para efecto de lo anterior, se deberán establecer procedimientos que definan la conservación y supresión de los datos personales, que deberán incluir los mecanismos que permitan cumplir con los plazos correspondientes, realizando revisiones periódicas sobre la necesidad de conservar los datos personales de los que se trate.

c) Encargados

Las Unidades Administrativas deberán de formalizar mediante contrato o instrumento jurídico, la relación que mantengan con los encargados, esto les permitirá delimitar el alcance de su relación y la responsabilidad en el manejo de los datos personales, el contrato o instrumento jurídico debe de observar el cumplimiento de las siguientes obligaciones:

1.- El tratamiento de los datos personales se hará de acuerdo a las instrucciones del responsable.

2.- Abstenerse de tratar los datos personales para finalidades distintas a las indicadas por el responsable.

3.- Implementación de medidas de seguridad.

4.- Informar al responsable cuando ocurra una vulneración a los datos personales.

5.- Guardar confidencialidad respecto de los datos personales tratados.

6.- Cuando la relación contractual se haya cumplido, se deberán suprimir o devolver los datos personales.

7.- No realizar transferencia alguna de datos personales.

8.- Permitir al responsable realizar verificaciones en el lugar donde se lleva a cabo el tratamiento.

9.- Colaborar con el responsable en las verificaciones que lleve a cabo.

10.- Generar, actualizar y conservar la documentación que permita acreditar el cumplimiento de sus obligaciones.

En el caso de las subcontrataciones que pudieran realizar los encargados, será en los contratos primigenios donde se podrá establecer si se autorizan o se prohíben y las condiciones para ello.

d) Cómputo en la nube.

Esta obligación versa sobre la necesidad de contratar servicios de cómputo en la nube, garantizando la protección de datos personales de acuerdo a lo establecido en la

LGPDPPSO, los Lineamientos y demás disposiciones aplicables, el tratamiento de los datos personales deberá quedar señalado en las cláusulas contractuales, por lo tanto, éstas se deben verificar previo a la formalización de la contratación.

Los servicios de cómputo en la nube deberán de cumplir con lo siguiente:

1.- Establecer políticas de protección de datos personales, a fines a la LGPDPPSO y demás normas aplicables.

2.- Transparentar las subcontrataciones que involucre la información sobre la que se presta el servicio.

3.- Abstener de incluir clausulado que permita al proveedor asumir la titularidad o propiedad de la información.

4.- Guardar estricta confidencialidad respecto de los datos personales que maneje.

Los servicios contratados deben de dar a conocer sus políticas de privacidad, deberán permitir al responsable limitar el tratamiento de datos personales que traten, también deberá de contar con medidas de seguridad para la protección de los datos personales sobre los cuales presta el servicio, garantizar que cuando el servicio haya terminado, se realizará la supresión de los datos personales correspondientes y por último, restringir el acceso a los datos personales a todas aquellas personas que no cuentan con privilegios.

El tratamiento de los datos personales debe darse de acuerdo a lo siguiente:

1.- El tratamiento de los datos personales se hará de acuerdo a las instrucciones del responsable.

2.- Abstenerse de tratar los datos personales para finalidades distintas a las indicadas por el responsable.

3.- Implementación de medidas de seguridad.

4.- Informar al responsable cuando ocurra una vulneración a los datos personales.

5.- Guardar confidencialidad respecto de los datos personales tratados.

6.- Cuando la relación contractual se haya cumplido, se deberán suprimir o devolver los datos personales.

7.- No realizar transferencia alguna de datos personales.

8.- Permitir al responsable realizar verificaciones en el lugar donde se lleva a cabo el tratamiento.

9.- Colaborar con el responsable en las verificaciones que lleve a cabo.

10.- Generar, actualizar y conservar la documentación que permita acreditar el cumplimiento de sus obligaciones.

e) Transferencias

La obligación corresponde, en caso de que se realice, a formalizar las transferencias nacionales o internacionales mediante la suscripción de cláusulas contractuales, convenios de colaboración o algún otro instrumento jurídico en el que se emita evidencia del tratamiento de los datos personales, indicando las obligaciones y responsabilidades que las partes asumen.

f) Atención solicitudes de ejercicio de Derechos ARCO.

Los derechos ARCO están reconocidos en el artículo 16 de la Constitución de los Estados Unidos Mexicanos. A continuación se conceptualiza cada uno:

1.- Derecho de Acceso: derecho del titular de solicitar el acceso a sus datos personales contenidos en bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, así como de conocer información relacionada con su uso.

2.- Derecho de Rectificación: derecho del titular de solicitar al responsable la rectificación o corrección de sus datos personales cuando éstos seas inexactos o se encuentren incompletos o bien, no estén actualizados.

3.- Derecho de Cancelación: derecho del titular de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos del responsable que los posee, almacena o utiliza, cuando resulte procedente.

4.- Derecho de Oposición: derecho del titular de solicitar que sus datos personales no se utilicen para ciertos fines, o de requerir que se concluya el uso de éstos a fin de evitar el daño a su persona, cuando resulte procedente.

La Unidad de Transparencia de Impresora y Encuadernadora Progreso, S.A. de C.V., al recibir una solicitud de Derechos ARCO a través de la Plataforma Nacional de Transparencia, llevará a cabo el siguiente procedimiento:

En caso de ser competente se verifica:

Información general. Que toda solicitud de ejercicio de derechos ARCO contenga lo siguiente: (Artículo 52 de la LGPDPPSO y 83 de los Lineamientos Generales).

- ✓ Nombre del titular de los datos personales.
- ✓ Documentos que acrediten la identidad del titular.
- ✓ En su caso, nombre de su representante y documentos para acreditar su identidad y personalidad.
- ✓ Domicilio o cualquier medio para recibir notificaciones.
- ✓ Descripción clara y precisa de los datos personales que se quiera rectificar, cancelar u oponerse a su tratamiento.
- ✓ Descripción del derecho que se quiere ejercer o de lo que solicita el titular.
- ✓ En su caso, documentos o información que faciliten la localización de los datos personales, entre ella, el área responsable del tratamiento.

Información específica. Además de la información general antes señalada, dependiendo del derecho que desee ejercer, se deberá incluir la siguiente información en la solicitud:

- ❖ **Derecho de ACCESO:** la modalidad en la que prefiere que se reproduzcan los datos personales solicitados.
- ❖ **Derecho de RECTIFICACIÓN:** las modificaciones que solicita que se realicen a sus datos personales, para lo cual, deberá aportar los documentos que sustenten la solicitud.
- ❖ **Derecho de CANCELACIÓN:** las causas que motivan la petición de que se supriman sus datos personales en los archivos, registros o bases de datos.
- ❖ **Derecho de OPOSICIÓN:** las causas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.

En caso de que la Entidad no sea competente para atender la solicitud para el ejercicio de los derechos ARCO, se le hará saber al particular dentro de los tres días siguientes a la presentación de la solicitud (Artículo 53 de la LGPPDPPSO).

Cuando la solicitud no sea clara, o falte alguno de los requisitos señalados o se requieran mayores elementos, se requerirá la información faltante, a fin de que el particular la proporcione a la Unidad de Transparencia en un plazo no mayor a diez días hábiles; en caso de no atender el requerimiento, su solicitud se tendrá como no presentada. (Artículo 52 de la LGPDPPSO y 87 de los Lineamientos Generales).

Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCO.

La solicitud se deberá acompañar de copia simple de una identificación oficial del titular

de los datos personales, así como de su representante, en caso de que éste sea quien presente la solicitud

La personalidad del representante, en su caso, se podrá acreditar con cualquiera de las siguientes opciones:

1) Carta poder simple suscrita ante dos testigos, anexando copia simple de sus identificaciones oficiales,
2) Poder notarial; o
3) Comparecer el particular y su representante a la oficina de la Unidad de Transparencia.

Es importante tener en cuenta que la identidad del titular y su representante, así como la personalidad de este último, deberán quedar debidamente acreditadas previo al ejercicio del derecho del que se trate, en caso de que resulte procedente, mediante la presentación de los documentos originales antes señalados o copia certificada de los mismos, para su cotejo.

Solicitudes relacionadas con datos personales de menores de edad, personas en estado de interdicción o incapacidad declarada por ley, y personas fallecidas.

Para el ejercicio de derechos ARCO de este grupo de titulares, además de la presentación de la solicitud con la información descrita antes señalada, se deberán aportar los siguientes documentos, según sea el caso:

Menores de edad. Si los padres ejercen la patria potestad y son los que presenten la solicitud:

- Documento que acredite la identidad del menor.
- Acta de nacimiento del menor.
- Identificación oficial del padre o de la madre, que pretenda ejercer el derecho.
- Carta en la que se manifieste, bajo protesta de decir verdad, que el padre o la madre es quien ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

Si una persona distinta a los padres es quien ejerce la patria potestad, y es quien presenta la solicitud:

- Documento que acredite la identidad del menor.
- Acta de nacimiento del menor.
- Documento legal que acredite la posesión de la patria potestad.
- Identificación oficial de quien presenta la solicitud y posee la patria potestad.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

Cuando un tutor es quien ejerce la patria potestad:

- Documento que acredite la identidad del menor.
- Acta de nacimiento del menor.
- Documento legal que acredite la tutela.
- Identificación oficial del tutor.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la tutela.

Para solicitudes de derechos ARCO de datos personales de personas en estado de interdicción o incapacidad legal:

- Documento que acredite la identidad del titular de los datos personales.
- Instrumento legal de designación del tutor.
- Identificación oficial del tutor.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de lo alguno de los supuestos legales de suspensión o limitación de la misma.

Para solicitudes de derechos ARCO de personas fallecidas:

- Acta de defunción del titular.
- Documentos que acrediten el interés jurídico de quien pretende ejercer el derecho.
- Identificación oficial de quien solicita el ejercicio de los derechos ARCO.

Se entenderá por interés jurídico aquel derecho subjetivo derivado de una ley que permite a una persona actuar a nombre de otra que por su situación le es imposible. Ello, a efecto de solicitar el ejercicio efectivo de los derechos ARCO.

Quienes pueden alegarlo son de manera enunciativa mas no limitativa: el albacea, los herederos, los legatarios o cualquier persona que haya sido designada previamente por el titular para ejercer los derechos ARCO en su nombre, lo que se acreditará con copia simple del documento delegatorio, pasado ante la fe de notario público o suscrito ante dos testigos.

En el supuesto de que el titular sea un menor de edad, el interés jurídico se acreditará con la copia del acta de defunción, de las identificaciones del menor y de quien ejercía la patria potestad y/o tutela, así como una carta en la que el requirente manifieste, bajo protesta de decir verdad, que no se encontraba dentro de alguno de los supuestos legales de suspensión o limitación de la misma. En ambos supuestos, se deberá acompañar una carta en la cual se expresen los motivos por los cuales solicita el acceso, rectificación, cancelación u oposición de los datos de la persona fallecida.

Plazos y procedimiento para la atención de las solicitudes de ejercicio de derechos ARCO.

Una vez que se presentó la solicitud y ésta cumplió con los requisitos antes descritos, la Unidad de Transparencia realizará lo siguiente:

- En un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, deberá informarle si procede o no el ejercicio del derecho solicitado. Este plazo podrá ampliarse por 10 días hábiles más cuando existan causas justificadas.
- De ser procedente el ejercicio del derecho, llevará a cabo las acciones necesarias para hacerlo efectivo, en un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la puesta a disposición.

Una vez verificado lo anterior la Unidad de Transparencia de la Entidad turna las solicitudes para el ejercicio de los derechos ARCO a las Unidades Administrativas competentes, (Articulo 88 Lineamientos).

En caso de que la solicitud para el ejercicio de los derechos ARCO en escrito libre se presente directamente ante una unidad administrativa distinta a la Unidad de Transparencia del responsable, la unidad administrativa debe remitir la solicitud a la Unidad de Transparencia a más tardar al día siguiente de su presentación. (Artículo 86 Lineamientos)

En caso de que IEPSA declare inexistencia de los datos personales en sus archivos, registros, sistemas o expediente, dicha declaración se hará saber al particular mediante una resolución del Comité de Transparencia que confirme la inexistencia de los datos personales.

El ejercicio de los derechos ARCO será sencillo y gratuito, sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación de documentos o envío de información.

En caso de proceder la reproducción de los datos personales en copias simples o certificadas será gratuita cuando no excedan de veinte hojas, o bien, las primeras veinte hojas reproducidas o certificadas de conformidad a lo establecido en el Artículo 89 de los Lineamientos.

En caso de proceder algún costo de reproducción certificación y/o envió, o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO, se establecerán en el oficio de respuesta. El plazo que tiene el titular para realizar el pago, el cual no podrá ser **menor de tres días.**

Una vez que el titular o, en su caso, su representante realice el pago deberá remitir copia

del recibo correspondiente, con la identificación del número de folio de la solicitud para el ejercicio de los derechos ARCO que corresponda, a más tardar al día siguiente de realizarse el pago a través del medio que señaló para oír y recibir notificaciones, o bien, presentando personalmente una copia ante la Unidad de Transparencia.

La Unidad de Transparencia tendrá a disposición del titular y, en su caso, de su representante los datos personales en el medio de reproducción solicitado y/o las constancias que acrediten el ejercicio efectivo de los derechos ARCO durante un plazo máximo de sesenta días, contados a partir del día siguiente en que se hubiere notificado la respuesta de procedencia al titular. (Artículo 98 Lineamientos)

Por último, cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCO, se le informará la existencia de este, en un plazo no mayor a 5 días siguientes a la presentación de la solicitud, a efecto de que decida si ejerce sus derechos a través del trámite específico, o bien, por medio del procedimiento anteriormente descrito.

Recurso de Revisión.

En caso de estar inconforme con la respuesta a su solicitud de derechos ARCO, podrá presentar un recurso de revisión ante el INAI en un plazo de 15 días hábiles siguientes a la notificación de la respuesta.

g) Portabilidad

La portabilidad de los datos personales confiere a los titulares la prerrogativa de obtener y reutilizar sus datos personales, para fines propios y en diferentes servicios. En este sentido, el derecho a la portabilidad busca facilitar la capacidad para obtener, copiar o transmitir fácilmente datos personales de un sistema de tratamiento automatizado a otro sistema en un formato electrónico estructurado y comúnmente utilizado.

Por lo tanto, IEPSA deberá de otorgar una copia de los datos personales en un formato electrónico estructurado y de uso común para que el titular tenga la oportunidad de seguir haciendo uso de ellos.

6.4.- Obligaciones en la etapa de Eliminación de los datos personales

a) Supresión de los datos personales.

Esta obligación corresponde a suprimir los datos personales cuando ya han dejado de ser necesarios para el cumplimiento de las finalidades establecidas en el Aviso de Privacidad y una vez que haya vencido el plazo de su conservación. Para poder suprimir los datos

personales hay que garantizar que la probabilidad de que se puedan recuperar o reutilizar sea mínima.

6.5.- Otras obligaciones

a) Responsabilidad

IEPSA deberá de observar lo siguiente:

- Establecer programas y políticas orientadas a la protección de datos personales.
- Elaborar un programa de protección de datos personales.
- Establecer un programa de capacitación de su personal en materia de protección de datos personales.
- Realizar una revisión periódica de su programa de protección de datos personales y determinar las modificaciones de mejora que se requieran.
- Garantizar que el programa de protección de datos personales cumpla con lo estipulado en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

7.- Sanciones

Serán causales de sanción de incumplimiento de las obligaciones previstas en LGPDPPSO cuando las personas servidoras públicas que realizan el tratamiento de datos personales, recaigan en los siguientes supuestos (Artículo 163 de la LGPDPPSO):

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 presente Ley 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 presente Ley

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 presente Ley, 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 presente Ley;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente Ley;

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

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;

XI. Obstruir los actos de verificación de la autoridad;

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley;

XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes, y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

Fuentes consultadas:

- Cámara de Diputados (2017) **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf [Fecha de consulta: 15 de enero de 2024]
- Diario Oficial de la Federación (2018). **Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público**. https://dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018#gsc.tab=0 [Fecha de consulta: 15 de enero de 2024]
- Comisión Ejecutiva de Atención a Víctimas (2023). **Programa de Protección de Datos Personales de la Comisión Ejecutiva de Atención a Víctimas.** http://transparencia.ceav.gob.mx/DatosPersonales/doc/Programa_Proteccion_Datos_Personales_CEAV_2023.pdf [Fecha de consulta: 15 de enero de 2024]
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2015). **Guía para implementar un Sistema de Seguridad de Datos Personales.** Junio 2015. https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf [Fecha de consulta: 15 de enero de 2024]
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. **Políticas Internas para la Gestión y Tratamiento de Datos Personales**. https://inicio.inai.org.mx/doc/DGAJ/ApartadoPDP/Deberes/Seguridad/Pol%C3%ADticas%20internas%20para%20la%20gesti%C3%B3n%20y%20tratamiento%20de%20datos%20personales%20INAI%20DS-2021.pdf [Fecha de consulta: 15 de enero de 2024]
- Secretaría de Hacienda y Crédito Público (2023). Unidad de Transparencia. **Programa de Protección de Datos Personales 2023-2024.** https://www.transparencia.hacienda.gob.mx/work/models/transparencia/docs/Proteccion_Datos_Personales/PROGRAMA_PDP_SHCP_2021_2022.pdf [Fecha de consulta: 15 de enero de 2024]