Programa de Protección de Datos Personales

Presentación

De conformidad con el artículo 34 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) un sistema de gestión es un conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, así como, el cumplimiento de los principios, deberes y obligaciones previstos en dicha ley y las demás disposiciones que resulten aplicables en la materia. Para la elaboración del presente documento, se identificaron las obligaciones que establece la LGPDPPSO y, a partir de ello, se definieron las acciones a seguir para su cumplimiento.

Objetivo del Programa

El presente programa tiene como objetivos los siguientes:

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión de las Direcciones de Área del Centro de Investigaciones en Óptica, A.C.;
2. Cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
3. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua.

Responsabilidades dentro del Programa

Con fundamento en lo dispuesto por los artículos 83 y 84, fracción I de la LGPDPPSO, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este programa:

- Elaborar, aprobar, coordinar y supervisar el Programa;
- Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
- Dar a conocer el Programa al interior del sujeto obligado;
- Coordinar la implementación del Programa en las Direcciones de Área del sujeto obligado;
- Asesorar a las Direcciones de Área en la implementación de este Programa;
- Supervisar la correcta implementación del Programa;
- Presentar un informe anual al titular de la institución, en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Programa;
- Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con el área de Recursos Humanos, y
- Las demás que de manera expresa señale el propio Programa.

El Programa será de observancia obligatoria para todas las personas servidoras públicas del CIO que en el ejercicio de sus funciones traten datos personales.

Las unidades administrativas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán prever lo que se requiera en sus respectivos programas anuales de trabajo.

Alcance del Programa

El presente programa aplicará a todos los tratamientos de datos personales que se realicen en las unidades administrativas del CIO en ejercicio de sus atribuciones.

Política de gestión de los 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 lo cual este programa establecerá el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo.

Es responsabilidad del servidor público que recabe, maneje, administre y/o transfiera datos personales identificar 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.

Inventario de tratamiento de Datos Personales

Para el debido cumplimiento de las obligaciones que se establecen en este programa, es necesario que cada una de las unidades administrativas realicen un diagnóstico de los tratamientos de datos personales que llevan a cabo.

El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en el CIO. Dicho inventario identificará los siguientes elementos:

1. ¿Qué tratamientos de datos personales realiza la unidad administrativa?

   Hay que identificar cada uno de los procesos en los que la unidad administrativa trata datos personales.

2. ¿Qué unidad administrativa está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos?

   Hay que identificar o definir si la unidad administrativa está a cargo del proceso en donde se tratan los datos personales, según las atribuciones o facultades normativas.

   Podría ocurrir que una unidad administrativa trate datos personales recabados en el marco de un proceso del cual no es responsable. Asimismo, podría darse el caso en que dos o más unidades administrativas estén a cargo de un proceso mediante el cual se recaban los datos personales y que administren las bases de datos correspondientes de manera conjunta.

   En ese sentido, para definir quién está a cargo del proceso mediante el cual se recaban los datos personales y que, por tanto, administre las bases de datos o archivos correspondientes, es necesario analizar la función que realiza cada unidad administrativa dentro del proceso, y las atribuciones o facultades normativas que resulten aplicables.

3. Una vez que hayan sido identificados los tratamientos de los cuales está a cargo la unidad administrativa, será necesario determinar lo siguiente:

¿Cómo se obtienen los datos personales?
¿Qué tipo de datos personales se tratan? ¿son sensibles?
¿Dónde se almacenan y realiza el tratamiento de los datos personales?
¿Para qué finalidades se utilizan los datos personales?
¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quién se comunican los datos personales al interior del sujeto obligado?
¿Intervienen encargados en el tratamiento de los datos personales?
¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?
¿Se difunden los datos personales?
¿Cuál es el plazo de conservación de los datos personales?

En caso de que alguna Dirección de Área no cuente con unidades administrativas que hagan tratamiento de datos personales, deberá comunicarlo mediante oficio dirigido al Comité de Transparencia.

Cumplimiento de obligaciones

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

La Dirección de Área, que cuente con unidades administrativas que realicen tratamiento de datos personales, deberá elaborar un documento de seguridad, que deberá contener, al menos, la siguiente información: el inventario de datos personales y de los sistemas de tratamiento, las funciones y obligaciones de las personas que traten datos personales, el análisis de riesgos, el análisis de brecha, el plan de trabajo, los mecanismos de monitoreo y revisión de las medidas de seguridad (administrativas, físicas y técnicas), los mecanismos que se deben adoptar en caso de vulneraciones de seguridad y el programa general de capacitación.

Redactar los avisos de privacidad que se requieran conforme a los tratamientos que lleven a cabo las unidades administrativas. Como regla general, se requerirá un aviso de privacidad por tratamiento. Sólo en los casos en que la información a incluir en el aviso de privacidad de distintos tratamientos sea la misma en su mayoría, se podrá redactar un aviso de privacidad común. El criterio para este supuesto es que la redacción del aviso de privacidad compartido no sea confusa.

Sanciones por incumplimiento

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.

Glosario de términos

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por la Dirección de Área y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.

CIO: Centro de Investigaciones en Óptica, A.C.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

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.

Direcciones de Área: Se refiere a aquellas que dependen de forma inmediata de la Dirección General del CIO, es decir, la Dirección de Administración, la Dirección de Investigación, la Dirección de Formación Académica y la Dirección de Tecnología e Innovación.

Documento de Seguridad: Instrumento que describe y da cuenta, de manera general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o juntamente con otras trate datos personales a nombre y por cuenta del responsable.

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus obligaciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Programa: Programa de Protección de Datos Personales.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

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.

Unidad Administrativa: Área a la que se le confieren atribuciones específicas y que se encuentran adscritas a las Direcciones de Área o a la Dirección General del CIO.

Con fundamento en el artículo 84, fracción I y IV de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados el Comité de Transparencia del Centro de Investigaciones en Óptica, A.C. emite el presente programa en agosto del 2024.

Luis Kevin Hernández Foy
Titular de la Unidad de Transparencia

Oscar Leonel Rodríguez Quiñones
Director de Administración

Anya Lizzette Bermúdez Torres
UA del OICE en CONAHCYT en el CIO