Principales obligaciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

I. Presentación

El presente documento tiene por objeto señalar las principales obligaciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante, Ley General) que son exigibles a cualquier autoridad, entidad órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos y fideicomisos y fondos públicos del orden federal y partidos políticos con la entrada en vigor del ordenamiento aludido, o bien, aquéllas que están sujetas a condiciones normativas para su efectivo cumplimiento.

II. Objeto de la Ley General

La Ley General tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de todo ente público de los tres órdenes de gobierno, así como de partidos políticos.

En este sentido, el derecho a la protección de datos personales es entendido como el poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso.

III. Sujetos obligados a cumplir con la Ley General

Las disposiciones de la Ley General son exigibles a cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos y partidos políticos del orden federal, estatal y municipal que en el ejercicio de sus atribuciones y funciones utilicen datos personales.

Es importante destacar, que la Ley General ya resulta aplicable a todos los entes públicos federales y partidos políticos. Por su parte, los Congresos estatales cuentan con un plazo máximo de seis meses, contados a partir de la entrada en vigor de la Ley aludida, para realizar las adecuaciones normativas correspondientes a su legislación existente en la materia, con el fin de que ésta responda a los nuevos estándares que señala la Ley aludida.

Mientras este periodo de armonización sucede, el ejercicio y tutela de los datos personales en posesión de instancias públicas del orden estatal y municipal se regirá por la normatividad actual en cada entidad federativa como hasta el día de hoy.

IV. Conceptos rectores para entender la Ley General

1. Datos personales

Un dato tiene la connotación de personal en la medida en que pueda vincularse a una persona física identificada o identificable, el cual puede estar expresado en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o de cualquier otro tipo. Se entiende que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente, mediante cualquier información que no implique plazos o actividades desproporcionadas.

Algunos ejemplos de datos personales son, nombre, domicilio, número telefónico, número de seguridad social, cargo o puesto, edad, Registro Federal de Contribuyentes, entre otros.

2. Datos personales sensibles

Un dato personal adquiere la categoría de sensible en cualquiera de los siguientes supuestos: cuando afecte la esfera más íntima de la persona, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para ésta, o bien, cuando se revelen aspectos de la persona como es su origen étnico o racial, estado de salud, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

3. Responsable

Cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, fideicomisos y fondos públicos del orden federal y partidos políticos que decide o determina las finalidades del tratamiento o el uso que se le dará a los datos personales; el tipo de datos que se requieren; los medios a utilizar en el tratamiento de datos personales; las transferencias de información personal que, en su caso, se efectúen; la forma o mecanismos para obtener, almacenar y suprimir los datos personales; casos en que se divulgarán, entre otros factores que implican tener y ejercer un poder de decisión en cuanto al alcance, contenido y medios del tratamiento o el uso de la información personal.

Al respecto, con la Ley General se rompe la errónea concepción que se tiene hasta el momento que el responsable de determinado tratamiento de datos personales es el servidor público que operativamente utiliza los datos personales para el ejercicio de sus funciones; cuando en realidad adquiere el carácter de responsable la instancia pública *per se* entiéndase la Secretaría de la Función Pública, la Secretaría de Gobernación, el Instituto Mexicano del Seguro Social, el Instituto Nacional de Desarrollo Social, la Comisión Nacional de Derechos Humanos, el Instituto Nacional Electoral o el propio Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI o Instituto), por mencionar algunos ejemplos.

4. Titular

La persona física a la que le concierne los datos personales, esto es, cualquier persona a quien se le brinda un servicio público y que a través del mismo es necesario la utilización de datos personales, como podrían ser los beneficiarios de un programa social, o los ciudadanos mayores de 18 años que solicitan su credencial para votar, o los derechohabientes del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado.

5. Tratamiento

El conjunto de operaciones realizadas con los datos personales para la consecución de ciertos fines que persigue el responsable, concretamente, consiste en las distintas operaciones llevadas a cabo durante el ciclo de vida de los datos personales, es decir, desde el momento de su obtención, pasando por su explotación o aprovechamiento, hasta su supresión o eliminación.

A manera de estricta referencia y de manera enunciativa más no limitativa, un tratamiento de datos personales se distingue por 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, disposición de datos personales, entre otras.

V. Obligaciones de cumplimiento inmediato

A continuación se presentan aquellas obligaciones que son exigibles con la entrada en vigor de la Ley General:

Fundamento legal	Obligaciones
• **1. Relacionadas antes, durante y después de utilizar datos personales**	
Artículo 17 (principio de licitud)	• Identificar que cuente con facultades o atribuciones expresas en la normatividad que le resulte aplicable para utilizar datos personales. Por ejemplo, los artículos de los ordenamientos que habilitarían a la instancia pública a utilizar datos personales.
Artículo 18 (principio de finalidad)	• Determinar los usos concretos que se van a dar a los datos personales, los cuales deben ser acordes con las atribuciones que la normatividad aplicable le confiera a la instancia pública. A manera de ejemplo, en un programa social los datos personales de los beneficiarios podrían utilizarse para conocer su condición socioeconómica; brindar el apoyo económico en especie o de otra categoría; realizar estadísticas; desarrollar políticas públicas orientadas a ciertos objetivos, entre otros. • Contar con atribuciones conferidas en ley y solicitar el consentimiento del titular para utilizar los datos personales para finalidades diferentes a aquéllas que motivaron su obtención.
Artículo 19 (principio de lealtad)	• No actuar de manera engañosa o fraudulenta, es decir, sin que medie dolo, error o mala fe por parte de la instancia pública respecto al tratamiento de datos personales que efectúe.
Artículos 20, 21 y 22 (principio del consentimiento)	• Recabar el consentimiento del titular para el tratamiento de sus datos personales, ya sea en su modalidad tácita o expresa según corresponda, salvo que se actualice alguna de las siguientes causales de excepción: ▪ 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. ▪ 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. ▪ Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente. ▪ Para el reconocimiento o defensa de derechos del titular ante autoridad competente. ▪ Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.

Fundamento legal	Obligaciones
	▪ Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes. ▪ Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria. ▪ Cuando los datos personales figuren en fuentes de acceso público entendidas como las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general; los directorios telefónicos en términos de la normativa específica; los diarios, gacetas o boletines oficiales, de acuerdo con su normativa; los medios de comunicación social y los registros públicos conforme a las disposiciones que les resulten aplicables. ▪ Cuando los datos personales se sometan a un procedimiento previo de disociación, o ▪ Cuando el titular de los datos personales sea una persona reportada como desaparecida en ▪ los términos de la ley en la materia. • Por regla general, el consentimiento que resulta aplicable a todo tratamiento de datos personales es el tácito que se traduce en la simple puesta a disposición del aviso de privacidad al titular, salvo que una disposición exija que la voluntad del titular se manifieste de manera expresa, es decir, por escrito, verbal, medios electrónicos, ópticos o cualquier otra tecnología.
Artículos 23 y 24 (principio de calidad)	• Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales. El tiempo de actualización de los datos personales dependerá de las necesidades de cada instancia pública del orden federal. • Suprimir de los archivos, registros, sistemas de información o expedientes los datos personales una vez que dejen de ser necesarios para el cumplimiento de las finalidades que motivaron su utilización. • Establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales. En la definición de los plazos de conservación de los datos personales se deben considerar los valores administrativos, contables, fiscales, jurídicos e históricos que pudieran llegar a tener éstos. • Cabe destacar, que esta última obligación está íntimamente vinculada con los instrumentos de consulta y control archivístico que cada instancia pública del orden federal está obligada a generar.

Fundamento legal	Obligaciones
Artículo 25 (principio de proporcionalidad)	• Recabar y utilizar los datos personales que resulten estrictamente necesarios para las finalidades que justifican su tratamiento. Por ejemplo, sería desproporcional que en un proceso de reclutamiento y selección de personal de cierta instancia pública del orden federal se recabara la creencia religiosa de un candidato a obtener un puesto de asistente telefónico.
Artículos 26, 27 y 28 (principio de información)	• Dar a conocer al titular el aviso de privacidad en la modalidad simplificada y en un momento posterior en su modalidad integral. • El aviso de privacidad puede ser difundido en medidos electrónico o físicos con los que cuente la instancia pública. • El aviso de privacidad simplificado debe señalar la siguiente información: ▪ La denominación del responsable. ▪ Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular. ▪ Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar: a) las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales y b) las finalidades de estas transferencias. ▪ Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular, y ▪ El sitio donde se podrá consultar el aviso de privacidad integral. • El aviso de privacidad integral, además de señalar la información prevista en el aviso de privacidad simplificado, debe informar lo siguiente: ▪ El domicilio del responsable. ▪ Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles. ▪ El fundamento legal que faculta al responsable para llevar a cabo el tratamiento. ▪ Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular. ▪ Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO.

Fundamento legal	Obligaciones
	▪ El domicilio de la Unidad de Transparencia, y ▪ Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad. • Es importante señalar, que lo que antes se denominaba leyenda de información ahora se transforma en aviso de privacidad, el cual contiene mayores elementos de información orientados a que el titular conozca las características principales del tratamiento al que serán sometidos sus datos personales, a fin de que tome decisiones informadas al respecto.
Artículos 29 y 30 (principio de responsabilidad)	• Implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley General como son, de manera enunciativa más no limitativa: ▪ Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable. ▪ Establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de las políticas de protección de datos personales. ▪ Diseñar, desarrollar e implementar políticas públicas, programas, servicios o sistemas de conformidad con las disposiciones previstas en la Ley General. ▪ Garantizar que las políticas públicas, programas, servicios o sistemas cumplan por defecto con las obligaciones previstas en la Ley General, entre otros.
2. Relacionadas con medidas de seguridad para la protección de los datos personales	
Artículos 31, 32, 33, 34, 35 y 36	• Establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico que permitan garantizar la confidencialidad, integridad y disponibilidad de los datos personales, tales como: ▪ 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. ▪ Físicas: prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información; proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización y proveer a los equipos que contienen

Fundamento legal	Obligaciones
	o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad. ▪ Técnicas: prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales. ▪ Determinar y establecer las medidas de seguridad que resulten aplicables a los datos personales en función de una serie de factores como son el riesgo inherente de los datos personales; la sensibilidad de éstos; el desarrollo tecnológico; las transferencias de datos personales que, en su caso, se efectúen; las vulneraciones de seguridad ocurridas, entre otros factores. • Diseñar e implementar un sistema de gestión de la seguridad de los datos personales, 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 • Elaborar un documento de seguridad que contenga lo previsto en el artículo 35 de la Ley General y actualizarlo en los supuestos señalados en el artículo 36 del mismo ordenamiento, el cual desde la legislación pasada ya existía por lo que tendría que actualizarse conforme a los nuevos estándares que prevé la Ley General.
3. Relacionadas con las vulneraciones de seguridad de datos personales	
Artículos 37, 38 39, 40 y 41	• Si ocurre una pérdida, destrucción no autorizada, robo, extravío o copia no autorizada uso, acceso o tratamiento no autorizado, o daño, la alteración o modificación no autorizada de datos personales que afecten de manera significativa los derechos patrimoniales o morales de los titulares, la instancia pública deberá dar aviso a éstos y al Instituto, sin dilación alguna en cuanto confirme la existencia de la vulneración. • En este aviso se deberá informar: ▪ La naturaleza del incidente. ▪ Los datos personales comprometidos.

Fundamento legal	Obligaciones
	▪ Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. ▪ Las acciones correctivas realizadas de forma inmediata. ▪ Los medios donde puede obtener más información al respecto. • Asimismo, la instancia pública del orden federal deberá llevar una bitácora sobre las vulneraciones de seguridad ocurridas, registrando, al menos, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.
Artículo 42	Establecer controles o mecanismos para asegurar que toda persona que intervenga en cualquier fase del tratamiento de los datos personales guarde confidencialidad respecto de éstos. Por ejemplo la suscripción de cláusulas de confidencialidad con los servidores púbicos.
4. Relacionadas con los derechos de acceso, rectificación, cancelación y oposición	
Artículo 44 (derecho de acceso)	• Proporcionar al titular o, en su caso, su representante acceso a sus datos personales, así como a la información relacionada con los términos y características generales o particulares de su tratamiento.
Artículo 45 (derecho de rectificación)	• Llevar a cabo la rectificación o corrección de los datos personales del titular cuando resulten ser inexactos, incompletos o no se encuentren actualizados.
Artículo 46 (derecho de cancelación)	• Suprimir o eliminar los datos personales del titular a fin de que los mismos dejen de ser tratados.
Artículo 47 (derecho de oposición)	• Cesar en el tratamiento de los datos personales cuando el titular tenga una causa legítima y su situación específica así lo requiera para evitar que su persistencia le cause un daño o perjuicio; o bien, cuando los datos personales sean objeto de un tratamiento automatizado que produzca al titular efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades.

Fundamento legal	Obligaciones
Artículo 48, 49, 50, 51, 52, 53, 54, 55, 56 y 86.	• Establecer procedimientos sencillos que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (en adelante, derechos ARCO), bajo las siguientes condiciones: ▪ Los derechos ARCO se pueden ejercer en cualquier momento, donde el ejercicio de cualquiera de ellos no es requisito previo, ni impide el ejercicio de otro. ▪ Las únicas personas acreditadas para ejercer derechos ARCO son el titular o su representante, menores de edad o personas que se encuentren estado de interdicción o incapacidad declarada en ley con su debida representación conforme a las reglas civiles que resulten aplicables y personas vinculadas a fallecidos. ▪ La prohibición de imponer al titular mayores requisitos en las solicitudes para el ejercicio de los derechos ARCO que las señaladas en el artículo 52 de la Ley General. ▪ La prohibición de aumentar los plazos previstos en el artículo 51 de la Ley General para la atención y respuesta de solicitudes para el ejercicio de los derechos ARCO, los cuales se traducen en 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para que el responsable determine la procedencia o improcedencia del derecho de que se trate, el cual podrá ampliarse por una sola vez hasta por 10 días hábiles. En caso de que proceda el ejercicio de los derechos ARCO, el responsable debe hacerlo efectivo en un plazo que no podrá exceder de 15 días hábiles, contados a partir del día siguiente en que se haya notificado la respuesta al titular. ▪ La prohibición de cobrar costos al titular por el ejercicio de sus derechos ARCO, más allá de aquellos relacionados con la reproducción, certificación y envío de datos personales. ▪ Se podrá determinar la improcedencia del ejercicio de los derechos ARCO cuando se actualice alguna de las siguientes razones: - Cuando el titular o su representante no estén debidamente acreditados para ello. - Cuando los datos personales no se encuentren en posesión del responsable. - Cuando exista un impedimento legal. - Cuando se lesionen los derechos de un tercero; - Cuando se obstaculicen actuaciones judiciales o administrativas. - Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos. - Cuando la cancelación u oposición haya sido previamente realizada.

Fundamento legal	Obligaciones
	- Cuando el responsable no sea competente. - Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular. - Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular. - Cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano. - Cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades. • Procurar que las personas con alguna discapacidad o perteneciente a algún grupo vulnerable puedan ejercer en igualdad de circunstancias su derecho a la protección de datos personales.
5. Relacionadas con la contratación de prestadores de servicios que efectúen tratamientos de datos personales a nombre y por cuenta del responsable	
Artículos 58, 59, 60, 61,62, 63 y 64	• La Ley General denomina a este tipo de prestadores de servicios como “encargado”, el cual puede ser una persona física o jurídica, pública o privada, ajena a la organización de la instancia pública del orden federal, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta de ésta. • En este sentido, la instancia pública del orden federal deberá observar lo siguiente en la contratación de estos servicios, desde el punto de vista del derecho a la protección de datos personales: ▪ Formalizar toda prestación de servicios que involucre un tratamiento de datos personales, a través de la suscripción de un contrato o cualquier otro instrumento jurídico, considerando, al menos, las cláusulas que expresamente prevé el artículo 59 de la Ley General. ▪ Autorizar expresamente la subcontratación de servicios que involucren el tratamiento de datos personales, ya sea en el propio contrato o instrumento jurídico que suscribe con el prestador de servicios, o bien, previo a la contratación. ▪ Contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube que cumplan con los principios y deberes establecidos en la Ley General.

Fundamento legal	Obligaciones
	• Cabe resaltar, que las comunicaciones de datos personales que se realicen entre la instancia pública del orden federal y el prestador de servicios no deben ser informadas al titular ni solicitar su consentimiento.
6. Relacionadas con transferencias de datos personales	
Artículos 65, 66, 67, 68, 69, 70 y 71	• La ley General señala que una transferencia es toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado. • En este sentido, cuando cualquier instancia pública del orden federal decida realizar una transferencia de datos personales, nacional o internacional, está obligada a cumplir con lo siguiente: ▪ Obtener el consentimiento del titular para la transferencia de datos personales, sea nacional o internacional, salvo las excepciones previstas en el artículo 70 de la Ley General. ▪ Comunicar al receptor o destinario de los datos personales el aviso de privacidad del responsable transferente. ▪ Formalizar las transferencias de datos personales que se efectúen con el destinatario, mediante la suscripción de cláusulas contractuales, convenios o cualquier otro instrumento jurídico, salvo las excepciones previstas en el artículo 66 de la Ley General.
7. Relacionadas con el tratamiento de datos personales por instancias de seguridad, procuración y administración de justicia del orden federal	
Artículos 80, 81 y 82	• Utilizar los datos personales conforme a las disposiciones previstas en la Ley General. • Implementar medidas de seguridad de nivel alto.
8. Relacionadas con el Comité y Unidad de Transparencia	
Artículos 83 y 84	• Conocer que el Comité de Transparencia es la máxima autoridad en materia de protección de datos personales con las siguientes funciones: ▪ Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la Ley General. ▪ Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO.

Fundamento legal	Obligaciones
	▪ Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la Ley General, entre otras.
Artículo 85	• Instruir a la Unidad de Transparencia a llevar a cabo las siguientes funciones: ▪ 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. ▪ Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, entre otras.
Artículo 85	• Designar a un oficial de protección de datos personales cuando el responsable, en el ejercicio de sus funciones, lleve a cabo tratamientos relevantes o intensivos de datos personales los cuales adquieren esta connotación a partir de los riesgos inherentes a los datos personales a tratar; los datos personales sensibles, y se efectúen o pretendan efectuar transferencias de datos personales (facultad potestativa).
9. Relacionadas con la capacitación de los servidores públicos	
Artículo 92	• Colaborar con el INAI para capacitar y actualizar de forma permanente a sus servidores públicos.
10. Relacionadas con la sustanciación del recurso de revisión	
Artículos 100, 102, 107, 108 y 144	• Atender los requerimientos de información del Instituto en la sustanciación del recurso de revisión. • Presentar cualquier tipo de pruebas a que se refiere el artículo 102 de la Ley General. • Manifestar su voluntad para conciliar dentro del procedimiento. • Cumplir con las resoluciones emitidas por el Instituto en los tiempos y formas previstas en éstas. • Conocer que el plazo que tiene el Instituto para emitir la resolución correspondiente es de 40 días hábiles, el cual podrá ampliarse por 20 días más.
11. Relacionadas con el procedimiento de verificación	
Artículos 146, 147, 149 y 151	• Proporcionar al INAI la documentación que solicite con motivo de un procedimiento de verificación.

Fundamento legal	Obligaciones
	• Verificar que todo procedimiento de verificación inicie con una orden que funde y motive la actuación del Instituto. • Atender las medidas cautelares impuestas por el Instituto, durante la sustanciación del procedimiento de verificación, así como llevar a cabo las gestiones que determine el INAI para que las mismas puedan quedar sin efecto. • Conocer que el procedimiento de verificación tiene una duración máxima de 50 días hábiles, los cuales no podrán ampliarse. • Solicitar al INAI la realización de auditorías voluntarias que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la Ley General respecto de determinado tratamiento de datos personales.

III. Obligaciones sujetas a la emisión de normatividad

En seguida se muestran aquellas obligaciones que serán exigibles al responsable, una vez que entre en vigor el marco normativo correspondiente.

Fundamento legal	Obligaciones
12. Relacionadas con la implementación de medidas compensatorias	
Artículo 26	• Cuando se considere conveniente, implementar medidas compensatorias cuando resulte imposible dar a conocer el aviso de privacidad de manera directa al titular o le exija esfuerzos desproporcionados, una vez que entre en vigor la normatividad que deberá emitir el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante, Sistema Nacional de Transparencia) en la materia. • Las medidas compensatorias se traducen en mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance.
13. Relacionadas con el derecho a la portabilidad de los datos personales	

Fundamento legal	Obligaciones
Artículo 57	• Atender las solicitudes para ejercer el derecho a la portabilidad de los datos personales, una vez que entre en vigor los lineamientos que deberá emitir el Sistema Nacional de Transparencia. • El derecho a la portabilidad permite al titular solicitar sus datos personales en un formato electrónico estructurado y comúnmente utilizado con la finalidad de seguirlos utilizándolos.
14. Relacionadas con las evaluaciones de impacto a la protección de datos personales	
Artículos 74, 77 y 78	• Realizar una evaluación de impacto a la protección de datos personales previa a la puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen el tratamiento intensivo o relevante de datos personales, salvo que dicha evaluación pueda comprometer los efectos que se pretenden con la puesta en operación o modificación del tratamiento de datos personales, o bien, se trate de situaciones de emergencia o urgencia. • Una evaluación de impacto a la protección de datos personales es un documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable. • Presentar al INAI dicha evaluación 30 días hábiles antes de la fecha en que se pretenda poner en marcha la operación o modificación. • Conocer que el Instituto tiene 30 días hábiles para emitir recomendaciones no vinculantes por cada evaluación de impacto a la protección de datos que le sea presentada. Lo anterior, una vez que entre en vigor las disposiciones que regularán el contenido de las evaluaciones de impacto a la protección de datos personales y la valoración de las mismas a que se refieren los artículos 14, fracciones XIX y XX y 74 de la Ley General.
15. Relacionadas con esquemas de mejores prácticas	

Fundamento legal	Obligaciones
Artículos 72 y 73	• Cuando lo considere conveniente el responsable, adoptar esquema de mejores prácticas, los cuales tengan por objeto elevar el nivel de protección de los datos personales previstos en la Ley General (facultad potestativa), una vez que entren en vigor los parámetros y reglas de operación que deberá emitir el Instituto. • Los esquemas de mejores prácticas tienen por objeto: ▪ Elevar el nivel de protección de los datos personales. ▪ Armonizar el tratamiento de datos personales en un sector específico. ▪ Facilitar el ejercicio de los derechos ARCO por parte de los titulares. ▪ Facilitar las transferencias de datos personales. ▪ Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales. ▪ Demostrar ante el Instituto el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales. • Los esquemas de mejores prácticas podrán ser reconocidos o validados por el Instituto, conforme a la normativa que se emita el respecto.