GUÍA PARA LA PROTECCIÓN DE DATOS PERSONALES:

¿Cómo adecuarse a la ley y evitar sanciones?

2016

BDO

CONTENIDO

INTRODUCCIÓN

La presente guía tiene el objetivo de contribuir a lograr un mejor entendimiento sobre ley de protección de datos personales por parte de las organizaciones, lo que permitirá a las mismas estar mejor preparadas y mitigar posibles riesgos de sanción por incumplimiento.

I. introducción

El 22 de marzo del 2013 se aprobó mediante DECRETO SUPREMO N° 003-2013, el reglamento de la Ley de Protección de Datos Personales (Ley N° 29733) con la finalidad de garantizar el derecho fundamental de toda persona a la protección de sus datos personales, derecho constitucionalmente reconocido. La mencionada Ley abarca a toda organización pública o privada que realiza tratamiento (recopilación, registro, almacenamiento, entre otros) de datos personales en sus operaciones.

El plazo de adecuación a la Ley dispuesto por el reglamento de la ley finalizó el 8 de mayo de 2015. Es por ello que la Dirección de Protección de Datos Personales perteneciente al Ministerio de Justicia (también conocida como Autoridad de Protección de Datos Personales o la Autoridad), ha iniciado visitas de fiscalización algunas de las cuales han concluido en procedimientos administrativos sancionadores a empresas de distintos sectores por el incumplimiento de las disposiciones presentadas en la ley y su reglamento. Las penalidades pueden alcanzar hasta 100 UIT (1 UIT = S/. 3,950.00 – a la fecha de la publicación de la presente guía) y ser acumulativas hasta el 10% de los ingresos brutos de la organización.

EL 8 DE MAYO DE 2015

finalizó el plazo de adecuación a la Ley de Protección de Datos Personales.

En tal sentido, la presente guía tiene la finalidad de presentarle conceptos básicos de la Ley, evaluar que tan expuesta está la organización a la que pertenece y asistirlo paso a paso en el proceso de adecuación a fin de evitar posibles sanciones por la Autoridad.

I. Conceptos básicos

Alcance de la presente ley

La Ley de Protección de Datos Personales (LPDP) es de aplicación a todas las organizaciones públicas y privadas tratamiento de datos personales de personas naturales en sus operaciones. Se entiende por tratamiento a cualquier operación o procedimiento técnico, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

Datos personales

Se entiende por datos personales a toda información sobre una persona natural que la identifica o la hace identificable a través de medios que puedan ser razonablemente utilizados. Dentro de esta definición se encuentran los llamados "datos sensibles", que son datos personales referidos al origen racial y étnico, ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical, e información relacionada a la salud o a la vida sexual; estos datos son objeto de especial protección.

Datos sensibles

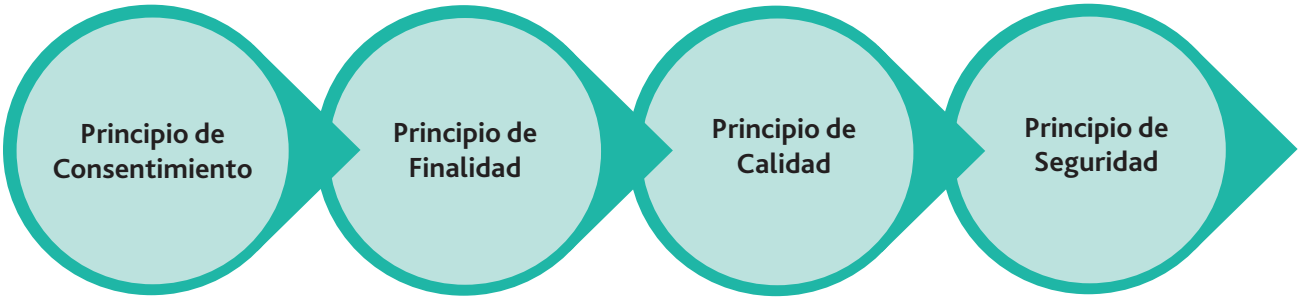
Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.

Banco de datos personales

El Banco de datos personales es un conjunto organizado de datos personales contenido ya sea en un soporte físico, magnético, digital, óptico u otros, y administrado por una persona natural o una persona jurídica de derecho privado, o una entidad pública. Cuando se constituya un banco de datos personales, se debe publicar su existencia, finalidad, identidad y domicilio de su titular y, de ser el caso, de su encargado. Asimismo, debe inscribirse en el Registro Nacional de Protección de Datos Personales

Principios rectores

La ley de protección de datos personales obliga a las organizaciones a cumplir con los siguientes principios rectores:



El tratamiento de los datos personales es lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco.

Una finalidad está determinada cuando haya sido expresada con claridad, sin lugar a confusión y cuando de manera objetiva se especifica el objeto que tendrá el tratamiento de los datos personales.

Los datos contenidos en un banco de datos personales, deben ajustarse con precisión a la realidad. Se presume que los datos directamente facilitados por el titular de los mismos son exactos.

El tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley o al presente reglamento.

II. Enfoque para el cumplimiento de la norma

Una organización (sea pública o privada) requiere realizar dos (2) acciones:

1	**Inscribir los Bancos de Datos Personales ante la Autoridad**
2	**Establecer Medidas de Seguridad para la Protección de Datos Personales**

1. Inscribir los Bancos de Datos Personales ante la Autoridad

El proceso de inscripción significa que la organización inscriba sus bancos de datos personales en el Registro Nacional de Protección de Bancos de Datos (RNPDP) a cargo de la Autoridad de Protección de Datos Personales (para mayor información, dirigirse a siguiente enlace: http://www.minjus.gob.pe/wp-content/uploads/2014/09/Cartilla-Registro-NEW-BAJA.pdf.) La no inscripción del banco de datos personales constituye una INFRACCIÓN GRAVE conforme lo dispone el artículo 38 de la LPDP.

2. Establecer medidas de seguridad

Es requerido por ley, establecer medidas de seguridad organizativas, jurídicas y técnicas. A continuación una descripción de cada una de ellas:

- Organizativas: Orientadas a definir una estructura organizacional, roles y responsabilidades y procesos que permitan el cumplimiento sostenible de la Ley de Protección de Datos Personales en la organización.
- Jurídicas: Orientadas a definir medidas que protejan legalmente a la organización en relación al tratamiento de datos personales.
- Técnicas: Orientadas a establecer controles técnicos de seguridad de la información para resguardar los datos personales que están siendo tratados por la organización.

La Directiva de Seguridad de la Información, publicada el 11 de octubre de 2013 para apoyar la implementación de la LPDP, define una serie de recomendaciones para la implementación de las medidas que permitan proteger el tratamiento de datos personales de cualquier organización. Para mayor detalle dirigirse al siguiente enlace: http://www.minjus.gob.pe/legislacion/

III. Infracciones y sanciones administrativas

El procedimiento sancionador se inicia de oficio, por la Autoridad Nacional de Protección de Datos Personales o por denuncia de parte, ante la presunta comisión de actos contrarios a lo dispuesto en la presente ley.

En principio, las infracciones se califican como leves, graves y muy graves.

Infracción leve	Tratar los Datos Personales sin consentimiento expreso del titular de la información.	5 UIT
Infracción grave	Rechazar reiteradas veces las solicitudes de actualización de información por parte del titular.	50 UIT
Infracción muy grave	Crear, modificar, cancelar o mantener un Banco de Datos Personales sin cumplir con la Ley (procedimientos establecidos).	100 UIT
Infracción muy grave	No inscribir el Banco de Datos Personales de su Organización ante el Registro Nacional de Protección de Datos Personales pese a lo requerido.	100 UIT

Para mayor detalle presentamos algunos ejemplos de infracciones a la Ley:

Se consideran infracciones leves:
- Dar tratamiento a datos personales sin recabar el consentimiento de sus titulares, cuando el mismo sea necesario.
- No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales, cuando legalmente proceda.
- Obstruir el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales.

Se consideran infracciones graves:
- Dar tratamiento a los datos personales contraviniendo las reglas básicas establecidas en la presente ley.
- Incumplir la obligación de confidencialidad.
- No atender, impedir u obstaculizar, en forma sistemática, el ejercicio de los derechos del titular de datos personales, cuando legalmente proceda.
- Obstruir, en forma sistemática, el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales.
- No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales.

Se consideran infracciones muy graves:
- Dar tratamiento a los datos personales contraviniendo las reglas básicas establecidas en la presente ley, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
- Crear, modificar, cancelar o mantener bancos de datos personales sin cumplir con lo establecido en la presente ley.
- Suministrar documentos o información falsa o incompleta a la Autoridad Nacional de Protección de Datos Personales.
- No cesar en el tratamiento ilícito de datos personales, cuando existiese un previo requerimiento de la Autoridad Nacional de Protección de Datos Personales.
- No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales, no obstante haber sido requerido para ello por la Autoridad Nacional de Protección de Datos Personales.

IV. Sanciones Efectuadas

La Dirección de Protección de Datos Personales ha ejecutado veinte (20) procesos administrativos sancionadores a organizaciones públicas y privadas. Las sanciones se dividen por sector según cuadro mostrado a continuación:

N°	Sector	# de organizaciones sancionadas
1	Educación	7
2	Salud	6
3	Retail	3
4	Colegios profesionales	2
5	Centrales de riesgo	1
6	Transporte	1
TOTAL		20

1. Consentimiento inválido

La recopilación de datos personales por cualquier medio (físico o electrónico) requiere de una fórmula válida para obtener el consentimiento dispuesto en la Ley. Por ejemplo, el consentimiento debe ser otorgado con anterioridad a la recopilación de datos personales y no se admiten formas de consentimiento en donde este no haya sido expresado de forma directa. Las sanciones impuestas por este aspecto han llegado hasta cinco (5) unidades impositivas tributarias (S/. 19,750.00).

2. No inscripción del banco de datos

Existen empresas que no han registrado sus bancos de datos, o que no han registrado todos los bancos de datos personales que utilizan en sus operaciones. Por ejemplo, una empresa ha sido sancionada por no registrar el banco de datos de pacientes con veinticinco (25) unidades impositivas tributarias (S/. 98,750.00).

3. Incumplimiento de disposiciones de flujo transfronterizo de datos

No comunicar que los datos personales son transferidos a otras entidades fuera del territorio nacional genera sanciones por parte del ente rector, las cuales han ascendido hasta quince (15) unidades impositivas tributarias (S/. 59,250.00).

4. Utilización de imágenes de alumnos o clientes, sin consentimiento

Para efectos de marketing o eventos institucionales se utilizan imágenes del personal o clientes, sin embargo, no contar con un consentimiento explícito genera sanciones por el ente rector. Se han impuesto multas de hasta cinco (5) unidades impositivas tributarias (S/. 19,750.00) por el incumplimiento.

5. Obstrucción de fiscalización

Son cuatro (4) organizaciones que han obstaculizado el trabajo de la Autoridad de Protección de Datos Personales y que por ello han sido sancionadas con multas de hasta quince (15) unidades impositivas tributarias (S/. 59,250.00).

Puede revisar los procesos administrativos sancionadores efectuados por la Autoridad en el siguiente enlace: http://www.minjus.gob.pe/procedimientos-administrativos-sancionadores/

V. Nivel de exposición a una sanción

Para determinar cuál es el nivel de exposición de su organización ante una sanción, se han definido actividades que deben ser realizadas y que el no efectuarse pueden ser puntos de sanción a ser considerados por la Autoridad. Entre ellas se encuentran:

N°	Requerimiento de la Ley de Protección de Datos Personales	Sanción
1	¿Se han inscrito los bancos de datos personales de la organización en el Registro de Nacional de Protección de Datos Personales?	GRAVE - HASTA 50 UIT
2	¿Se han inscrito el Flujo Transfronterizo de Datos Personales (para datos personales transferidos al exterior) en el Registro Nacional de Protección de Datos Personales?	GRAVE - HASTA 50 UIT
3	¿Se solicita el consentimiento con una finalidad específica en todos los canales de la organización en los cuales se recopila datos personales?	GRAVE - HASTA 50 UIT
4	¿Se cuenta con acuerdos formales con terceros, incluyendo cláusulas de confidencialidad, cuando la organización transfiere datos personales?	GRAVE - HASTA 50 UIT
5	¿Se han implementado medidas de seguridad técnicas como control de acceso, trazabilidad sobre el uso de datos personales, respaldo y recuperación de datos personales, entre otras medidas que protejan los datos personales?	GRAVE - HASTA 50 UIT

En base a las respuestas a cada a uno de los requerimientos básicos presentados, se puede dimensionar que tan cercana o lejana está la organización en relación a la adecuación a la LPDP. Es importante mencionar que el cuadro presentado no reemplaza a un análisis a mayor profundidad del cumplimiento de la LPDP por la organización, dado que existen mayores requerimientos que evaluar a fin de mitigar cualquier riesgo de sanción.

VI. Conclusiones

A fin de abordar una iniciativa para adecuar su organización a la Ley de Protección de Datos Personales se debe considerar:

Enfoque Transversal

La adecuación a la ley de protección de datos personales requiere de un enfoque transversal que cubra todas las áreas de la organización sin excepción. La ausencia de identificación del uso y tratamiento de datos personales en un área en específico puede incrementar el riesgo de sanción por parte de la autoridad.

El registro del banco de datos no es suficiente

Las organizaciones privadas y públicas están registrando sus bancos de datos ante el Ministerio de Justicia considerando que es la única acción a realizar, sin embargo, las fiscalizaciones y sanciones efectuadas a la fecha también están orientadas al cumplimiento de la adopción de medidas organizativas, jurídicas y técnicas para proteger los bancos de datos.

Gobierno de datos personales

En el marco de la presente ley, las organizaciones deben incrementar su nivel de gobierno de datos personales que utilizan en sus operaciones a través de la documentación del ciclo de vida del dato desde su creación, tratamiento, transferencia y baja del mismo.

Asistencia especializada

Para evitar sanciones, es importante contar con asistencia especializada en la adecuación a la ley de protección de datos personales que cuente con un enfoque en donde participan tres tipos de expertos:

- Experto en Procesos de Negocio.
- Experto en Asesoría Legal.
- Experto en Seguridad de la Información y Tecnología.

BDO ha asistido a organizaciones líderes en su sector (tanto públicas como privadas) en la adecuación a la LPDP con bastante éxito.
Son más de 20 empresas asesoradas por nuestros expertos.
La gente que conoce, conoce BDO.

CONTACTO

Marco Caldas
Socio
mcaldas@bdo.com.pe

Victor Vera Tudela
Gerente Senior de Consultoría
vveratudela@bdo.com.pe

www.bdo.com.pe
+51 1 7053535