

SE PUBLICA MODIFICACIÓN AL REGLAMENTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES

El 30 de noviembre de 2024, se publicó el Decreto Supremo 016-2024-JUS "Nuevo Reglamento de Protección de Datos Personales".

¿CUÁLES SON LAS PRINCIPALES NOVEDADES QUE TRAE EL NUEVO REGLAMENTO?

El proyecto de Reglamento señala diversas modificaciones, entre las más relevantes encontramos las siguientes:

DESIGNACIÓN OBLIGATORIA DE UN OFICIAL DE DATOS PERSONALES

El Responsable del Tratamiento y el encargado del tratamiento debeN designar un Oficial de Datos Personales en los siguientes supuestos:

1. El tratamiento lo lleve una autoridad u organismo público (Ley de Gobierno Digital).
2. Se realicen tratamiento de grandes volúmenes de datos (en cantidad o tipos) que puedan afectar a un gran número de personas, o cuando se trate datos sensibles que produzca un perjuicio a los derechos o libertades de los titulares de los datos.
3. La principal actividad sea el tratamiento de datos personales sensibles.

Contingencia: Infracción leve, pasible a ser sancionada con una multa entre las 0.5 a 50UIT.

EVALUACIÓN DE IMPACTO

El Responsable del Tratamiento puede realizar (de manera facultativa) una evaluación de impacto cuando trate grandes volúmenes de datos, datos sensibles, datos con fines de crear perfiles personales, datos de personas en especial situación de vulnerabilidad u otros supuestos que determine la Autoridad.

La evaluación debe elaborar tomando en cuenta la NTP-ISO/IEC 27005 y la NTP-ISO 31000 en su edición vigente.

NOTIFICACIÓN OBLIGATORIA DE INCIDENTES DE SEGURIDAD

En caso exista un incidente de seguridad, se debe notificar a la Autoridad de Protección de Datos Personales dentro de las 48 horas de haber tenido constancia de ello, el contenido de la notificación debe contener como mínimo:

1. Naturaleza del incidente.
2. Comunicar el nombre y los datos de contacto del oficial de datos personales.
3. Posibles consecuencias del incidente.
4. Medidas adoptadas.

Contingencia: Infracción grave, pasible a ser sancionada con una multa entre las 5 a 50 UIT(s).

PRINCIPIO DE RESPONSABILIDAD PROACTIVA

Se agregó el principio de responsabilidad proactiva, el cual señala que en el tratamiento de datos personales se deben aplicar las medidas legales, técnicas y organizativas a fin de garantizar el cumplimiento efectivo de la implementación de la normativa de datos personales.

FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

Se señaló que cuando el Responsable del Tratamiento realice un flujo transfronterizo de datos personales a un país que no cuente con un nivel adecuado de protección de datos personales debe exigir garantías adecuadas para el flujo transfronterizo de datos, las cuales son cláusulas modelo, o un código de conducta que cuente con una opinión favorable de la Autoridad.

TRATAMIENTO ESPECIALES DE DATOS PERSONALES

- Se agregó a el tratamiento de datos para publicidad y prospección comercial como una categoría de tratamiento especial. Asimismo, se señaló criterios que el Responsable del Tratamiento debe tomar en cuenta cuando contrate a un tercero (Encargado del Tratamiento).
- Se ha enfatizado las obligaciones del Responsable del tratamiento frente a al tratamiento de datos de menores de edad a fin de garantizar la protección del niño y de sus derechos, en especial en la publicación o difusión de sus datos personales a través de servicios digitales.

MEDIAS DE SEGURIDAD

Se han agregado obligaciones relativas a medidas de seguridad como:

1. El Responsable del Tratamiento debe contar con una política de seguridad aprobada formalmente con fecha cierta.
2. Controles para mantener las áreas seguras
3. Controles para mantener los equipos seguros dentro y fuera de las instalaciones.

PORTABILIDAD

Se ha regulado la figura de la portabilidad, señalando que el titular de los datos personales puede solicitar la transferencia de sus datos a otro Responsable del Tratamiento cuando:

1. El tratamiento este basado en el consentimiento o en una relación contractual en la que el titular del dato es parte.
2. El tratamiento se ejerza mediante medios automatizados

¿QUÉ INFRACCIONES SE HAN MODIFICADO Y/O INCORPORADO?

Infraacciones leves	Infraacciones graves	Infraacciones muy graves
<p>Incorporado: Informar de forma incompleta de dos o menos de dos condiciones del tratamiento de los datos personales señaladas en el artículo 18 de la Ley.</p> <p>Incorporado: Atender fuera de plazo el ejercicio material de los derechos del titular de datos personales, cuando legalmente proceda</p> <p>Incorporado: No designar al Oficial de Datos Personales, cuando así corresponda.</p>	<p>Incorporado: No inscribir o actualizar en el Registro Nacional de Protección de Datos Personales los actos establecidos en el artículo 34 de la Ley, luego de que ello hubiera sido requerido por la Autoridad Nacional de Protección de Datos Personales.</p> <p>Incorporado: Obstruir el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales.</p>	<p>Incorporado: Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia, y generando con ello un perjuicio al titular del dato personal sensible o una exposición no autorizada de sus datos personales sensibles.</p>

¿CUÁNDO ENTRA EN VIGENCIA EL REGLAMENTO?

1 año después de la fecha de publicación del reglamento.



Empresas con ventas anuales superiores a 2300 UIT

2 años después de la fecha de publicación del reglamento.



Empresas con ventas anuales superiores a 1700 UIT y hasta el monto máximo de 2300 UIT.

3 años después de la fecha de publicación del reglamento.



Empresas con ventas anuales superiores a 150 UIT y hasta el monto máximo de 1700 UIT.

4 años después de la fecha de publicación del reglamento.



Empresas con ventas anuales superiores a 150 UIT y otros equivalentes.

Material preparado por el área de Protección de Datos Personales y Seguridad de la Información.

Para más información puede contactar a carolquiroz@esola.com.pe



Carol Quiroz
Socia



Daniela Chávez
Asociada