

Entró en vigencia el Nuevo Reglamento de la Ley de Protección de Datos Personales

A partir del 30 de marzo de 2025, las siguientes obligaciones contenidas en el nuevo Reglamento de la LPDP entrarán en vigencia:

1. Designación obligatoria de un Oficial de Protección de Datos en los siguientes casos:

- (a) 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 de datos sensibles que produzca un perjuicio a los derechos o libertades de los titulares de los datos.
- (b) La principal actividad sea el tratamiento de datos personales sensibles.

La falta de nombramiento del OPD será considerada una infracción leve, pasible de una multa entre las 0.5 a 5 UIT. Esta obligación será obligatoria en noviembre del 2025 para empresas con ventas anuales superiores a 2300 UIT.

2. Notificación de incidentes de seguridad digital

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:

- (a) Naturaleza del incidente.
- (b) Comunicar el nombre y los datos de contacto del oficial de datos personales.
- (c) Posibles consecuencias del incidente.
- (d) Medidas adoptadas.

La falta de notificación de los incidentes será considerada una infracción grave, pasible de una multa entre las 5 a 50 UIT.

3. Comunicar la existencia de decisiones automatizadas

Esta obligación incluye cualquier decisión automatizada, incluida la **elaboración de perfiles**, tomando en consideración las consecuencias para el titular del dato. El titular del dato personal tiene derecho a no ser objeto de decisiones, automatizadas o no, que le produzcan efectos jurídicos, discriminación o le afecten de manera significativa.

Se deberá comunicar en la política de privacidad.

La falta de cumplimiento podrá ser considerada como un incumplimiento al deber de informar lo que constituye una infracción grave, pasible de una multa entre las 5 a 50 UIT.

4. Aplicación del principio de responsabilidad proactiva para responsables y encargados del tratamiento

Lo cual implica que se deberán adoptar medidas legales, técnicas y organizativas para **garantizar** el cumplimiento efectivo de la normativa de datos personales, contando con la **capacidad de demostrar tal cumplimiento**.

Aplicar este principio contribuirá a atenuar la responsabilidad administrativa.

5. Protección de menores de edad en entornos digitales

Implica obtener el consentimiento del tutor o representante legal. Excepcionalmente se permite el consentimiento de mayores de 14 y menores de 18, para productos o servicios adaptados a su edad, mediante políticas con lenguaje comprensible.

Se deberá realizar esfuerzos razonables para la verificación de identidad (edad) de quienes otorgan el consentimiento.

6. Tratamiento de datos para publicidad y prospección comercial

Se regula el primer contacto, el cual es posible siempre y cuando se haya obtenido de manera lícita los datos personales. En caso el titular quiera revocar su consentimiento, el responsable del tratamiento tiene un plazo máximo de diez (10) días hábiles para atender el reclamo.

No obtener el consentimiento será considerado como una infracción grave, pasible de una multa entre las 5 a 50 UIT.

7. Nuevas reglas para el flujo transfronterizo de datos

La ANPD emitirá resoluciones con el detalle de países que cumplen con el nivel adecuado de tratamiento de los datos personales.

Si el país receptor no cuenta con un nivel adecuado de tratamiento, se deberá aplicar las "Cláusulas Contractuales Modelo" de la Red Iberoamericana de Protección de Datos, aprobadas por la ANPD mediante R.D. 074-2022-JUS/DGTAIPD.

Se mantiene la obligación de comunicar el flujo transfronterizo de datos personales.

No cumplir con las reglas del flujo transfronterizo podrá ser considerada una multa leve en el caso de falta de inscripción, o una multa grave, en el caso de falta del deber de informar.

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

Para más información, contactarse a los siguientes correos electrónicos:

- carolquiroz@esola.com.pe
- danielachavez@esola.com.pe



Carol Quiroz
Socia



Daniela Chávez
Asociada