Client Memo

# Conoce los aspectos clave del Nuevo Reglamento de la Ley de Protección de Datos Personales

Payet Rey Cauvi Pérez

La Ley N° 29733, Ley de Protección de Datos Personales (la "LPDP"), cuenta con un reglamento desde el año 2013. No obstante, la Autoridad Nacional de Protección de Datos Personales (la "ANPDP") consideró que era necesario actualizar dicho reglamento en atención a los avances tecnológicos y nuevas tendencias en la materia. En ese sentido, el 30 de noviembre de 2024 se publicó el Decreto Supremo N° 016-2024-JUS por medio del cual se aprueba el nuevo reglamento de la LPDP (el "Nuevo Reglamento").

A continuación, detallamos las principales novedades del Nuevo Reglamento:

## I. Nuevas definiciones y definiciones modificadas

- Se han incorporado nuevas definiciones, dentro de las cuales se encuentran las siguientes: (i) elaboración de perfiles; (ii) evaluación de impacto relativo a la protección de datos personales; (iii) incidente de seguridad de datos personales; (iv) oficial de datos personales; y, (v) representante.[1]

- Asimismo, se han modificado diversas definiciones contenidas en el antiguo reglamento de la LPDP. Entre ellas destacamos la definición de "datos sensibles" que contempla la categoría de datos neuronales.

## II. Sobre el ámbito de aplicación territorial

- Se añaden dos (2) supuestos en los que la LPDP y el Nuevo Reglamento son de aplicación al titular o responsable del tratamiento que no se encuentra establecido en territorio peruano:

| | |
|---|---|
| **Cuando la oferta de bienes o servicios este dirigida a titulares de datos personales ubicados en el territorio peruano.** | **Cuando realiza actividades de análisis de comportamiento o elaboración de perfiles de titulares de datos personales ubicados en territorio peruano.** |

1 **Elaboración de perfiles**: forma de tratamiento automatizado de datos personales que permite evaluar aspectos de una persona natural, de manera específica y continua (por ejemplo, preferencias personales).
**Evaluación de impacto relativo a la protección de datos personales:** mecanismo por medio del cual el titular del banco de datos personales o responsable del tratamiento de datos realiza, de forma previa al tratamiento de los mismos, un análisis o evaluación del impacto o riesgos que implica el tratamiento de datos.
**Incidente de seguridad de datos personales:** toda vulneración de la seguridad que ocasione la destrucción, pérdida, alteración ilícita de los datos personales o la comunicación o exposición no autorizada a dichos datos.
**Oficial de Datos Personales:** persona designada para la verificación, asesoramiento e implementación del cumplimiento del régimen jurídico sobre protección de datos personales.
**Representante:** persona natural o jurídica designada de manera expresa, por el titular del banco de datos personales o responsable, para fines del tratamiento de datos personales.

- En los casos en que los titulares o responsables no se encuentren en el territorio peruano y les sea aplicable la LPDP y el Nuevo Reglamento, se deberá -entre otros- **designar un representante en el territorio peruano o para el territorio peruano** que actúe como punto de contacto con la ANPDP. La designación podrá realizarse (i) informándolo públicamente a través de su política de privacidad; o, (ii) comunicándolo a la ANPDP.

## III. Obligaciones previstas en el Nuevo Reglamento

- Sobre el deber de consentimiento

Para que el **consentimiento sea "informado**", se agregan dos (2) condiciones que deben ser puestas en conocimiento del titular de los datos no previstas en la LPDP:

i. La existencia de decisiones automatizadas y elaboración de perfiles, así como las consecuencias de ello para los titulares de los datos personales; y,
ii. La fuente de recopilación de los datos (en caso los datos hayan sido recopilados de fuentes accesibles al público o no hayan sido recopilados directamente del titular de los datos personales y de ser requerido por este último).[2]

Se contempla la figura del **"primer contacto" como mecanismo válido** para obtener el consentimiento del titular del dato personal para finalidades publicitarias y de prospección comercial.

En caso el titular de los datos personales revoque su consentimiento, se deberá **adecuar el tratamiento a la revocatoria en un plazo no mayor a diez (10) días hábiles.** [3]

- Sobre las notificaciones de incidentes de seguridad:

  - En caso de un incidente de seguridad que genere una gran exposición de datos o pueda afectar a un gran número de personas, el titular del banco de datos o responsable deberá **comunicarlo a la ANPDP** en un plazo máximo de cuarenta y ocho (48) horas desde que tomó conocimiento o constancia del incidente. En caso el reporte exceda dicho plazo, se deberá justificar la dilación, indicando los motivos y sustento.

  - Se deberá **comunicar a los titulares de datos personales** sobre dicho incidente de seguridad si este afecta otros de sus derechos. La comunicación debe ser un lenguaje sencillo y claro.

  - Si el **incidente de seguridad se generó a través de un entorno digital**, también deberá ser comunicado al Centro Nacional de Seguridad Digital.

  - Los titulares de banco de datos o responsables tienen el **deber de documentar cualquier incidente de seguridad,** incluyendo los hechos, efectos y medidas adoptadas.

- Sobre el Oficial de Datos Personales:

  - **El titular, responsable y encargado de tratamiento** deben designar a un Oficial de Datos Personales cuando se presente alguno de los siguientes supuestos:

2 Con relación a la condición "fuente de recopilación de los datos", se precisa que ello deberá ser informado en el primer contacto que se realice con el titular de los datos personales.
3 Se incrementa el plazo para adecuar el tratamiento de datos en el caso de revocatoria, de 5 a 10 días hábiles.

El tratamiento lo lleve a cabo una entidad pública

Cuando se realice tratamiento de grandes volúmenes de datos personales, en cantidad o tipo de datos, o que pueda afectar a un gran número de personas o cuando se trate de datos sensibles o cuando se produzca un perjuicio evidente a otros derechos o libertades del titular del dato personal.

Cuando realicen actividades cuyo giro del negocio comprenda tratamiento de datos sensibles

- Se indica que los **grupos empresariales** también podrán nombrar a un único Oficial de Datos Personales, siempre y cuando sea fácil contactarlo desde cada establecimiento.
- Los **datos de contacto del Oficial de Datos Personales deben ser publicados** en un lugar visible para que los titulares puedan tener conocimiento de ello.

- Sobre las medidas de seguridad:

| | | |
|---|---|---|
| Se establece el deber de contar con un **"documento de seguridad"** aprobado formalmente y con fecha cierta. | Se deberán establecer **controles para garantizar la seguridad de las áreas.** | Se deberán establecer **controles para garantizar la seguridad de los equipos dentro y fuera de las instalaciones.** |

Asimismo, se establecen plazos vinculados a la implementación de las medidas de seguridad:

- **Verificación periódica de la gestión de privilegios:** Como mínimo, de forma semestral.
- **Copias de respaldo seguras y continuas**: Como mínimo, con una frecuencia semanal.
- **Registros de interacciones lógicas:** Estos deben realizarse de forma continua y conservarse, como mínimo, por dos (2) años.

- Sobre los derechos de los titulares de datos personales

  - Se establece un nuevo derecho de los titulares de datos personales: **el derecho de portabilidad** como manifestación del derecho de acceso. Por medio de este derecho, el titular de los datos puede solicitar sus datos personales en un formato estructurado, de uso común y lectura mecánica, **y transmitirlos a otro responsable de datos** cuando: (i) el tratamiento esté basado en el consentimiento o en una relación contractual en la que el titular es parte; y, (ii) el tratamiento se realiza de manera automatizada.

  - El ejercicio de los derechos ARCO podrá realizarse ante los encargados de tratamiento. Sin embargo, estos deberán trasladar la solicitud a los titulares o responsables de tratamiento en un plazo máximo de tres (3) días hábiles, para que estos últimos la atiendan.

## IV. Sobre la tipificación de infracciones

El Nuevo Reglamento ha incorporado -entre otras- las siguientes infracciones:

**Infracciones graves**

- No cumplir con el deber de información o informar de forma incompleta de tres (3) a más condiciones del tratamiento.
- Realizar el tratamiento de datos personales incumpliendo las medidas de seguridad establecidas, y generando con ello un perjuicio al titular del dato personal o una exposición no autorizada de sus datos personales.
- Negar o demorar injustificadamente a la ANPDP el ingreso a las instalaciones objeto de la fiscalización.

- Negarse injustificadamente a proporcionar a la ANPDP la información o la documentación relativa al tratamiento de datos personales que esta le requiera en el marco de un procedimiento administrativo en curso.
- No comunicar a la ANPDP un incidente de seguridad de acuerdo con lo dispuesto en el Nuevo Reglamento.

**Infracciones muy graves**

- Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas, y generando con ello un perjuicio al titular del dato personal sensible o una exposición no autorizada de sus datos personales sensibles.

## V. Otras disposiciones relevantes del Nuevo Reglamento

- De forma facultativa y previa al tratamiento de datos personales, se podrán realizar **evaluaciones de impacto relativo a la protección de datos personales.** Ello especialmente cuando se traten datos sensibles, de personas en situaciones de vulnerabilidad (e.g. menores de edad, personas con discapacidad, entre otros); o cuando se realice tratamiento de grandes volúmenes de datos u otros supuestos determinados por la ANPDP.

- **Eliminación de tasas administrativas:** La inscripción, modificación y cancelación de registros de bancos de datos personales serán trámites gratuitos. Asimismo, el procedimiento de inscripción de bancos de datos es de **aprobación automática.**

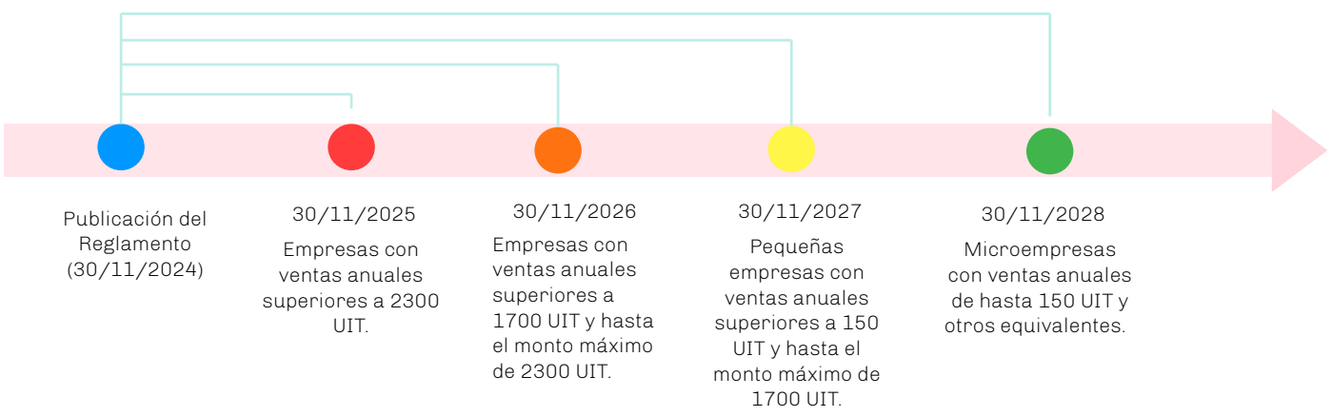
- Sobre el beneficio de pronto pago (reducción del 40% de la multa impuesta), se precisa que **solo será aplicable si el administrado no interpone recurso de apelación contra la resolución que impone la sanción.**

## VI. Entrada en vigor del Nuevo Reglamento

- El Nuevo Reglamento entrará en vigor el 30 de marzo de 2025.

- Las disposiciones vinculadas al derecho de portabilidad entrarán en vigor el 30 de septiembre de 2025.

- Las disposiciones vinculadas a la designación del Oficial de Datos Personales se implementarán conforme al siguiente cronograma:




**Carlos Patrón**
**cap@prcp.com.pe**
SOCIO
VER PERFIL

**Julia Loret de Mola**
**jld@prcp.com.pe**
SOCIO
VER PERFIL

**Marianna Vallvé**
**mvg@prcp.com.pe**
SENIOR EXPERT
VER PERFIL

**Ana Lucía Figueroa**
**afd@prcp.com.pe**
ASOCIADA
VER PERFIL

**Jimena Pérez**
**jpd@prcp.com.pe**
ASOCIADA
VER PERFIL

**Luciana Márquez**
**lma@prcp.com.pe**
ASOCIADA
VER PERFIL