

# COMPENDIO SOBRE PROTECCIÓN DE DATOS PERSONALES: NORMATIVA Y CRITERIOS INTERPRETATIVOS RELEVANTES

PRIMERA EDICIÓN OFICIAL



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos



# COMPENDIO SOBRE PROTECCIÓN DE DATOS PERSONALES: NORMATIVA Y CRITERIOS INTERPRETATIVOS RELEVANTES

PRIMERA EDICIÓN OFICIAL



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Primera Edición Oficial: diciembre 2025  
Formato digital

**JOSÉ ENRIQUE JERÍ ORÉ**  
Presidente de la República del Perú

**WALTER ELEODORO MARTÍNEZ LAURA**  
Ministro de Justicia y Derechos Humanos

**SHADIA ELIZABETH VALDEZ TEJADA**  
Viceministra de Justicia

**WALTHER JAVIER IBEROS GUEVARA**  
Viceministro de Derechos Humanos y Acceso a la Justicia

**CÉSAR AUGUSTO BORDA GONZALES**  
Director General de Desarrollo Normativo y Calidad Regulatoria



**EDUARDO LUNA CERVANTES**  
Director General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales

**ANA MARIA CECILIA VALENCIA CATUNTA**  
Directora de Sistematización Jurídica y Difusión

**MARÍA ALEJANDRA GONZÁLES LUNA**  
Directora de la Dirección de Protección de Datos Personales (e)

**INGRID MARIA DEL CARMEN BOCANEGRA CALDERÓN**  
Analista Legal de Textos Legales Oficiales

**NICOLE STEPHANIE CÁCERES CHATA**  
Asistente Legal de Textos Oficiales

Colaboración de la Revisión y Actualización:

**SETI JAIR ANGELINO PÉREZ**  
Ejecutivo de la Dirección de Sistematización Jurídica y Difusión

**Elaboración de las opiniones consultivas:**  
Equipo de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

**Diseño y diagramación:** Personal de la Oficina General de Imagen y Comunicaciones del Ministerio de Justicia y Derechos Humanos.

**DERECHOS RESERVADOS**  
**DECRETO LEGISLATIVO N° 822**

### **DISTRIBUCIÓN GRATUITA**

Derechos de Edición  
2025 - Ministerio de Justicia y Derechos Humanos  
Calle Scipión Llona N° 350 - Miraflores, Lima 18  
Dirección General de Desarrollo Normativo y Calidad Regulatoria  
Dirección de Sistematización Jurídica y Difusión

Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2025-15342



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos



## PRÓLOGO

El progreso de las tecnologías de la información y la comunicación de las últimas décadas, ha hecho más accesibles y cotidianas actividades de toda índole, teniendo influencia no solo en la vida del individuo, sino en escenarios colectivos, en la sociedad misma, llegando a crear nuevos espacios para tales actividades, como sucede con el comercio electrónico, los procedimientos administrativos o las redes sociales, cada una con finalidades muy distintas, pero que comparten una característica: El uso de información como insumo principal para su funcionamiento y más específicamente, de datos personales. Lo que para el usuario de una aplicación móvil o de un sitio web es la simplificación de una actividad como comprar productos en el extranjero o presentar una solicitud a una entidad pública, representa operaciones de tratamiento de datos personales más complejas y más riesgosas para los derechos fundamentales de las personas a las que corresponden estos datos, debido a nuevas amenazas que suelen exceder la mera intromisión a sus espacios íntimos o privados, pudiendo afectar otros bienes jurídicos, como actos de discriminación, de afectaciones al patrimonio de dichas personas o la recolección y manipulación descontrolada de datos sensibles, como datos de salud o datos relativos a sus ingresos económicos.

La protección de dicha clase de información no es ajena a nuestro ordenamiento jurídico, se le reconoce como un derecho fundamental en el artículo 2, inciso 6, de la Constitución Política del Perú, así como jurisprudencialmente, en sentencias del Tribunal Constitucional. Es con la Ley N° 29733, Ley de Protección de Datos Personales, que se garantiza tal derecho fundamental en la práctica, estableciendo principios rectores para la licitud y adecuación del tratamiento de datos personales, obligaciones por parte de las personas y entidades responsables de su realización, así como los derechos específicos (los derechos ARCO) que asisten a las personas por su condición de titulares de datos personales; y primordialmente, el órgano responsable de tal garantía, la Autoridad de Protección de Datos Personales, ejercida por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Cabe señalar que esta ley es complementada por su reglamento recientemente renovado, aprobado por el Decreto Supremo N° 016-2024-JUS, en vigencia desde el 31 de marzo de 2025. Por medio de esta norma reglamentaria, se reconocen los principios de Transparencia y especialmente, el de Responsabilidad Proactiva, que establece la obligación de los responsables del tratamiento de ser capaces, permanentemente, de adoptar medidas encaminadas al cumplimiento de la normativa, haciendo perenne la función preventiva sobre los riesgos que deriven de las actividades de tratamiento que efectúen. Destacan también, la introducción de obligaciones aplicables a circunstancias especiales de tratamiento, como la notificación de incidentes de seguridad sobre datos personales.

Estas innovaciones a la normativa obedecen a la necesidad de que los responsables del tratamiento de datos personales, asuman un mayor compromiso para prevenir alguna situación ilícita o riesgosa para los derechos de las personas, considerando su dominio sobre tales actividades, que le brinda una mejor posición para su control, renovando el enfoque de la protección de datos personales, pasando de una etapa de control basada meramente en la fiscalización a un enfoque preventivo, de anticipación necesaria a los crecientes riesgos que las nuevas tecnologías de la información y la mayor masificación del tratamiento conllevan.

Para confrontar este nuevo escenario exitosamente, es necesario que los profesionales responsables sobre las actividades de tratamiento de datos personales en las entidades públicas y privadas, tengan acceso a estos cambios normativos, así como a los criterios que la Autoridad Nacional de Protección de Datos Personales ha adoptado respecto de situaciones frecuentes y que con tales conocimientos, puedan aportar respuestas eficientes para sus finalidades y primordialmente, equilibradas y respetuosas de los derechos fundamentales de las personas.

Esta publicación ofrece manifestaciones de la experiencia práctica en la materia de protección de datos personales, plasmada en las consultas absueltas por la mencionada autoridad, en mérito de las funciones atribuidas legalmente, atendiendo a las interrogantes planteadas por diversas entidades públicas y privadas respecto de la interpretación y aplicación de la normativa de protección de datos personales. Con ello, se presentan respuestas normativas aplicables a las temáticas sobre las cuales se consulta, demostrando la conciliación que, efectivamente, existe entre normativa sectorial o relativa a funciones de una entidad específica, y el desarrollo del derecho fundamental a la protección de datos personales: Por ejemplo, la legitimación de la publicación de datos de servidores públicos en el Registro Nacional de Sanciones no requiere de consentimiento de parte de estos, ni la Contraloría General de la República lo requiere para acceder a ellos, en razón del ejercicio regular de sus funciones legalmente establecidas, sin perjuicio del acatamiento de otros principios rectores del tratamiento de datos personales, establecidos en la mencionada ley.

El presente compendio, que se acompaña con una edición oficial actualizada de la Ley N° 29733, Ley de Protección de Datos Personales, y de su reglamento, aprobado por el Decreto Supremo N° 016-2024-JUS, del 30 de noviembre de 2024, da cuenta de algunos de los criterios de interpretación más destacados entre las opiniones consultivas emitidas en el período 2022-2025, evidenciando con ello la evolución en la función orientativa de la Autoridad Nacional de Protección de Datos Personales y su esfuerzo por conjugar lo abstracto de las normas, sus límites y las obligaciones que demandan, con la experiencia concreta y cotidiana del quehacer estatal y privado.

Esperamos que esta publicación sea de utilidad para los distintos actores, públicos y privados, que interactúan con los titulares del derecho fundamental a la protección de datos personales y asuman su rol vinculado a la instauración de una cultura favorable a la protección de datos personales en sus organizaciones y en la sociedad. La promoción y vigencia de los derechos humanos es un asunto que nos compete a todos y todas, y es un indicativo incontestable de la democracia constitucional y el Estado de Derecho que cobija a la nación.

**Eduardo Luna Cervantes**

Director General

Dirección General de Transparencia, Acceso a la  
Información Pública  
y Protección de Datos Personales

## PRESENTACIÓN

La protección de los datos personales es un derecho fundamental que el Estado democrático y social de Derecho brinda a la persona para su desarrollo y dignidad, gracias al cual puede decidir cuánto de su personalidad comparte con los entornos públicos, donde se desenvuelve y cómo lo hace, reservando así ciertos aspectos para su espacio privado e íntimo; todo ello, mediante el control del adecuado tratamiento de su información personal.

Este derecho se encuentra desarrollado en el artículo 2, inciso 6, de la Constitución Política del Perú, el cual establece que toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. Esto se desarrolla a través de una serie de facultades que tiene para ejercer control sobre la información personal que le concierne, contenida en registros de entidades particulares o privadas, constituyendo una autodeterminación de la vida íntima con la que resguarda los rasgos de su personalidad que se plasmen a través de dicha información.

Este derecho fundamental, entonces, protege a la persona no solo de la intromisión o escrutinio, también de perjuicios tangibles para otros bienes, como la vulneración de otros derechos fundamentales, daños materiales o económicos, factibles por medio del manejo ilícito y descontrolado de la información personal, siendo este riesgo aún mayor en el entorno de la progresiva evolución de las tecnologías de la información y comunicación.

Las garantías y concreción de tal derecho se desarrollan en la Ley N° 29733, Ley de Protección de Datos Personales, que cuenta con el complemento de su nuevo reglamento, aprobado por el Decreto Supremo N° 016-2024-JUS, vigente desde el 31 de marzo de 2025. Estas normas regulan los principios rectores del tratamiento de datos personales, los derechos del titular de datos personales, obligaciones del responsable y encargado del tratamiento de datos personales, así como el régimen de infracciones y sanciones en esta materia; regulación que presta atención a las mencionadas innovaciones tecnológicas que conllevan situaciones especiales de uso de información personal, tales como el flujo transfronterizo de esta, acciones

de perfilamiento y recopilación con el empleo de herramientas de geolocalización, big data e inteligencia artificial, entre otras innovaciones; el tratamiento de datos sensibles como los datos biométricos, datos de salud, datos neuronales; así como las condiciones especiales de los datos personales y sus titulares, como sucede con los datos personales de niños y adolescentes.

El legislador peruano ha encargado al Ministerio de Justicia y Derechos Humanos, a través de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, ejercer Autoridad Nacional de Protección de Datos Personales (ANPD), la cual ejercita ciertas funciones especiales dirigidas

a garantizar la efectividad del derecho fundamental a la protección de datos personales, velando por el cumplimiento de la normativa mencionada.

En desempeño de su función orientadora, prevista en el artículo 33 de la Ley N° 29733, Ley de Protección de Datos Personales, la ANPD emite criterios interpretativos acerca de la aplicación de dicha normativa en determinadas situaciones generales, con lo que procuran guiar la actuación de los sujetos para que cumplan con las obligaciones establecidas en dicha ley y en su reglamento, así como robustecer el conocimiento de los derechos que esta premune a los titulares de los datos personales y de las formas de ejercerlo.

Para cumplir tales finalidades, es necesaria la promoción y difusión de las normas mencionadas, así como de los documentos que desarrollen a profundidad los criterios de aplicación, con mayor razón si tratan diversos escenarios de tratamiento de datos personales en actividades sectoriales (actividades de salud, desarrollo de funciones públicas y cumplimiento normativo), en los que se aprecia la transversalidad de dichas normas y la interacción del derecho fundamental a la protección de datos personales con otros bienes jurídicos relevantes.

En ese marco, el presente compendio constituye un valioso esfuerzo de sistematización de la normativa de protección de datos personales vigente en nuestro país a la fecha, con la novedad del Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, aprobado por el Decreto Supremo N° 016-2024-JUS, normativa que se presenta complementada con una cuidadosa selección de los criterios interpretativos más relevantes emitidos por la Autoridad Nacional de Protección de Datos Personales, que sirven para reflejar la aplicación de tales normas a supuestos prácticos frecuentes en las actividades privadas y públicas.

Por lo expuesto, nos complace presentar la Primera Edición Oficial del “Compendio sobre Protección de Datos Personales: normativa y criterios interpretativos relevantes”.

Diciembre 2025,

Walter Eleodoro Martínez Laura  
Ministro de Justicia y Derechos Humanos



# Resolución Viceministerial

Lima, 21 NOV. 2025

N 011-2025-JUS-VMJ

**VISTOS**, el Informe N° 146-2025-JUS/DGDNCR-DSJD, de la Dirección de Sistematización Jurídica y Difusión; el Oficio N° 2299-2025-JUS/DGDNCR, de la Dirección General de Desarrollo Normativo y Calidad Regulatoria; el Informe N° 473-2025-JUS/OGPM, de la Oficina General de Planeamiento, Presupuesto y Modernización; y, el Informe N° 1550-2025-JUS/OGAJ, de la Oficina General de Asesoría Jurídica;

**CONSIDERANDO:**

Que, el literal j) del artículo 7 de la Ley N° 29809, Ley de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, establece como función específica de esta Entidad, sistematizar la legislación e información jurídica de carácter general y promover su estudio y difusión, así como disponer su edición oficial;

Que, los literales c) y j) del artículo 11 de la citada norma establecen que el Viceministro de Justicia, por encargo del Ministro, tiene las funciones de velar por la sistematización y difusión de la legislación de carácter general de los tres niveles de Gobierno; y, emitir resoluciones viceministeriales en los asuntos que le corresponden, conforme a ley, respectivamente;

Que, el artículo 53 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N° 013-2017-JUS, señala que la Dirección General de Desarrollo Normativo y Calidad Regulatoria es el órgano de línea encargado, entre otras funciones, de sistematizar y difundir la legislación nacional y la jurisprudencia vinculante con la finalidad de mantener la coherencia y el perfeccionamiento del ordenamiento jurídico;

Que, asimismo, conforme al literal k) del artículo 54 del citado Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, la mencionada Dirección General tiene como función editar textos legales conteniendo la legislación nacional, con carácter de edición oficial;

Que, el literal g) del artículo 57 del mencionado Reglamento, establece que la Dirección de Sistematización Jurídica y Difusión, tiene entre sus funciones, editar y publicar con carácter de edición oficial, a través de medios impresos, electrónicos u otros similares, las normas legales sistematizadas, en particular códigos, leyes y compendios especializados de la legislación;

Que, mediante Informe N° 146-2025-JUS/DGDNCR-DSJD, la Dirección de Sistematización Jurídica y Difusión propone que es necesaria la publicación digital de la Primera Edición Oficial del "Compendio sobre Protección de Datos Personales: normativa y criterios interpretativos relevantes";



S. VALDEZ T.



B. CHAMORRO



P. R. FUJIV.



J. ROJAS G.

Que, en este contexto normativo, la Dirección General de Desarrollo Normativo y Calidad Regulatoria ha concluido que, con la finalidad de difundir tan importante norma de nuestro ordenamiento jurídico, es necesaria la publicación digital de la Edición Oficial indicada en el considerando anterior;

Que, mediante Informe N° 473-2025-JUS/OGPM, la Oficina General de Planeamiento, Presupuesto y Modernización señala que, en el ámbito de planeamiento respecto a la publicación digital de la Primera Edición Oficial del "Compendio sobre Protección de Datos Personales: normativa y criterios interpretativos relevantes", se vincula a la actividad operativa AOI00001500520: Edición y publicación con carácter oficial de la legislación nacional por medios impresos y/o electrónicos, del POI 2025 Actualizado - Versión 1, la misma que se encuentra alineada a la acción estratégica institucional AEI.03.02: Asesoría jurídica oportuna para las entidades públicas con el objetivo estratégico institucional OEI.03: Fortalecer la Seguridad Jurídica de la Sociedad, del PEI 2025-2030 del MINJUSDH; en ese sentido, no se manifiesta objeción a la aprobación de la señalada publicación digital mediante Resolución Viceministerial; y en materia presupuestal, no demandará asignación de mayores recursos presupuestarios para su financiamiento; por lo que se emite opinión favorable;

Que, en atención a las funciones del Viceministerio de Justicia, corresponde aprobar la publicación digital de la Primera Edición Oficial del "Compendio sobre Protección de Datos Personales: normativa y criterios interpretativos relevantes";

Con los visados de la Dirección General de Desarrollo Normativo y Calidad Regulatoria; de la Oficina General de Planeamiento, Presupuesto y Modernización; y de la Oficina General de Asesoría Jurídica;

De conformidad con lo dispuesto en la Ley N° 29809, Ley de Organización y Funciones del Ministerio de Justicia y Derechos Humanos; y, el Decreto Supremo N° 013-2017-JUS, que aprueba el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos;

**SE RESUELVE:**

**Artículo 1.-** Aprobar la publicación digital de la Primera Edición Oficial del "Compendio sobre Protección de Datos Personales: normativa y criterios interpretativos relevantes".

**Artículo 2.-** Autorizar a la Dirección General de Desarrollo Normativo y Calidad Regulatoria a estampar el sello de dicha Dirección General en la publicación digital de la Primera Edición Oficial del "Compendio sobre Protección de Datos Personales: normativa y criterios interpretativos relevantes".

**Artículo 3.-** Disponer la publicación digital de la Primera Edición Oficial del "Compendio sobre Protección de Datos Personales: normativa y criterios interpretativos relevantes", en la Sede Digital del Ministerio de Justicia y Derechos Humanos ([www.gob.pe/minjus](http://www.gob.pe/minjus)) y en el Portal del Sistema Peruano de Información Jurídica ([spijweb.minjus.gob.pe](http://spijweb.minjus.gob.pe)).

**Regístrese y comuníquese.**



B. CHAMORRO



D. R. RUIZ V.



J. ROJAS G.

*[Firma manuscrita]*  
**SABINA ELIZABETH VALDEZ TEJADA**  
Viceministra de Justicia  
Ministerio de Justicia y Derechos Humanos

## GUÍA DEL LECTOR

Para el correcto uso de la presente edición, el lector deberá tener en cuenta lo siguiente:

1. La presente edición consta de dos partes:

La primera parte contiene la Ley N° 29733 – Ley de Protección de Datos Personales y el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales aprobado mediante Decreto Supremo N° 016-2024-JUS.

La segunda parte contiene una selección sistematizada por materia de los criterios interpretativos relevantes emitidos por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, siendo esta una publicación desarrollada en formato digital.

2. El personal de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales realizó la selección sistematizada por materia de los criterios interpretativos emitidos por la Dirección General en mención.
3. El texto de cada artículo es el vigente al momento de la presente publicación.
4. El Texto del articulado es copia fiel del diario oficial El Peruano en lo que respecta a su contenido, incluyendo signos de puntuación y ortografía en general.
5. Las notas de pie de página se encuentran identificadas con números y hacen referencia a los dispositivos legales que modifican, incorporan, sustituyen o derogan artículos, párrafos e incisos de la Ley de Protección de Datos Personales y su reglamento, así como a las Fe de Erratas que rectifican el texto de los artículos.
6. Las fechas que aparecen entre paréntesis corresponden a las fechas de publicación de las normas en el diario oficial El Peruano.
7. La presente edición se encuentra actualizada hasta el 22 de noviembre de 2025.



---

# COMPENDIO SOBRE PROTECCIÓN DE DATOS PERSONALES

---



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos



---

# COMPENDIO NORMATIVO

---



## **Ley de protección de datos personales LEY N° 29733**

EL PRESIDENTE DE LA REPUBLICA

POR CUANTO:

El Congreso de la República

ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

### **LEY DE PROTECCIÓN DE DATOS PERSONALES**

Título Preliminar: Disposiciones generales.

Título I: Principios rectores.

Título II: Tratamiento de datos personales.

Título III: Derechos del titular de datos personales.

Título IV: Obligaciones del titular y del encargado del banco de datos personales.

Título V: Bancos de datos personales.

Título VI: Autoridad Nacional de Protección de Datos Personales.

Título VII: Infracciones y sanciones administrativas.

Disposiciones complementarias finales

## TÍTULO PRELIMINAR DISPOSICIONES GENERALES

### Artículo 1. Objeto de la Ley

La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

### Artículo 2. Definiciones

Para todos los efectos de la presente Ley, se entiende por:

- 1. Banco de datos personales.** Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.
- 2. Banco de datos personales de administración privada.** Banco de datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.
- 3. Banco de datos personales de administración pública.** Banco de datos personales cuya titularidad corresponde a una entidad pública.
- 4. Datos personales.** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
- 5. Datos sensibles.** Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos 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.
- 6. Días.** Días hábiles.
- 7. Encargado de tratamiento de datos personales.** Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos

personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales.

- 8. Encargo de tratamiento.** Entrega por parte del titular del banco de datos personales a un encargado de tratamiento de datos personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del encargado de tratamiento de los datos personales.
- 9. Entidad pública.** Entidad comprendida en el artículo I del Título Preliminar de la Ley N° 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces.
- 10. Flujo transfronterizo de datos personales.** Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.
- 11. Fuentes accesibles para el público.** Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso. Las fuentes accesibles para el público son determinadas en el reglamento.
- 12. Nivel suficiente de protección para los datos personales.** Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.
- 13. Persona jurídica de derecho privado.** Para efectos de esta Ley, la persona jurídica no comprendida en los alcances del artículo I del Título Preliminar de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- 14. Procedimiento de anonimización.** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.
- 15. Procedimiento de disociación.** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.

- 16. Titular de datos personales.** Persona natural a quien corresponde los datos personales.
- 17. Titular del banco de datos personales.** Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.
- 18. Transferencia de datos personales.** Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.
- 19. Tratamiento de datos personales.** Cualquier operación o procedimiento técnico, automatizado o no, 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<sup>1</sup>.

---

<sup>1</sup> Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

Artículo 2. Definiciones

Para todos los efectos de la presente Ley, se entiende por:

1. Banco de datos personales. Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.
2. Banco de datos personales de administración privada. Banco de datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.
3. Banco de datos personales de administración pública. Banco de datos personales cuya titularidad corresponde a una entidad pública.
4. Datos personales. Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
5. Datos sensibles. Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos 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.
6. Encargado del banco de datos personales. Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales.
7. Entidad pública. Entidad comprendida en el artículo I del Título Preliminar de la Ley N° 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces.
8. Flujo transfronterizo de datos personales. Transferencia internacional de datos

### **Artículo 3. Ámbito de aplicación**

La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles.

Las disposiciones de esta Ley no son de aplicación a los siguientes datos personales:

1. A los contenidos o destinados a ser contenidos en bancos de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar.
2. A los contenidos o destinados a ser contenidos en bancos de datos de

---

personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

9. Fuentes accesibles para el público. Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso. Las fuentes accesibles para el público son determinadas en el reglamento.
10. Nivel suficiente de protección para los datos personales. Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.
11. Persona jurídica de derecho privado. Para efectos de esta Ley, la persona jurídica no comprendida en los alcances del artículo I del Título Preliminar de la Ley N° 27444, Ley del Procedimiento Administrativo General.
12. Procedimiento de anonimización. Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.
13. Procedimiento de disociación. Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.
14. Titular de datos personales. Persona natural a quien corresponde los datos personales.
15. Titular del banco de datos personales. Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.
16. Transferencia de datos personales. Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.
17. Tratamiento de datos personales. Cualquier operación o procedimiento técnico, automatizado o no, 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.

El reglamento de esta Ley puede realizar un mayor desarrollo de las definiciones existentes.

administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito<sup>2</sup>.

## TÍTULO I PRINCIPIOS RECTORES

### **Artículo 4. Principio de legalidad**

El tratamiento de los datos personales se hace conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.

### **Artículo 5. Principio de consentimiento**

Para el tratamiento de los datos personales debe mediar el consentimiento de su titular.

### **Artículo 6. Principio de finalidad**

Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

---

2 Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

Artículo 3. Ámbito de aplicación

La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles.

Las disposiciones de esta Ley no son de aplicación a los siguientes datos personales:

1. A los contenidos o destinados a ser contenidos en bancos de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar.
2. A los contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito.

### **Artículo 7. Principio de proporcionalidad**

Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

### **Artículo 8. Principio de calidad**

Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento.

### **Artículo 9. Principio de seguridad**

El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

### **Artículo 10. Principio de disposición de recurso**

Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

### **Artículo 11. Principio de nivel de protección adecuado**

Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta Ley o por los estándares internacionales en la materia.

### **Artículo 12. Valor de los principios**

La actuación de los titulares y encargados de tratamiento de datos personales y, en general, de todos los que intervengan con relación a datos personales, debe ajustarse a los principios rectores a que se refiere este Título. Esta relación de principios rectores es enunciativa.

Los principios rectores señalados sirven también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia<sup>3</sup>.

<sup>3</sup> Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

## TÍTULO II TRATAMIENTO DE DATOS PERSONALES

### Artículo 13. Alcances sobre el tratamiento de datos personales

- 13.1. El tratamiento de datos personales debe realizarse con pleno respeto de los derechos fundamentales de sus titulares y de los derechos que esta Ley les confiere. Igual regla rige para su utilización por terceros.
- 13.2. Las limitaciones al ejercicio del derecho fundamental a la protección de datos personales solo pueden ser establecidas por ley, respetando su contenido esencial y estar justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos.
- 13.3. Mediante reglamento se dictan medidas especiales para el tratamiento de los datos personales de los niños y de los adolescentes, así como para la protección y garantía de sus derechos. Para el ejercicio de los derechos que esta Ley reconoce, los niños y los adolescentes actúan a través de sus representantes legales, pudiendo el reglamento determinar las excepciones aplicables, de ser el caso, teniendo en cuenta para ello el interés superior del niño y del adolescente.
- 13.4. Las comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos, cuando sean de carácter privado o uso privado, solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez o con autorización de su titular, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen. Los datos personales obtenidos con violación de este precepto carecen de efecto legal.
- 13.5. Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco.
- 13.6. En el caso de datos sensibles, el consentimiento para efectos de

---

#### **Texto anterior a la modificación:**

Artículo 12. Valor de los principios

La actuación de los titulares y encargados de los bancos de datos personales y, en general, de todos los que intervengan con relación a datos personales, debe ajustarse a los principios rectores a que se refiere este Título. Esta relación de principios rectores es enunciativa.

Los principios rectores señalados sirven también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia.

su tratamiento, además, debe efectuarse por escrito. Aun cuando no mediara el consentimiento del titular, el tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público.

- 13.7. El titular de datos personales puede revocar su consentimiento en cualquier momento, observando al efecto los mismos requisitos que con ocasión de su otorgamiento.
- 13.8. El tratamiento de datos personales relativos a la comisión de infracciones penales o administrativas solo puede ser efectuado por las entidades públicas competentes, salvo convenio de encargo de gestión conforme a la Ley N° 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces. Cuando se haya producido la cancelación de los antecedentes penales, judiciales, policiales y administrativos, estos datos no pueden ser suministrados salvo que sean requeridos por el Poder Judicial o el Ministerio Público, conforme a ley.
- 13.9. La comercialización de datos personales contenidos o destinados a ser contenidos en bancos de datos personales se sujeta a los principios previstos en la presente Ley.

#### **Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales**

No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:

1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley N° 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.

5. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.
8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.
9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales.
10. Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.
11. En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir información entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada.

12. Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.
13. Otros que deriven del ejercicio de competencias expresamente establecidas por Ley<sup>4</sup>.

### **Artículo 15. Flujo transfronterizo de datos personales**

El titular y el encargado de tratamiento de datos personales deben realizar el flujo transfronterizo de datos personales solo si el país destinatario mantiene niveles de protección adecuados conforme a la presente Ley.

---

4 Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales

No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:

1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley N° 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
5. Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.
8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.
9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de datos personales.
10. Otros establecidos por ley, o por el reglamento otorgado de conformidad con la presente Ley.

En caso de que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales debe garantizar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto por la presente Ley.

No se aplica lo dispuesto en el segundo párrafo en los siguientes casos:

1. Acuerdos en el marco de tratados internacionales sobre la materia en los cuales la República del Perú sea parte.
2. Cooperación judicial internacional.
3. Cooperación internacional entre organismos de inteligencia para la lucha contra el terrorismo, tráfico ilícito de drogas, lavado de activos, corrupción, trata de personas y otras formas de criminalidad organizada.
4. Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte, incluyendo lo necesario para actividades como la autenticación de usuario, mejora y soporte del servicio, monitoreo de la calidad del servicio, soporte para el mantenimiento y facturación de la cuenta y aquellas actividades que el manejo de la relación contractual requiera.
5. Cuando se trate de transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme a la ley aplicable.
6. Cuando el flujo transfronterizo de datos personales se realice para la protección, prevención, diagnóstico o tratamiento médico o quirúrgico de su titular; o cuando sea necesario para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7. Cuando el titular de los datos personales haya dado su consentimiento previo, informado, expreso e inequívoco.

8. Otros que establezca el reglamento de la presente Ley, con sujeción a lo dispuesto en el artículo 12<sup>5 6</sup>.

### **Artículo 16. Seguridad del tratamiento de datos personales**

Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.

---

5 Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

#### **Texto anterior a la modificación:**

Artículo 15. Flujo transfronterizo de datos personales

El titular y el encargado del banco de datos personales deben realizar el flujo transfronterizo de datos personales solo si el país destinatario mantiene niveles de protección adecuados conforme a la presente Ley.

En caso de que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales debe garantizar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto por la presente Ley.

No se aplica lo dispuesto en el segundo párrafo en los siguientes casos:

1. Acuerdos en el marco de tratados internacionales sobre la materia en los cuales la República del Perú sea parte.
  2. Cooperación judicial internacional.
  3. Cooperación internacional entre organismos de inteligencia para la lucha contra el terrorismo, tráfico ilícito de drogas, lavado de activos, corrupción, trata de personas y otras formas de criminalidad organizada.
  4. Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte, incluyendo lo necesario para actividades como la autenticación de usuario, mejora y soporte del servicio, monitoreo de la calidad del servicio, soporte para el mantenimiento y facturación de la cuenta y aquellas actividades que el manejo de la relación contractual requiera.
  5. Cuando se trate de transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme a la ley aplicable.
  6. Cuando el flujo transfronterizo de datos personales se realice para la protección, prevención, diagnóstico o tratamiento médico o quirúrgico de su titular; o cuando sea necesario para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
  7. Cuando el titular de los datos personales haya dado su consentimiento previo, informado, expreso e inequívoco.
  8. Otros que establezca el reglamento de la presente Ley, con sujeción a lo dispuesto en el artículo 12.
- 6 Fe de Erratas publicado el 12 de enero de 2017.

Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo.

### **Artículo 17. Confidencialidad de datos personales**

El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales.

El obligado puede ser relevado de la obligación de confidencialidad cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública, sin perjuicio del derecho a guardar el secreto profesional.

## **TÍTULO III DERECHOS DEL TITULAR DE DATOS PERSONALES**

**Artículo 18.** Derecho de información del titular de datos personales El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.

Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables.

En el caso que el titular del banco de datos establezca vinculación con un encargado de tratamiento de manera posterior al consentimiento,

el accionar del encargado queda bajo responsabilidad del Titular del Banco de Datos, debiendo establecer un mecanismo de información personalizado para el titular de los datos personales sobre dicho nuevo encargado de tratamiento.

Si con posterioridad al consentimiento se produce la transferencia de datos personales por fusión, adquisición de cartera, o supuestos similares, el nuevo titular del banco de datos debe establecer un mecanismo de información eficaz para el titular de los datos personales sobre dicho nuevo encargado de tratamiento<sup>7</sup>.

### **Artículo 19. Derecho de acceso del titular de datos personales**

El titular de datos personales tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.

### **Artículo 20. Derecho de actualización, inclusión, rectificación y supresión**

El titular de datos personales tiene derecho a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.

<sup>7</sup> Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

#### **Texto anterior a la modificación:**

Artículo 18. Derecho de información del titular de datos personales

El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.

Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables.

Si sus datos personales hubieran sido transferidos previamente, el encargado de tratamiento de datos personales debe comunicar la actualización, inclusión, rectificación o supresión a quienes se hayan transferido, en el caso que se mantenga el tratamiento por este último, quien debe también proceder a la actualización, inclusión, rectificación o supresión, según corresponda.

Durante el proceso de actualización, inclusión, rectificación o supresión de datos personales, el encargado de tratamiento de datos personales dispone su bloqueo, quedando impedido de permitir que terceros accedan a ellos. Dicho bloqueo no es aplicable a las entidades públicas que requieren de tal información para el adecuado ejercicio de sus competencias, según ley, las que deben informar que se encuentra en trámite cualquiera de los mencionados procesos.

La supresión de datos personales contenidos en bancos de datos personales de administración pública se sujeta a lo dispuesto en el artículo 21 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, o la que haga sus veces<sup>8</sup>.

---

8 Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

Artículo 20. Derecho de actualización, inclusión, rectificación y supresión

El titular de datos personales tiene derecho a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.

Si sus datos personales hubieran sido transferidos previamente, el encargado del banco de datos personales debe comunicar la actualización, inclusión, rectificación o supresión a quienes se hayan transferido, en el caso que se mantenga el tratamiento por este último, quien debe también proceder a la actualización, inclusión, rectificación o supresión, según corresponda.

Durante el proceso de actualización, inclusión, rectificación o supresión de datos personales, el encargado del banco de datos personales dispone su bloqueo, quedando impedido de permitir que terceros accedan a ellos. Dicho bloqueo no es aplicable a las entidades públicas que requieren de tal información para el adecuado ejercicio de sus competencias, según ley, las que deben informar que se encuentra en trámite cualquiera de los mencionados procesos.

La supresión de datos personales contenidos en bancos de datos personales de administración pública se sujeta a lo dispuesto en el artículo 21 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, o la que haga sus veces.

### **Artículo 21. Derecho a impedir el suministro**

El titular de datos personales tiene derecho a impedir que estos sean suministrados, especialmente cuando ello afecte sus derechos fundamentales. El derecho a impedir el suministro no aplica para la relación entre el titular del banco de datos personales y el encargado de tratamiento de datos personales para los efectos del tratamiento de estos<sup>9</sup>.

### **Artículo 22. Derecho de oposición**

Siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En caso de oposición justificada, el titular o el encargado de tratamiento de datos personales, según corresponda, debe proceder a su supresión, conforme a ley<sup>10</sup>.

### **Artículo 23. Derecho al tratamiento objetivo**

El titular de datos personales tiene derecho a no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, sustentada únicamente en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad o conducta, salvo que ello ocurra en el marco de la negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines de incorporación a una entidad pública, de acuerdo a ley, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés.

9 Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

Artículo 21. Derecho a impedir el suministro

El titular de datos personales tiene derecho a impedir que estos sean suministrados, especialmente cuando ello afecte sus derechos fundamentales. El derecho a impedir el suministro no aplica para la relación entre el titular del banco de datos personales y el encargado del banco de datos personales para los efectos del tratamiento de estos.

10 Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

Artículo 22. Derecho de oposición

Siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En caso de oposición justificada, el titular o el encargado del banco de datos personales, según corresponda, debe proceder a su supresión, conforme a ley.

### **Artículo 24. Derecho a la tutela**

En caso de que el titular o el encargado del banco de datos personales deniegue al titular de datos personales, total o parcialmente, el ejercicio de los derechos establecidos en esta Ley, este puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de hábeas data.

El procedimiento a seguir ante la Autoridad Nacional de Protección de Datos Personales se sujeta a lo dispuesto en los artículos 219 y siguientes de la Ley N° 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces.

La resolución de la Autoridad Nacional de Protección de Datos Personales agota la vía administrativa y habilita la imposición de las sanciones administrativas previstas en el artículo 39. El reglamento determina las instancias correspondientes.

Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa.

### **Artículo 25. Derecho a ser indemnizado**

El titular de datos personales que sea afectado a consecuencia del incumplimiento de la presente Ley por el titular o por el encargado de tratamiento de datos personales o por terceros, tiene derecho a obtener la indemnización correspondiente, conforme a ley<sup>11</sup>.

### **Artículo 26. Contraprestación**

La contraprestación que debe abonar el titular de datos personales por el ejercicio de los derechos contemplados en los artículos 19, 20, 21, 22 y 23 ante los bancos de datos personales de administración pública se sujeta a las disposiciones previstas en la Ley N° 27444, Ley del Procedimiento Administrativo General.

Ante los bancos de datos personales de administración privada, el ejercicio de los derechos mencionados se sujeta a lo dispuesto por las normas especiales sobre la materia.

<sup>11</sup> Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

**Artículo 25. Derecho a ser indemnizado**

El titular de datos personales que sea afectado a consecuencia del incumplimiento de la presente Ley por el titular o por el encargado del banco de datos personales o por terceros, tiene derecho a obtener la indemnización correspondiente, conforme a ley.

### **Artículo 27. Limitaciones**

Los titulares y los encargados de tratamiento de datos personales de administración pública pueden denegar el ejercicio de los derechos de acceso, supresión y oposición por razones fundadas en la protección de derechos e intereses de terceros o cuando ello pueda obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, a las investigaciones penales sobre la comisión de faltas o delitos, al desarrollo de funciones de control de la salud y del medio ambiente, a la verificación de infracciones administrativas, o cuando así lo disponga la ley<sup>12</sup>.

## **TÍTULO IV OBLIGACIONES DEL TITULAR Y DEL ENCARGADO DE TRATAMIENTO DE DATOS PERSONALES<sup>13</sup>**

### **Artículo 28. Obligaciones**

El titular y el encargado de tratamiento de datos personales, según sea el caso, tienen las siguientes obligaciones:

1. Efectuar el tratamiento de datos personales, solo previo consentimiento informado, expreso e inequívoco del titular de los datos personales, salvo ley autoritativa, con excepción de los supuestos consignados en el artículo 14 de la presente Ley.

---

12 Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

Artículo 27. Limitaciones

Los titulares y encargados de los bancos de datos personales de administración pública pueden denegar el ejercicio de los derechos de acceso, supresión y oposición por razones fundadas en la protección de derechos e intereses de terceros o cuando ello pueda obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, a las investigaciones penales sobre la comisión de faltas o delitos, al desarrollo de funciones de control de la salud y del medio ambiente, a la verificación de infracciones administrativas, o cuando así lo disponga la ley.

13 Denominación modificada por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

TÍTULO IV

OBLIGACIONES DEL TITULAR Y DEL ENCARGADO DEL BANCO DE DATOS PERSONALES

2. No recopilar datos personales por medios fraudulentos, desleales o ilícitos.
3. Recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido.
4. No utilizar los datos personales objeto de tratamiento para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación.
5. Almacenar los datos personales de manera que se posibilite el ejercicio de los derechos de su titular.
6. Suprimir y sustituir o, en su caso, completar los datos personales objeto de tratamiento cuando tenga conocimiento de su carácter inexacto o incompleto, sin perjuicio de los derechos del titular al respecto.
7. Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación.
8. Proporcionar a la Autoridad Nacional de Protección de Datos Personales la información relativa al tratamiento de datos personales que esta le requiera y permitirle el acceso a los bancos de datos personales que administra, para el ejercicio de sus funciones, en el marco de un procedimiento administrativo en curso solicitado por la parte afectada.
9. Otras establecidas en esta Ley y en su reglamento<sup>14</sup>.

---

14 Artículo modificado por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

Artículo 28. Obligaciones

El titular y el encargado del banco de datos personales, según sea el caso, tienen las siguientes obligaciones:

1. Efectuar el tratamiento de datos personales, solo previo consentimiento informado, expreso e inequívoco del titular de los datos personales, salvo ley autoritativa, con excepción de los supuestos consignados en el artículo 14 de la presente Ley.
2. No recopilar datos personales por medios fraudulentos, desleales o ilícitos.
3. Recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido.
4. No utilizar los datos personales objeto de tratamiento para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación.

## **TÍTULO V**

### **BANCOS DE DATOS PERSONALES**

#### **Artículo 29. Creación, modificación o cancelación de bancos de datos personales**

La creación, modificación o cancelación de bancos de datos personales de administración pública y de administración privada se sujetan a lo que establezca el reglamento, salvo la existencia de disposiciones especiales contenidas en otras leyes. En todo caso, se garantiza la publicidad sobre su existencia, finalidad, identidad y el domicilio de su titular y, de ser el caso, de su encargado.

#### **Artículo 30. Prestación de servicios de tratamiento de datos personales**

Cuando, por cuenta de terceros, se presten servicios de tratamiento de datos personales, estos no pueden aplicarse o utilizarse con un fin distinto al que figura en el contrato o convenio celebrado ni ser transferidos a otras personas, ni aun para su conservación.

Una vez ejecutada la prestación materia del contrato o del convenio, según el caso, los datos personales tratados deben ser suprimidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se pueden conservar con las debidas condiciones de seguridad, hasta por el plazo que determine el reglamento de esta Ley.

#### **Artículo 31. Códigos de conducta**

31.1 Las entidades representativas de los titulares o encargados de tratamiento de datos personales administración privada pueden elaborar códigos de conducta que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función

- 
5. Almacenar los datos personales de manera que se posibilite el ejercicio de los derechos de su titular.
  6. Suprimir y sustituir o, en su caso, completar los datos personales objeto de tratamiento cuando tenga conocimiento de su carácter inexacto o incompleto, sin perjuicio de los derechos del titular al respecto.
  7. Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación.
  8. Proporcionar a la Autoridad Nacional de Protección de Datos Personales la información relativa al tratamiento de datos personales que esta le requiera y permitirle el acceso a los bancos de datos personales que administra, para el ejercicio de sus funciones, en el marco de un procedimiento administrativo en curso solicitado por la parte afectada.
  9. Otras establecidas en esta Ley y en su reglamento.

de los principios rectores establecidos en esta Ley<sup>15</sup>.

## **TÍTULO VI**

### **AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES**

#### **Artículo 32. Órgano competente y régimen jurídico**

El Ministerio de Justicia, a través de la Dirección Nacional de Justicia, es la Autoridad Nacional de Protección de Datos Personales. Para el adecuado desempeño de sus funciones, puede crear oficinas en todo el país.

La Autoridad Nacional de Protección de Datos Personales se rige por lo dispuesto en esta Ley, en su reglamento y en los artículos pertinentes del Reglamento de Organización y Funciones del Ministerio de Justicia.

Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la presente Ley y de su reglamento. Para tal efecto, goza de potestad sancionadora, de conformidad con la Ley N° 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces, así como de potestad coactiva, de conformidad con la Ley N° 26979, Ley de Procedimiento de Ejecución Coactiva, o la que haga sus veces.

La Autoridad Nacional de Protección de Datos Personales debe presentar periódicamente un informe sobre sus actividades al Ministro de Justicia.

Para el cumplimiento de sus funciones, la Autoridad Nacional de Protección de Datos Personales cuenta con el apoyo y asesoramiento técnico de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros, o la que haga sus veces.

#### **Artículo 33. Funciones de la Autoridad Nacional de Protección de Datos Personales**

La Autoridad Nacional de Protección de Datos Personales ejerce las

<sup>15</sup> Artículo modificado por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

Artículo 31. Códigos de conducta

Las entidades representativas de los titulares o encargados de bancos de datos personales de administración privada pueden elaborar códigos de conducta que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios rectores establecidos en esta Ley.

funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:

1. Representar al país ante las instancias internacionales en materia de protección de datos personales.
2. Cooperar con las autoridades extranjeras de protección de datos personales para el cumplimiento de sus competencias y generar mecanismos de cooperación bilateral y multilateral para asistirse entre sí y prestarse debido auxilio mutuo cuando se requiera.
3. Administrar y mantener actualizado el Registro Nacional de Protección de Datos Personales.
4. Publicitar, a través del portal institucional, la relación actualizada de bancos de datos personales de administración pública y privada.
5. Promover campañas de difusión y promoción sobre la protección de datos personales.
6. Promover y fortalecer una cultura de protección de los datos personales de los niños y de los adolescentes.
7. Coordinar la inclusión de información sobre la importancia de la vida privada y de la protección de datos personales en los planes de estudios de todos los niveles educativos y fomentar, asimismo, la capacitación de los docentes en estos temas.
8. Supervisar el cumplimiento de las exigencias previstas en esta Ley, para el flujo transfronterizo de datos personales.
9. Emitir autorizaciones, cuando corresponda, conforme al reglamento de esta Ley.
10. Absolver consultas sobre protección de datos personales y el sentido de las normas vigentes en la materia, particularmente sobre las que ella hubiera emitido.
11. Emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la que es vinculante.
12. Emitir las directivas que correspondan para la mejor aplicación de lo previsto en esta Ley y en su reglamento, especialmente en materia de

seguridad de los bancos de datos personales, así como supervisar su cumplimiento, en coordinación con los sectores involucrados.

13. Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales.
14. Celebrar convenios de cooperación interinstitucional o internacional con la finalidad de velar por los derechos de las personas en materia de protección de datos personales que son tratados dentro y fuera del territorio nacional.
15. Atender solicitudes de interés particular del administrado o general de la colectividad, así como solicitudes de información.
16. Conocer, instruir y resolver las reclamaciones formuladas por los titulares de datos personales por la vulneración de los derechos que les conciernen y dictar las medidas cautelares o correctivas que establezca el reglamento.
17. Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores.
18. En el marco de un procedimiento administrativo en curso, solicitado por la parte afectada, obtener de los titulares de los bancos de datos personales la información que estime necesaria para el cumplimiento de las normas sobre protección de datos personales y el desempeño de sus funciones.
19. Supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales a las disposiciones técnicas que ella emita y, en caso de contravención, disponer las acciones que correspondan conforme a ley.
20. Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento.
21. Las demás funciones que le asignen esta Ley y su reglamento.

#### **Artículo 34. Registro Nacional de Protección de Datos Personales**

Créase el Registro Nacional de Protección de Datos Personales como registro de carácter administrativo a cargo de la Autoridad Nacional de

Protección de Datos Personales, con la finalidad de inscribir en forma diferenciada, a nivel nacional, lo siguiente:

1. Los bancos de datos personales de administración pública o privada, así como los datos relativos a estos que sean necesarios para el ejercicio de los derechos que corresponden a los titulares de datos personales, conforme a lo dispuesto en esta Ley y en su reglamento.

El ejercicio de esta función no posibilita el conocimiento del contenido de los bancos de datos personales por parte de la Autoridad Nacional de Protección de Datos Personales, salvo procedimiento administrativo en curso.

2. Las comunicaciones de flujo transfronterizo de datos personales.
3. Las sanciones, medidas cautelares o correctivas impuestas por la Autoridad Nacional de Protección de Datos Personales conforme a esta Ley y a su reglamento.

Cualquier persona puede consultar en el Registro Nacional de Protección de Datos Personales la existencia de bancos de datos personales, sus finalidades, así como la identidad y domicilio de sus titulares y, de ser el caso, de sus encargados<sup>16</sup>.

16 Artículo modificado por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

Artículo 34. Registro Nacional de Protección de Datos Personales

Créase el Registro Nacional de Protección de Datos Personales como registro de carácter administrativo a cargo de la Autoridad Nacional de Protección de Datos Personales, con la finalidad de inscribir en forma diferenciada, a nivel nacional, lo siguiente:

1. Los bancos de datos personales de administración pública o privada, así como los datos relativos a estos que sean necesarios para el ejercicio de los derechos que corresponden a los titulares de datos personales, conforme a lo dispuesto en esta Ley y en su reglamento. El ejercicio de esta función no posibilita el conocimiento del contenido de los bancos de datos personales por parte de la Autoridad Nacional de Protección de Datos Personales, salvo procedimiento administrativo en curso.
2. Las autorizaciones emitidas conforme al reglamento de la presente Ley.
3. Las sanciones, medidas cautelares o correctivas impuestas por la Autoridad Nacional de Protección de Datos Personales conforme a esta Ley y a su reglamento.
4. Los códigos de conducta de las entidades representativas de los titulares o encargados de bancos de datos personales de administración privada.
5. Otros actos materia de inscripción conforme al reglamento.

Cualquier persona puede consultar en el Registro Nacional de Protección de Datos Personales la existencia de bancos de datos personales, sus finalidades, así como la identidad y domicilio de sus titulares y, de ser el caso, de sus encargados.

### **Artículo 35. Confidencialidad**

El personal de la Autoridad Nacional de Protección de Datos Personales está sujeto a la obligación de guardar confidencialidad sobre los datos personales que conozca con motivo de sus funciones. Esta obligación subsiste aun después de finalizada toda relación con dicha autoridad nacional, bajo responsabilidad.

### **Artículo 36. Recursos de la Autoridad Nacional de Protección de Datos Personales**

Son recursos de la Autoridad Nacional de Protección de Datos Personales los siguientes:

1. Las tasas por concepto de derecho de trámite de los procedimientos administrativos y servicios de su competencia.
2. Los montos que recaude por concepto de multas.
3. Los recursos provenientes de la cooperación técnica internacional no reembolsable.
4. Los legados y donaciones que reciba.
5. Los recursos que se le transfieran conforme a ley.

Los recursos de la Autoridad Nacional de Protección de Datos Personales son destinados a financiar los gastos necesarios para el desarrollo de sus operaciones y para su funcionamiento.

## **TÍTULO VII INFRACCIONES Y SANCIONES ADMINISTRATIVAS**

### **Artículo 37. Procedimiento sancionador**

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 o en su reglamento, sin perjuicio del procedimiento seguido en el marco de lo dispuesto en el artículo 24.

Las resoluciones de la Autoridad Nacional de Protección de Datos Personales agotan la vía administrativa.

Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa.

### **Artículo 38.- Tipificación de infracciones**

Las infracciones se clasifican en leves, graves y muy graves, las cuales son tipificadas vía reglamentaria, de acuerdo a lo establecido en el numeral 4) del artículo 230 de la Ley N° 27444, Ley del Procedimiento Administrativo General, mediante Decreto Supremo con el voto aprobatorio del Consejo de Ministros.

Sin perjuicio de las sanciones que en el marco de su competencia imponga la autoridad competente, esta puede ordenar la implementación de una o más medidas correctivas, con el objetivo de corregir o revertir los efectos que la conducta infractora hubiere ocasionado o evitar que ésta se produzca nuevamente.

Los administrados son responsables objetivamente por el incumplimiento de obligaciones derivadas de las normas sobre protección de datos personales<sup>17</sup>.

---

17 Artículo modificado por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 07 de enero de 2017, la misma que entró en vigencia al día siguiente de la publicación del Decreto Supremo que aprueba su Reglamento y la modificación del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

**Texto anterior a la modificación:**

**Artículo 38. Infracciones**

Constituye infracción sancionable toda acción u omisión que contravenga o incumpla alguna de las disposiciones contenidas en esta Ley o en su reglamento.

Las infracciones se califican como leves, graves y muy graves.

1. Son infracciones leves:

- a. Dar tratamiento a datos personales sin recabar el consentimiento de sus titulares, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley.
- b. No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales reconocidos en el título III, cuando legalmente proceda.
- c. Obstruir el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales.

2. Son infracciones graves:

- a. Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento.
- b. Incumplir la obligación de confidencialidad establecida en el artículo 17.
- c. No atender, impedir u obstaculizar, en forma sistemática, el ejercicio de los derechos del titular de datos personales reconocidos en el título III, cuando legalmente proceda.
- d. Obstruir, en forma sistemática, el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales.
- e. No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales.

3. Son infracciones muy graves:

- a. Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
- b. Crear, modificar, cancelar o mantener bancos de datos personales sin cumplir con lo establecido por la presente Ley o su reglamento.
- c. Suministrar documentos o información falsa o incompleta a la Autoridad Nacional de Protección de Datos Personales.

### **Artículo 39. Sanciones administrativas**

En caso de violación de las normas de esta Ley o de su reglamento, la Autoridad Nacional de Protección de Datos Personales puede aplicar las siguientes multas:

1. Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).
2. Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).
3. Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT).

En ningún caso, la multa impuesta puede exceder del diez por ciento de los ingresos brutos anuales que hubiera percibido el presunto infractor durante el ejercicio anterior.

La Autoridad Nacional de Protección de Datos Personales determina la infracción cometida y el monto de la multa imponible mediante resolución debidamente motivada. Para la graduación del monto de las multas, se toman en cuenta los criterios establecidos en el artículo 230, numeral 3), de la Ley N° 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces.

La imposición de la multa se efectúa sin perjuicio de las sanciones disciplinarias sobre el personal de las entidades públicas en los casos de bancos de datos personales de administración pública, así como de la indemnización por daños y perjuicios y de las sanciones penales a que hubiera lugar.

### **Artículo 40. Multas coercitivas**

En aplicación de lo dispuesto en el artículo 199 de la Ley N° 27444, Ley

- 
- d. No cesar en el tratamiento ilícito de datos personales, cuando existiese un previo requerimiento de la Autoridad Nacional de Protección de Datos Personales para ello.
  - e. 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.

La calificación, la graduación del monto de las multas, el procedimiento para su aplicación y otras tipificaciones se efectúan en el reglamento de la presente Ley.

del Procedimiento Administrativo General, o la que haga sus veces, la Autoridad Nacional de Protección de Datos Personales puede imponer multas coercitivas por un monto que no supere las diez unidades impositivas tributarias (UIT), frente al incumplimiento de las obligaciones accesorias a la sanción, impuestas en el procedimiento sancionador. Las multas coercitivas se imponen una vez vencido el plazo de cumplimiento.

La imposición de las multas coercitivas no impide el ejercicio de otro medio de ejecución forzosa, conforme a lo dispuesto en el artículo 196 de la Ley N° 27444, Ley del Procedimiento Administrativo General.

El reglamento de la presente Ley regula lo concerniente a la aplicación de las multas coercitivas.

## **DISPOSICIONES COMPLEMENTARIAS FINALES**

### **PRIMERA. Reglamento de la Ley**

Para la elaboración del proyecto de reglamento, se constituye una comisión multisectorial, la que es presidida por la Autoridad Nacional de Protección de Datos Personales.

El proyecto de reglamento es elaborado en un plazo máximo de ciento veinte días hábiles, a partir de la instalación de la comisión multisectorial, lo que debe ocurrir en un plazo no mayor de quince días hábiles, contado a partir del día siguiente de la publicación de la presente Ley.

### **SEGUNDA. Directiva de seguridad**

La Autoridad Nacional de Protección de Datos Personales elabora la directiva de seguridad de la información administrada por los bancos de datos personales en un plazo no mayor de ciento veinte días hábiles, contado a partir del día siguiente de la publicación de la presente Ley.

En tanto se apruebe y rija la referida directiva, se mantienen vigentes las disposiciones sectoriales sobre la materia.

### **TERCERA. Adecuación de documentos de gestión y del Texto Único de Procedimientos Administrativos del Ministerio de Justicia**

Estando a la creación de la Autoridad Nacional de Protección de Datos Personales, en un plazo máximo de ciento veinte días hábiles, contado a partir del día siguiente de la publicación de la presente Ley, el Ministerio de Justicia elabora las modificaciones pertinentes en sus documentos de gestión y en su Texto Único de Procedimientos Administrativos.

#### **CUARTA. Adecuación normativa**

Dentro del plazo de sesenta días hábiles, el Poder Ejecutivo remite al Congreso de la República un proyecto de ley que contenga las modificaciones necesarias a las leyes existentes a efectos de su adecuación a la presente Ley.

Para las normas de rango inferior, las entidades públicas competentes revisan la normativa correspondiente y elaboran las propuestas necesarias para su adecuación a lo dispuesto en esta Ley.

En ambos casos se requiere la opinión técnica favorable previa de la Autoridad Nacional de Protección de Datos Personales, de conformidad con el artículo 33 numeral 11.

#### **QUINTA. Bancos de datos personales preexistentes**

Los bancos de datos personales creados con anterioridad a la presente Ley y sus respectivos reglamentos deben adecuarse a esta norma dentro del plazo que establezca el reglamento. Sin perjuicio de ello, sus titulares deben declararlos ante la Autoridad Nacional de Protección de Datos Personales, con sujeción a lo dispuesto en el artículo 29.

#### **SEXTA. Hábeas data**

Las normas establecidas en el Código Procesal Constitucional sobre el proceso de hábeas data se aplican en el ámbito constitucional, independientemente del ámbito administrativo materia de la presente Ley. El procedimiento administrativo establecido en la presente Ley no constituye vía previa para el ejercicio del derecho vía proceso constitucional.

#### **SÉTIMA. Competencias del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi)**

La Autoridad Nacional de Protección de Datos Personales es competente para salvaguardar los derechos de los titulares de la información administrada por las Centrales Privadas de Información de Riesgos (Cepirs) o similares conforme a los términos establecidos en la presente Ley.

Sin perjuicio de ello, en materia de infracción a los derechos de los consumidores en general mediante la prestación de los servicios e información brindados por las Cepirs o similares, en el marco de las relaciones de consumo, son aplicables las normas sobre protección al consumidor, siendo el ente competente de manera exclusiva y excluyente para la supervisión de su cumplimiento la Comisión de Protección al Consumidor del Instituto Nacional de Defensa de la Competencia y de la

Protección de la Propiedad Intelectual (Indecopi), la que debe velar por la idoneidad de los bienes y servicios en función de la información brindada a los consumidores.

### **OCTAVA. Información sensible**

Para los efectos de lo dispuesto en la Ley N° 27489, Ley que Regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información, se entiende por información sensible la definida como dato sensible por la presente Ley.

Igualmente, precísase que la información confidencial a que se refiere el numeral 5) del artículo 17 del Texto Único Ordenado de la Ley N° 28706<sup>18</sup>, Ley de Transparencia y Acceso a la Información Pública, constituye dato sensible conforme a los alcances de esta Ley<sup>19</sup>.

### **NOVENA. Inafectación de facultades de la administración tributaria**

Lo dispuesto en la presente Ley no se debe interpretar en detrimento de las facultades de la administración tributaria respecto de la información que obre y requiera para sus registros, o para el cumplimiento de sus funciones.

### **DÉCIMA. Financiamiento**

La realización de las acciones necesarias para la aplicación de la presente Ley se ejecuta con cargo al presupuesto institucional del pliego Ministerio de Justicia y de los recursos a los que hace referencia el artículo 36, sin demandar recursos adicionales al Tesoro Público.

### **DUODÉCIMA. Vigencia de la Ley**

La presente Ley entra en vigencia conforme a lo siguiente:

1. Las disposiciones previstas en el Título II, en el primer párrafo del artículo 32 y en las primera, segunda, tercera, cuarta, novena y décima disposiciones complementarias finales rigen a partir del día siguiente de la publicación de esta Ley.
2. Las demás disposiciones rigen en el plazo de treinta días hábiles, contado a partir de la publicación del reglamento de la presente Ley.

18 En la presente edición de Normas Legales del Diario Oficial "El Peruano", dice: "Ley 28706 debiendo decir: "Ley 27806".

19 Confrontar con el Artículo 2 del Decreto Supremo N° 021-2019-JUS, publicado el 11 de diciembre de 2019.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los veintiún días del mes de junio de dos mil once.

CÉSAR ZUMAETA FLORES  
Presidente del Congreso de la República

ALDA LAZO RÍOS DE HORNUNG  
Segunda Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los dos días del mes de julio del año dos mil once.

ALAN GARCÍA PÉREZ  
Presidente Constitucional de la República

ROSARIO DEL PILAR FERNÁNDEZ FIGUEROA  
Presidenta del Consejo de Ministros y Ministra de Justicia

**Decreto Supremo que aprueba el Reglamento de la  
Ley N° 29733, Ley de Protección de Datos Personales  
DECRETO SUPREMO N° 016-2024-JUS<sup>20</sup>**

**(SEPARATA ESPECIAL)**

LA PRESIDENTA DE LA REPÚBLICA

CONSIDERANDO:

Que, el numeral 6 del artículo 2 de la Constitución Política del Perú señala que toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar;

Que, el artículo 1 de la Ley N° 29733, Ley de Protección de Datos Personales, señala que dicha Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el numeral 6 del artículo 2 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen;

Que, el artículo 32 de la precitada Ley, dispone que el Ministerio de Justicia y Derechos Humanos ejerce la Autoridad Nacional de Protección de Datos Personales;

Que, mediante el Decreto Supremo N° 003-2013-JUS se aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, el cual en su artículo 1 señala que tiene como objeto desarrollar la mencionada Ley, a fin de garantizar el derecho fundamental a la protección de datos personales, regulando un adecuado tratamiento, tanto por las entidades públicas, como por las instituciones pertenecientes al sector privado;

Que, el Decreto Legislativo N° 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, Fortalece el Régimen de Protección de Datos Personales y la Regulación de la Gestión de Intereses, a través de su tercera disposición complementaria modificatoria reformó algunas disposiciones de la Ley N° 29733, Ley de Protección de Datos Personales;

---

<sup>20</sup> Esta Exposición de Motivos no ha sido publicada en el diario oficial "El Peruano", ha sido enviada por la Secretaría General del Ministerio de Justicia y Derechos Humanos, mediante Memorando N° 1007-2024-JUS/SG de fecha 12 de diciembre de 2024.

Que, el literal a) del párrafo 4.2 del artículo 4 del Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, establece que uno de los ámbitos de la confianza digital en el entorno digital es la protección de datos personales y transparencia, siendo el Ministerio de Justicia y Derechos Humanos, quien ejerce las Autoridades Nacionales de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, y en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de transparencia y protección de datos personales;

Que, mediante Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, en sus párrafos 5.3 y 5.10 del artículo 5, se establecen como principios rectores del marco de gobernanza del gobierno digital, el principio de privacidad desde el diseño, por el cual, en el diseño y configuración de servicios digitales se adoptan las medidas preventivas de tipo tecnológico, organizacional, humano y procedimental; así como, el principio de nivel de protección adecuado para los datos personales, por el cual, el tratamiento de los datos personales debe realizarse conforme a lo establecido en la Ley de Protección de Datos Personales y su Reglamento;

Que, debido a los cambios en el marco normativo y los desafíos contemporáneos que representan la irrupción de nuevas tecnologías digitales, resulta necesario aprobar un nuevo Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales que permita que el país cuente con un marco normativo moderno y sólido que garantice una adecuada tutela de los derechos de los ciudadanos frente a los riesgos generados para los datos personales por el uso de las nuevas tecnologías digitales;

Que, mediante Resolución Ministerial N° 0270-2023-JUS, publicada el 26 de agosto de 2023 en el Diario Oficial El Peruano, se dispuso la publicación del Proyecto de Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales y la Exposición de Motivos que lo sustenta, por un plazo de treinta (30) días calendario, a fin de recibir sugerencias, comentarios o recomendaciones de las entidades públicas, instituciones privadas, organizaciones de la sociedad civil, así como de las personas naturales en general.

Que, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales recibió, procesó y sistematizó las sugerencias, comentarios y/o recomendaciones presentadas por ciudadanos y diversas instituciones, tanto del ámbito privado como público;

De conformidad con lo dispuesto en el numeral 6) del artículo 2 y el numeral 8 del artículo 118 de la Constitución Política del Perú; la Ley N° 29733, Ley de Protección de Datos Personales; la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento; la Ley N° 29809, Ley de Organización y Funciones del Ministerio de Justicia y Derechos Humanos; el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N° 013-2017-JUS; y el Reglamento de la Ley Marco para la producción y Sistematización Legislativa, aprobado por Decreto Supremo N° 007-2022-JUS;

Con el voto aprobatorio del Consejo de Ministros;

DECRETA:

### **Artículo 1. Aprobación**

Se aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, cuyo texto está compuesto de un (1) Título Preliminar, tres (3) Títulos, ciento treinta y cinco (135) artículos, seis (6) Disposiciones Complementarias Finales y dos (2) Disposiciones Complementarias Transitorias, que forman parte integrante del presente Decreto Supremo.

### **Artículo 2. Publicación**

El presente Decreto Supremo y el Reglamento aprobado en el artículo 1 son publicados en la Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano ([www.gob.pe](http://www.gob.pe)) y en la sede digital del Ministerio de Justicia y Derechos Humanos y de la Presidencia del Consejo de Ministros, el mismo día de su publicación de la presente norma en el Diario Oficial El Peruano.

### **Artículo 3. Financiamiento**

La implementación de lo dispuesto en el presente Decreto Supremo y el Reglamento aprobado en el artículo 1 se sujeta a la disponibilidad presupuestal de los pliegos involucrados, sin demandar recursos adicionales al Tesoro Público.

### **Artículo 4. Refrendo**

El presente Decreto Supremo es refrendado por el Ministro de Justicia y Derechos Humanos.

## **DISPOSICIÓN COMPLEMENTARIA DEROGATORIA**

### **Única. Derogación**

Se deroga el Decreto Supremo N° 003-2013-JUS que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.

Dado en la Casa de Gobierno, en Lima, a los veintinueve días del mes de noviembre del año dos mil veinticuatro.

DINA ERCILIA BOLUARTE ZEGARRA  
Presidenta de la República

EDUARDO MELCHOR ARANA YSA  
Ministro de Justicia y Derechos Humanos

## REGLAMENTO DE LA LEY N° 29733, LEY DE PROTECCIÓN DE DATOS PERSONALES

### TÍTULO PRELIMINAR

#### **Artículo I. Objeto**

El presente Reglamento tiene por objeto establecer disposiciones para la adecuada aplicación de la Ley N° 29733, Ley de Protección de Datos Personales, en adelante la Ley, a fin de garantizar el derecho fundamental a la protección de datos personales, regulando un adecuado tratamiento por parte de las personas naturales, entidades públicas y las instituciones pertenecientes al sector privado, particularmente, en el entorno digital.

#### **Artículo II. Finalidad**

El presente Reglamento tiene por finalidad garantizar una adecuada tutela del derecho fundamental a la protección de datos personales establecido en el numeral 6 del artículo 2 de la Constitución Política del Perú y la Ley N° 29733, Ley de Protección de Datos Personales, frente a los riesgos que pueden generar el uso de las nuevas tecnologías digitales.

#### **Artículo III. Definiciones**

Para la aplicación del presente Reglamento, sin perjuicio de las definiciones contenidas en la Ley, complementariamente, se debe entender las siguientes definiciones:

- 1. Banco de datos personales:** Es el conjunto de datos de personas naturales computarizado o no, y estructurado conforme a criterios específicos, que permita acceder sin esfuerzos desproporcionados a los datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.
- 2. Bloqueo:** Es la medida que consiste en la identificación y reserva de los datos personales adoptando medidas técnicas y organizativas para impedir su tratamiento, incluyendo su visualización, durante el periodo en que se esté procesando alguna solicitud de actualización, inclusión, rectificación o supresión, en concordancia con lo que dispone el tercer párrafo del artículo 20 de la Ley.

Se dispone también como paso previo a la cancelación por el tiempo necesario para determinar posibles responsabilidades en relación a los tratamientos durante el plazo de prescripción legal o prevista contractualmente.

- 3. Cancelación:** Es la acción o medida que en la Ley se describe como supresión, cuando se refiere a datos personales, que consiste en eliminar o suprimir los datos personales.
- 4. Datos personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales de las personas naturales que las identifica o las hace identificables. Se considera identificable cuando se puede verificar la identidad de la persona de manera directa o indirectamente a partir de la combinación de datos a través de medios que puedan ser razonablemente utilizados.
- 5. Datos personales relacionados con la salud:** Es aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo la información que se derive de un acto médico, el grado de discapacidad y su información genética.
- 6. Datos sensibles:** Es aquella información relativa a datos genéticos o biométricos de la persona natural, datos neuronales, datos 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 afiliación sindical, salud física o mental u otras análogas que afecten su intimidad.
- 7. Desindexación:** Es el proceso mediante el cual una dirección URL o contenido específico de un sitio web es eliminado o excluido de los resultados de motores de búsqueda. Este procedimiento, dependiendo de la situación y las circunstancias específicas, puede ser efectuado por el propietario del sitio web o por el motor de búsqueda.
- 8. Días:** Días hábiles.
- 9. Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales:** Es el órgano encargado de ejercer la Autoridad Nacional de Protección de Datos Personales a que se refiere el artículo 32 de la Ley, pudiendo usarse indistintamente cualquiera de dichas denominaciones en el presente Reglamento.
- 10. Encargado de tratamiento de datos personales:** Es la persona natural, persona jurídica de derecho privado o entidad pública que realiza tratamiento de datos por cuenta u orden del responsable de tratamiento o titular del banco de datos personales.

- 11. Elaboración de perfiles:** Es la forma de tratamiento automatizado de datos personales que permite evaluar aspectos de una persona natural, de manera específica y continua, para analizar o predecir aspectos relativos a su rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamientos o hábitos, ubicación o movimientos.
- 12. Emisor o exportador de datos personales:** Es el titular del banco de datos personales o aquel que resulte responsable del tratamiento de dichos datos, situado dentro del territorio nacional y que realiza una transferencia de datos personales a otro país, conforme a lo dispuesto en el presente Reglamento.
- 13. Evaluación de impacto relativo a la protección de datos personales:** Es el mecanismo de responsabilidad proactiva que consiste en que el titular del banco de datos personales o responsable del tratamiento de datos realice, de forma previa al tratamiento de los mismos, un análisis o evaluación del impacto o riesgos que implica el tratamiento de esos datos.
- 14. Fines de tránsito:** Implica que los medios no son usados para la finalidad específica de realizar el tratamiento de datos personales, tales como procesamiento, almacenamiento, descarga, visualización y/o similares, sino exclusivamente para hacer pasar datos personales de un lugar a otro.
- 15. Flujo transfronterizo de datos personales:** Se denomina flujo transfronterizo o transferencia internacional de datos personales a la transferencia de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.
- 16. Incidente de seguridad de datos personales:** Es 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.
- 17. Oficial de Datos Personales:** Es la persona designada por el responsable de tratamiento o encargado del tratamiento de datos personales para la verificación, asesoramiento e implementación del cumplimiento del régimen jurídico sobre protección de datos personales.

- 18. Receptor o importador de datos personales:** Es toda persona natural o jurídica de derecho privado, incluyendo las sucursales, filiales, vinculadas o similares o entidades públicas, que recibe los datos en caso de transferencia internacional, ya sea como titular del banco de datos personales o encargado del tratamiento.
- 19. Rectificación:** Es aquella acción destinada a afectar o modificar un dato personal ya sea para actualizarlo o corregirlo con datos exactos.
- 20. Representante:** Es la 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.
- 21. Repertorio de jurisprudencia:** Es el banco de resoluciones judiciales o administrativas, dictámenes fiscales, laudos arbitrales, resoluciones de comités de ética o similares, que se encuentra en soporte físico o digital, y organiza, entre otros, datos personales como fuente de consulta y habitualmente pública.
- 22. Responsable del tratamiento:** Es la persona natural, persona jurídica de derecho privado o entidad pública que decide sobre la finalidad y medios del tratamiento de datos personales. Esta definición no se restringe al titular del banco de datos, sino que incluye a cualquier persona que decida sobre el tratamiento de datos personales, aun cuando no se encuentre en un banco de datos personales.
- 23. Tratamiento:** Es cualquier operación o conjunto de operaciones, automatizados o no, que se realicen sobre los datos personales o conjuntos de datos personales.
- 24. Tercero:** Es toda persona natural, persona jurídica de derecho privado o entidad pública, distinta del titular de los datos personales, del titular del banco de datos o responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa de aquellos.

La referencia a “tercero” que hace el artículo 30 de la Ley constituye una excepción al significado previsto en este numeral.

#### **Artículo IV. Ámbito de aplicación**

- 4.1. El presente Reglamento es de aplicación al tratamiento de los datos personales, aun cuando no se encuentren en un banco de datos personales.

- 4.2. Se aplica a toda modalidad de tratamiento de datos personales, ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado, independientemente del soporte en el que se encuentren.
- 4.3. La existencia de normas o regímenes particulares o especiales, aun cuando incluyan regulaciones sobre datos personales, no excluye a las entidades públicas o instituciones privadas a las que dichos regímenes se aplican del ámbito de aplicación de la Ley y del presente Reglamento.
- 4.4. Lo dispuesto en el párrafo precedente no implica la derogatoria o inaplicación de las normas particulares, en tanto su aplicación no genere la afectación del derecho a la protección de datos personales.

## **Artículo V. Excepciones al ámbito de aplicación**

- 5.1. Las disposiciones de la Ley y del presente Reglamento no son de aplicación a los siguientes supuestos:
  1. El tratamiento de datos personales realizado por personas naturales para fines exclusivamente domésticos, personales o relacionados con su vida privada o familiar.
  2. Los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de la administración pública, solo en tanto la finalidad vigente del tratamiento resulte necesaria para el estricto cumplimiento de competencias asignadas por ley a las respectivas entidades públicas y siempre que tengan por objeto:
    - a) La defensa nacional,
    - b) La seguridad pública,
    - c) El desarrollo de actividades en materia penal para la investigación y represión del delito.
- 5.2. En el caso de que las entidades públicas referidas en el numeral 2 del párrafo 5.1. del presente artículo realicen el tratamiento de datos personales para una finalidad distinta a la vinculada al estricto cumplimiento de sus competencias, o para fines de archivo, administrativos, investigación histórica, científica o estadística, les es aplicable lo dispuesto en la Ley y en el presente Reglamento en lo pertinente.

## **Artículo VI. Ámbito de aplicación en y para territorio peruano**

Las disposiciones de la Ley y del presente Reglamento son de aplicación al tratamiento de datos personales cuando:

1. Sea efectuado en un establecimiento ubicado en territorio peruano correspondiente al titular del banco de datos personales o de quien resulte responsable del tratamiento.
2. Sea efectuado por un encargado del tratamiento, con independencia de su ubicación, a nombre de un titular de banco de datos personales establecido en territorio peruano o de quien sea el responsable del tratamiento.
3. El titular del banco de datos personales o quien resulte responsable no se encuentre establecido en territorio peruano, pero utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento de datos personales. Esta disposición comprende los siguientes supuestos:
  - 3.1. El titular del banco de datos personales o quien resulte responsable del tratamiento no se encuentre en territorio peruano, pero realiza actividades relacionadas a la oferta de bienes o servicios dirigidos a los titulares de datos personales ubicados en territorio peruano.
  - 3.2. El titular del banco de datos personales o quien resulte responsable del tratamiento no se encuentre en territorio peruano, pero realiza actividades orientadas al análisis de comportamiento de los titulares de datos personales ubicados en territorio peruano, así como la elaboración de perfiles que busquen predeterminedar conductas, preferencias, hábitos o similares.
4. El titular del banco de datos personales o quien resulte responsable del tratamiento no esté establecido en territorio peruano, pero le resulte aplicable la legislación peruana, por disposición contractual o del derecho internacional.

## **Artículo VII. Representante del titular del banco de datos personales o responsable del tratamiento de datos personales**

- 7.1. Para efectos de lo dispuesto en los numerales 3 y 4 del artículo VI, salvo se realice el tratamiento con fines de tránsito, el titular del banco de datos personales o quien resulte responsable, ubicado en el territorio peruano o fuera de este, debe proveer los medios necesarios para

el efectivo cumplimiento de las obligaciones previstas en la Ley y el Reglamento, y, designar un representante en el territorio peruano o para el territorio peruano, el cual es el punto de contacto con la Autoridad Nacional de Protección de Datos Personales.

- 7.2. El titular del banco de datos personales o quien resulte responsable puede realizar la designación del representante, de manera alternativa, de las siguientes formas:
1. Puede informarlo públicamente en la política de privacidad del titular del banco de datos personales o responsable del tratamiento; o,
  2. Puede comunicarlo a la Autoridad Nacional de Protección de Datos Personales, para lo cual debe tomar en cuenta lo establecido en el párrafo 7.3 siguiente.
- 7.3. En el caso de que la designación del representante sea comunicada a la Autoridad Nacional de Protección de Datos Personales, debe tomarse en cuenta los siguientes supuestos:
1. **Para un representante en territorio peruano:** debe realizarse de forma expresa a través de un documento válido a efectos de materializar su representación, de conformidad con los artículos 53 y 115 de la Ley N° 27444, Ley del Procedimiento Administrativo General o norma que lo sustituya.
  2. **Para un representante para el territorio peruano:** la designación debe comunicarse a la Autoridad por el canal establecido por el titular o encargado de tratamiento. Este representante debe estar acreditado para gestionar toda comunicación, solicitud de los titulares de datos personales, reclamación, denuncia o similar que se derive de los procedimientos administrativos, debiendo precisar para tales fines un correo electrónico para comunicaciones y contacto correspondiente.

## **Artículo VIII. Determinación de establecimiento**

- 8.1. En el caso de personas naturales, el establecimiento se entiende como el local en donde se encuentre el principal asiento de sus negocios o el que utilicen para el desempeño de sus actividades o su domicilio.
- 8.2. Tratándose de personas jurídicas, se entiende como el establecimiento el local en el que se encuentre la administración principal del negocio.

Si se trata de personas jurídicas residentes en el extranjero, se entiende que es el local en el que se encuentre la administración principal del negocio en territorio peruano, o en su defecto el que designen, o cualquier instalación estable que permita el ejercicio efectivo o real de una actividad.

8.3. Si no fuera posible establecer la dirección del establecimiento o del domicilio, se le considera con domicilio desconocido en territorio peruano.

### **Artículo IX. Principios rectores**

El titular del banco de datos personales, o en su caso, quien resulte responsable del tratamiento de datos personales, debe cumplir con el régimen jurídico en materia de protección de los datos personales de acuerdo con los principios rectores establecidos en la Ley; y, asimismo, conforme a los siguientes principios específicos:

- 1. Principio de transparencia:** El tratamiento de datos personales debe ser informado de manera permanente, clara, fácil de entender y accesible al titular de los datos personales. Este principio exige que el titular del dato personal tome conocimiento de las condiciones del tratamiento de sus datos personales, así como de los derechos que puede hacer valer respecto a aquellos y de las demás condiciones establecidas en el artículo 18 de la Ley.
- 2. Principio de responsabilidad proactiva:** En el tratamiento de datos personales se deben aplicar las medidas legales, técnicas y organizativas a fin de garantizar el cumplimiento efectivo de la normativa de datos personales, y el titular del banco de datos personales o quien resulte responsable, debe ser capaz de demostrar tal cumplimiento.

## **TÍTULO I TRATAMIENTO DE DATOS PERSONALES**

### **CAPÍTULO I CONSENTIMIENTO**

#### **Artículo 1. El consentimiento para el tratamiento de datos personales**

- 1.1. El titular del banco de datos personales o quien resulte como responsable del tratamiento, debe obtener el consentimiento para el tratamiento de los datos personales, de conformidad con lo establecido

en la Ley y en el presente Reglamento, salvo los supuestos establecidos en el artículo 14 de la Ley, en cuyo numeral 1 queda comprendido el tratamiento de datos personales que resulte imprescindible para ejecutar la interoperabilidad entre las entidades públicas.

- 1.2. La solicitud del consentimiento debe estar referida a un tratamiento o serie de tratamientos determinados, con expresa identificación de la finalidad o finalidades para las que se recaban los datos; así como las demás condiciones que concurran en el tratamiento o tratamientos, sin perjuicio de lo dispuesto en el siguiente artículo sobre las características del consentimiento.
- 1.3. Cuando el tratamiento de datos personales se refiera a finalidades distintas a los supuestos previstos en el artículo 14 de la Ley, debe obtenerse el consentimiento.
- 1.4. Cuando se solicite el consentimiento para una forma de tratamiento que incluya o pueda incluir la transferencia nacional o internacional de los datos, del titular de los mismos debe ser informado de forma que conozca inequívocamente tal circunstancia, además de la finalidad a la que se destinan sus datos y el tipo de actividad desarrollada por quien va a recibir los mismos.

## **Artículo 2. Características del consentimiento válido**

El consentimiento para el tratamiento de datos personales es válido si se cumplen las siguientes características:

1. Libre
2. Previo
3. Expreso e inequívoco
4. Informado

## **Artículo 3. Consentimiento libre**

- 3.1. Se considera que el consentimiento del titular de los datos personales es libre cuando se otorgue sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales.
- 3.2. El condicionamiento de la prestación de un servicio o la advertencia o la amenaza de denegar el acceso a beneficios o servicios que

normalmente son de acceso no restringido, sí afecta la libertad de quien otorga consentimiento para el tratamiento de sus datos personales, si los datos solicitados no son indispensables para la prestación de los beneficios o servicios.

- 3.3. La entrega de obsequios o beneficios al titular de los datos personales con ocasión de su consentimiento no afectan la condición de libertad que aquel tiene para otorgar tal consentimiento. Excepcionalmente, en el caso de niños, niñas y adolescentes, en los supuestos en que se admite su consentimiento, no se considera libre tal consentimiento otorgado mediando obsequios o beneficios.

#### **Artículo 4. Consentimiento previo**

El consentimiento debe ser solicitado al titular de los datos personales con anterioridad a la recopilación de tales datos o, en su caso, antes del tratamiento distinto a aquel por el cual ya se recopilaban dichos datos.

#### **Artículo 5. Consentimiento expreso e inequívoco**

- 5.1. Se considera que el consentimiento del titular de los datos personales es expreso cuando se haya exteriorizado a través de una acción que demuestre una aceptación concreta, directa y explícita respecto al tratamiento de los datos personales. Se puede considerar expreso cuando se realice en las siguientes formas:
  1. Verbal, cuando el titular del dato personal lo exterioriza oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral.
  2. Escrito, cuando se exterioriza mediante un documento o medio electrónico con su firma autógrafa, electrónica o digital, huella dactilar o cualquier otro mecanismo electrónico autorizado por el ordenamiento jurídico que pueda reflejar la manifestación de voluntad expresa.
  3. Por canales digitales, cuando se firma un documento a través de medios electrónicos o digitales, o cualquier otro mecanismo electrónico autorizado por el ordenamiento jurídico que pueda reflejar la manifestación expresa, así como la manifestación consistente en “hacer clic”, “clicquear” o “pinchar”, “dar un toque”, “touch” o “pad” u otros similares.
  4. Mediante cualquier otro medio conforme a lo establecido en el artículo 141 del Código Civil.

- 5.2. Se considera que el consentimiento es inequívoco cuando se pueda apreciar que los actos materiales por parte del titular del dato personal manifiestan la aceptación indubitable respecto a un determinado tratamiento de sus datos personales, sin generar posibilidad de duda o equivocación.
- 5.3. La sola expresión de voluntad en cualquiera de las formas reguladas en el presente artículo no exime del cumplimiento de los demás requisitos del consentimiento referidos a las características de libre, previo e informado.

## **Artículo 6. Consentimiento informado**

- 6.1. Cuando los datos personales son obtenidos directamente del titular de los datos personales se le debe comunicar de forma clara, con lenguaje sencillo, cuando menos lo siguiente:
  1. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos, y, cuando corresponda, del representante.
  2. La finalidad o finalidades del tratamiento a las que sus datos son sometidos.
  3. La identidad de los que son o pueden ser sus destinatarios, de ser el caso.
  4. La existencia e identificación del banco de datos personales en que se almacenarán, cuando corresponda.
  5. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.
  6. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
  7. En su caso, la transferencia nacional e internacional de datos que se efectúen.
  8. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y se transmita información relativa a las consecuencias para el titular del dato personal.

9. El plazo de conservación de los datos personales.
  10. Los mecanismos para el ejercicio de los derechos del Título III de la Ley.
- 6.2. Adicionalmente a lo previsto en el párrafo 6.1, cuando los datos personales no hayan sido recopilados de forma directa del titular de datos personales, el titular del banco de datos o quien resulte responsable debe estar en condiciones de informar, en el primer contacto y a requerimiento del titular de los datos personales, la fuente de recopilación de los datos personales.

### **Artículo 7. Políticas de privacidad**

La publicación de políticas de privacidad, de acuerdo con el segundo párrafo del artículo 18 de la Ley, se entiende como una forma de cumplimiento del deber de información y del principio de transparencia que no exonera del requisito de obtener el consentimiento del titular de los datos personales para el tratamiento de los mismos.

### **Artículo 8. Consentimiento y datos sensibles**

Tratándose de datos sensibles, además del cumplimiento de los requisitos para el consentimiento válido, este debe ser otorgado por escrito, a través de su firma manuscrita, digital, electrónica o cualquier otra modalidad que garantice la voluntad del titular de los datos personales.

### **Artículo 9. Consentimiento y carga de la prueba**

Para efectos de demostrar el consentimiento, en los términos establecidos en la Ley y en el presente Reglamento, la carga de la prueba recae en todos los casos en el titular del banco de datos personales o quien resulte el responsable del tratamiento.

### **Artículo 10. Negación, revocación y alcances del consentimiento**

- 10.1. El titular de los datos personales puede revocar su consentimiento para el tratamiento de sus datos personales en cualquier momento, sin justificación previa y sin que le atribuyan efectos retroactivos. Para la revocación del consentimiento se cumplen los mismos requisitos observados con ocasión de su otorgamiento, pudiendo ser estos más simples, si así se hubiera señalado en tal oportunidad.
- 10.2. El titular de los datos personales puede negar o revocar su consentimiento al tratamiento de sus datos personales para finalidades adicionales a aquellas que dan lugar a su tratamiento autorizado, sin que ello afecte la relación que da lugar al

consentimiento que sí ha otorgado o no ha revocado. En caso de revocatoria, es obligación de quien efectúa el tratamiento de los datos personales adecuar los nuevos tratamientos a la revocatoria y los tratamientos que estuvieran en proceso de efectuarse, en el plazo que resulte de una actuación diligente, que no puede ser mayor a diez (10) días.

- 10.3. Si la revocatoria afecta la totalidad del tratamiento de datos personales que se venía haciendo, el titular del banco de datos personales, encargado del tratamiento, o en su caso el responsable del tratamiento, aplica las reglas de cancelación o supresión de datos personales.
- 10.4. El titular del banco de datos personales o quien resulte responsable del tratamiento debe establecer mecanismos fácilmente accesibles e incondicionales, sencillos, rápidos y gratuitos para hacer efectiva la revocación.

## **CAPÍTULO II LIMITACIONES AL CONSENTIMIENTO**

### **Artículo 11. Tratamiento de los datos personales obtenidos a través de fuentes accesibles para el público**

- 11.1. Para los efectos de la Ley y el presente Reglamento, se consideran fuentes accesibles para el público, con independencia de que el acceso requiera contraprestación, las siguientes:
  1. Los medios de comunicación electrónica, óptica y de otra tecnología, siempre que el lugar en el que se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general, salvo una norma determine lo contrario.
  2. Las guías telefónicas, independientemente del soporte en el que estén a disposición y en los términos de su regulación específica.
  3. Los diarios y revistas independientemente del soporte en el que estén a disposición y en los términos de su regulación específica.
  4. Los medios de comunicación social.
  5. Las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión,

actividad, grado académico, dirección postal, número telefónico, número de fax, dirección de correo electrónico y aquellos que establezcan su pertenencia al grupo. En el caso de colegios profesionales, podrán indicarse además los siguientes datos de sus miembros: número de colegiatura, fecha de incorporación y situación gremial en relación al ejercicio profesional.

6. Los repertorios de jurisprudencia publicados conforme a ley.
  7. Los Registros Públicos administrados por la Superintendencia Nacional de Registros Públicos - SUNARP, así como todo otro registro o banco de datos calificado como público conforme a ley.
  8. Las entidades de la Administración Pública, en relación a la información que deba ser entregada en aplicación de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
- 11.2. Lo dispuesto en el numeral 8 del presente artículo no implica que todo dato personal contenido en información administrada por las entidades sujetas a la Ley de Transparencia y Acceso a la Información Pública sea considerado información de fuente accesible para el público. La evaluación del acceso a datos personales en posesión de entidades de administración pública se realiza atendiendo a las circunstancias de cada caso concreto, valorando la afectación probable a otros derechos fundamentales.
- 11.3. El tratamiento de los datos personales obtenidos a través de fuentes de acceso público debe respetar los principios establecidos en la Ley y en el presente Reglamento.

### **CAPÍTULO III TRANSFERENCIA DE DATOS PERSONALES**

#### **Artículo 12. Aspectos generales de la transferencia de datos personales**

- 12.1. La transferencia de datos personales es la comunicación de datos personales dentro o fuera del territorio nacional realizada a persona distinta al titular de los datos personales.
- 12.2. Aquel a quien se transfieran los datos personales se obliga, por el solo hecho de la transferencia, a la observancia de la Ley y del presente Reglamento.

### **Artículo 13. Condiciones para la transferencia de datos personales**

- 13.1. Toda transferencia de datos personales requiere el consentimiento de su titular, salvo las excepciones previstas en el artículo 14 de la Ley. Dicha transferencia debe limitarse a la finalidad que la justifique.
- 13.2. En todos los casos, la transferencia de datos personales debe ser informada al titular de los datos personales, conforme lo establece en el artículo 18 de la Ley.

### **Artículo 14. Carga de la prueba en la transferencia de datos personales**

Para efectos de demostrar que la transferencia se ha realizado conforme a lo que establece la Ley y el presente Reglamento, la carga de la prueba recae, en todos los casos, en el emisor o aquel que transfiere los datos personales.

### **Artículo 15. Transferencia dentro de un sector o grupo empresarial**

En el caso de transferencias de datos personales dentro de un grupo empresarial, sociedades subsidiarias afiliadas o vinculadas bajo el control común del mismo grupo empresarial o de aquellas afiliadas o vinculadas a una sociedad matriz o a cualquier sociedad del mismo grupo del titular del banco de datos o responsable del tratamiento, se debe solicitar el consentimiento del titular de los datos personales a menos que el tratamiento se enmarque en alguna de las excepciones previstas en el artículo 14 de la Ley, particularmente cuando se trate de un encargo de tratamiento de datos personales en el marco de una relación contractual previa.

### **Artículo 16. Receptor de los datos personales**

El receptor de los datos personales debe realizar el tratamiento de los datos personales cumpliendo con lo que el emisor informó al titular de los datos personales y respetando el contenido del consentimiento otorgado por el titular de datos personales. Para finalidades adicionales, debe recabar el consentimiento cuando así corresponda.

### **Artículo 17. Formalización de las transferencias nacionales**

La transferencia nacional se formaliza mediante mecanismos que permitan demostrar que el titular del banco de datos personales o el responsable del tratamiento cumple con comunicar al receptor de los datos personales las condiciones en las que el titular de los datos personales consintió el tratamiento de los mismos.

## **Artículo 18. Flujo transfronterizo de datos personales**

- 18.1. El flujo transfronterizo de datos personales se debe realizar cuando el receptor o importador de los datos personales se encuentre en un país que cuente con un nivel adecuado de protección de datos conforme a lo dispuesto en la Ley y el presente Reglamento.
- 18.2. En caso de que el país no cuente con el nivel adecuado de protección de datos, el emisor o exportador debe otorgar las garantías adecuadas para asegurar el tratamiento adecuado de datos personales fuera del territorio nacional, salvo las excepciones contempladas en el artículo 15 de la Ley.

## **Artículo 19. Nivel adecuado de protección de datos para el flujo transfronterizo**

- 19.1. Para determinar el nivel adecuado de protección de datos de un país, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales emite una resolución a efectos de determinar si este cuenta con una protección equiparable a lo dispuesto en la Ley y el presente Reglamento.
- 19.2. La evaluación precitada considera como mínimo y de modo concurrente, los siguientes criterios:
  1. La existencia de un marco jurídico legal de protección de datos personales.
  2. La existencia de principios para el tratamiento de los datos personales.
  3. La existencia de normas que reconozcan y garanticen los derechos de los titulares de datos y que puedan disponer de vías para ejercer los mismos.
  4. La existencia de una autoridad encargada de la protección de datos personales, o aquellas que hagan sus veces, para supervisar y sancionar por infracciones a la normativa, cuando corresponda.
- 19.3. La evaluación a la que se refiere el párrafo anterior es prescindible si el país, cuyo nivel adecuado de protección de datos que es materia de análisis, ha negociado y suscrito estándares comunes y generales de protección de datos personales con el Perú.

- 19.4. La resolución a la que se refiere el párrafo 19.1 se emite de oficio, a solicitud de parte o como consecuencia de las normas sectoriales que compelen a los sectores a recabar opinión técnica de la Autoridad Nacional de Protección de Datos Personales.

## **Artículo 20. Garantías para el flujo transfronterizo de datos personales**

- 20.1. Para efectos de lo señalado en el párrafo 18.2 del artículo 18 del presente Reglamento, el emisor o exportador puede valerse de cláusulas contractuales modelo u otros instrumentos jurídicos en los que se establezcan cuando menos las mismas obligaciones a las que se encuentra sujeto, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.
- 20.2. La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales emite modelos de cláusulas contractuales a fin de que los receptores o importadores asuman las obligaciones que corresponden al titular del banco de datos o responsable del tratamiento, y se establezca los derechos y libertades de los titulares de los datos personales y las obligaciones de los responsables de tratamiento.

## **Artículo 21. Opinión y registro del flujo transfronterizo de datos personales**

- 21.1. Sin perjuicio de lo señalado en los artículos 19 y 20 del presente Reglamento, los titulares del banco de datos personales o responsables del tratamiento, pueden solicitar opinión a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales respecto de si el flujo transfronterizo de datos personales que realizan cumple con la Ley y el presente Reglamento. Dicha opinión es emitida en un plazo máximo de treinta (30) días.
- 21.2. En cualquier caso, el flujo transfronterizo de datos personales debe ponerse en conocimiento de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, incluyendo la información que se requiere para la transferencia de datos personales y el registro de banco de datos. Dicha comunicación es inscrita en el Registro Nacional de Protección de Datos Personales a través del formato aprobado para tal efecto.

## **CAPÍTULO IV**

### **TRATAMIENTOS ESPECIALES DE DATOS PERSONALES**

#### **Artículo 22. Tratamiento de los datos personales de niños, niñas y adolescentes**

- 22.1. El tratamiento de los datos personales de niños, niñas y adolescentes se considera lícito cuando se obtenga el consentimiento de aquel o aquellos que ejercen la patria potestad o tutela, según corresponda.
- 22.2. Los mayores de catorce y menores de dieciocho años, de acuerdo a su capacidad, pueden otorgar el consentimiento para el tratamiento de sus datos personales siempre que la información proporcionada haya sido expresada en un lenguaje comprensible para ellos, conforme a la normativa de la materia.
- 22.3. En ningún caso el consentimiento para el tratamiento de datos personales de niños, niñas y adolescentes puede otorgarse para que accedan a actividades, vinculadas con bienes o servicios restringidos para su edad.

#### **Artículo 23. Prohibición de recopilación de datos a través niños, niñas y adolescentes**

- 23.1. No se puede recopilar datos personales de niños, niñas y adolescentes que permitan obtener información sobre los demás miembros de su grupo familiar, como son los datos relativos a la actividad profesional de sus progenitores, información económica, datos sociológicos o cualquier otro, sin el consentimiento de los titulares de tales datos.
- 23.2. Solo puede recopilarse los datos de identidad y dirección de los padres o de los tutores con la finalidad de obtener el consentimiento, en los casos en que así corresponda.

#### **Artículo 24. Fomento de la protección de los datos de niños, niñas y adolescentes**

Es obligación de todos los titulares de bancos de datos personales, especialmente de las entidades públicas, colaborar con el fomento del conocimiento del derecho a la protección de datos personales de los niños, niñas y adolescentes, así como de la necesidad de que su tratamiento se realice con especial responsabilidad y seguridad.

## **Artículo 25. Tratamiento de datos personales de niños, niñas y adolescentes en internet**

- 25.1. Es obligación de los titulares de bancos de datos personales, o de quien resulte responsable del tratamiento de datos de niños, niñas y adolescentes, garantizar la protección del interés superior del niño y de sus derechos fundamentales en el entorno digital.
- 25.2. En el marco de la oferta de servicios digitales para mayores de catorce y menores de dieciocho años, el tratamiento de datos personales es lícito cuando se haya obtenido su consentimiento.
- 25.3. En el marco de la oferta de servicios digitales dirigida a menores de catorce años de edad, el tratamiento de datos personales es lícito siempre que se cuente con el consentimiento de aquel o aquellos que ejercen la patria potestad o tutela, según corresponda.
- 25.4. El titular del banco de datos personales o responsable del tratamiento de datos en plataformas o servicios en el entorno digital realiza esfuerzos razonables para verificar, en los casos descritos en los párrafos 25.2 y 25.3, la identidad de quienes otorgan el consentimiento, teniendo en cuenta la tecnología disponible.

## **Artículo 26. Tratamiento de datos para publicidad y prospección comercial**

- 26.1. El tratamiento de datos personales para fines de publicidad y prospección comercial de productos y servicios es lícito cuando se obtiene el consentimiento de forma directa por parte del titular del dato personal.
- 26.2. Es posible obtener el consentimiento para el tratamiento de datos personales mediante un primer contacto, luego del cual, de no haberse logrado obtener el consentimiento, no es lícito realizar un nuevo contacto o tratamiento de datos personales.
- 26.3. Para el primer contacto, los datos personales pueden haber sido obtenidos de fuentes accesibles al público, en dicho supuesto, el responsable del tratamiento de datos personales debe estar en condiciones de informar, en el primer contacto y a requerimiento del titular de los datos personales, la fuente de recopilación de los datos personales.

- 26.4. Se presume que la responsabilidad del tratamiento de datos personales para publicidad y prospección comercial es de aquel en cuyo interés se realiza tal tratamiento, salvo prueba en contrario.
- 26.5. En todos los casos, el titular de datos personales tiene derecho de negarse, revocar u oponerse al tratamiento de sus datos personales para fines de publicidad y prospección comercial, para lo cual el responsable del tratamiento debe brindar un medio sencillo y gratuito para tramitar dicha solicitud, la cual se debe atender dentro del plazo máximo de diez (10) días. Negarse, revocar u oponerse al tratamiento de datos personales para fines de publicidad y prospección comercial no debe tener mayor complejidad que la empleada para otorgar el consentimiento.
- 26.6. El responsable del tratamiento establece los procedimientos necesarios a efectos de asegurar que aquellas solicitudes presentadas ante un encargado de tratamiento le sean remitidas a efectos de brindarles la atención oportuna.
- 26.7. La Autoridad Nacional de Protección de Datos Personales emite las disposiciones que considere pertinentes sobre lo regulado en el presente artículo.

### **Artículo 27. Tratamiento de datos personales en el sector comunicaciones y telecomunicaciones**

- 27.1. Los operadores de los servicios de comunicaciones o telecomunicaciones tienen la responsabilidad de velar por la confidencialidad, disponibilidad, uso adecuado e integridad de los datos personales que obtengan de sus abonados y usuarios, en el curso de sus operaciones comerciales.
- 27.2. Los operadores de los servicios de comunicaciones o telecomunicaciones no pueden realizar un tratamiento de los citados datos personales para finalidades distintas a las autorizadas por su titular, salvo orden judicial o mandato legal expreso.

### **Artículo 28. Tratamiento de los datos por medios tecnológicos tercerizados**

- 28.1. El tratamiento de datos personales por medios tecnológicos tercerizados, entre los que se encuentran servicios, aplicaciones, infraestructura, entre otros, está referido a aquellos en los que el procesamiento es automático, sin intervención humana.

- 28.2. Para los casos en los que en el tratamiento exista intervención humana se aplican los artículos 32 y 33 del presente Reglamento.
- 28.3. El tratamiento de datos personales por medios tecnológicos tercerizados, sea completo o parcial, puede ser contratado por el responsable del tratamiento de datos personales siempre y cuando para la ejecución de aquel se garantice el cumplimiento de lo establecido en la Ley y el presente Reglamento.

### **Artículo 29. Criterios a considerar para el tratamiento de datos personales por medios tecnológicos tercerizados**

Al realizar el tratamiento de los datos personales por medios tecnológicos tercerizados se debe considerar como prestaciones mínimas las siguientes:

1. Informar a los titulares de datos personales con transparencia las subcontrataciones que involucren la información sobre la que presta el servicio.
2. No incluir condiciones que autoricen o permitan al prestador asumir la titularidad sobre los bancos de datos personales tratados en la tercerización.
3. Garantizar la confidencialidad, integridad y disponibilidad respecto de los datos personales sobre los que preste el servicio.
4. Mantener el control, las decisiones y la responsabilidad sobre el proceso mediante el cual se realiza el tratamiento de los datos personales.
5. Garantizar y evidenciar la destrucción o la imposibilidad de acceder a los datos personales después de concluida la prestación.

### **Artículo 30. Mecanismos para la prestación del servicio de tratamiento de datos personales por medios tecnológicos tercerizados**

El prestador del servicio debe cumplir con los siguientes mecanismos:

1. Dar a conocer los cambios en sus políticas de privacidad o en las condiciones del servicio que presta al responsable del tratamiento, para obtener el consentimiento si ello significara incrementar sus facultades de tratamiento.
2. Permitir al responsable del tratamiento limitar el tipo de tratamiento de los datos personales sobre los que presta el servicio.

3. Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que presta el servicio.
4. Garantizar y evidenciar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último los haya podido recuperar.
5. Impedir el acceso a los datos personales a quienes no cuenten con privilegios de acceso, o bien en caso sea solicitada por la autoridad competente, informar de ese hecho al responsable.

### **Artículo 31. Prestación de servicios o tratamiento por encargo**

- 31.1. El encargado del tratamiento de datos personales se encuentra prohibido de transferir a terceros los datos personales objeto de la prestación de servicios de tratamiento, a menos que el titular del banco de datos personales o responsable del tratamiento que le encargó el tratamiento lo haya autorizado y el titular del dato personal haya brindado su consentimiento, en los supuestos que dicho consentimiento sea requerido conforme a Ley.
- 31.2. El plazo para la conservación de datos personales al que hace referencia el artículo 30 de la Ley es como máximo de dos (2) años contados desde la finalización del último encargo realizado. La conservación de datos personales en un plazo mayor al establecido sólo puede realizarse en el supuesto previsto en el segundo párrafo del artículo 30 de la Ley o porque así lo dispone expresamente una disposición normativa vigente, para tal caso los datos deben ser devueltos al responsable de tratamiento para su conservación mientras la obligación legal persista. La conservación indeterminada de los datos personales, por regla general, está prohibida.
- 31.3. Lo dispuesto en el presente artículo es aplicable, en lo que corresponda, a la subcontratación de la prestación de servicios de tratamiento de datos personales.

### **Artículo 32. Tratamiento a través de subcontratación**

- 32.1. El tratamiento de datos personales puede realizarse por un tercero diferente al encargado del tratamiento, a través de un convenio o contrato entre estos dos.
- 32.2. Para este supuesto se requiere, de manera previa, una autorización

por parte del titular del banco de datos personales o responsable del tratamiento. Dicha autorización se entiende también concedida si estaba prevista en el instrumento jurídico mediante el cual se formalizó la relación entre el responsable del tratamiento y el encargado del mismo.

- 32.3. El tratamiento que haga el subcontratista se realiza en nombre y por cuenta del responsable del tratamiento, pero la carga de probar la autorización le corresponde al encargado del tratamiento.

### **Artículo 33. Responsabilidad del tercero subcontratado**

La persona natural o jurídica subcontratada asume las mismas obligaciones que se establezcan para el encargado del tratamiento en la Ley, el presente Reglamento y demás disposiciones aplicables. Sin embargo, asume las obligaciones del titular del banco de datos personales cuando:

1. Destine o utilice los datos personales con una finalidad distinta a la autorizada por el titular del banco de datos o responsable del tratamiento; o,
2. Efectúe una transferencia, incumpliendo las instrucciones del titular del banco de datos personales, aun cuando sea para la conservación de dichos datos.

## **CAPÍTULO V**

### **OBLIGACIONES EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES**

#### **Artículo 34. Notificación del incidente de seguridad de datos personales**

- 34.1. En caso de un incidente de seguridad de datos personales que genere exposición de grandes volúmenes de los mismos, 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, el titular del banco de datos o el responsable del tratamiento debe notificar a la Autoridad Nacional de Protección de Datos Personales como máximo dentro de las 48 horas posteriores a haber tomado conocimiento o constancia de ello. Si dicha notificación se efectúa en un tiempo superior a 48 horas, debe ir acompañada de la indicación de los motivos y/o sustento probatorio de tal dilación. Esta obligación permanece aun cuando el responsable de tratamiento de datos personales considere que tal incidente haya sido subsanado o resuelto internamente.

- 34.2. La notificación del incidente de seguridad de datos personales debe

señalar y describir como mínimo lo siguiente:

1. La naturaleza del incidente de seguridad de los datos personales, inclusive, cuando sea posible, los tipos de datos y el número aproximado de titulares de datos afectados.
  2. El nombre y los datos de contacto del Oficial de datos personales o de otro punto de contacto en el que pueda obtenerse más información.
  3. Las posibles consecuencias del incidente de seguridad de los datos personales.
  4. Las medidas adoptadas o propuestas por el titular del banco de datos o responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- 34.3. El titular del banco de datos o responsable del tratamiento que advierta un incidente de seguridad de datos personales que afecte al titular de los mismos en otros de sus derechos, debe comunicarlo dentro de las 48 horas a dicho titular sin dilación indebida, en un lenguaje sencillo y claro para su comprensión, así como de las medidas adoptadas para mitigar sus efectos. Si dicha comunicación se efectúa en un tiempo superior a las 48 horas debe ir acompañada de la indicación de los motivos de tal dilación.
- 34.4. Cuando el incidente de seguridad de datos personales no produjo la afectación antes descrita y fue superado totalmente por las medidas adoptadas no subsiste la obligación de comunicar dicho incidente al titular de los datos personales.
- 34.5. En caso de que el incidente de seguridad de datos personales se desarrolle en y/o mediante el entorno digital la notificación se realiza, además de la Autoridad Nacional de Protección de Datos Personales, al Centro Nacional de Seguridad Digital para su incorporación al Registro Nacional de Incidentes de Seguridad Digital conforme a lo establecido en el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, su Reglamento y normas complementarias.
- 34.6. Siempre que sea indispensable para la gestión de incidentes de seguridad de datos personales, la recopilación y transferencia de dichos datos hacia o entre entidades públicas, con competencia legal para realizar dicha gestión, no requiere consentimiento, en el marco de lo dispuesto en el numeral 1 del artículo 14 de la Ley N° 29733, Ley de Protección de Datos Personales.

- 34.6.<sup>21</sup>La Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros y la Autoridad Nacional de Protección de Datos Personales proponen y establecen protocolos para asegurar la interoperabilidad, colaboración e intercambio de información sobre las notificaciones de incidentes de seguridad de datos personales cuando se desarrollen en y mediante el entorno digital.
- 34.7.<sup>22</sup>La Autoridad Nacional de Protección de Datos Personas aprueba las disposiciones y/o lineamientos necesarios para el debido cumplimiento del presente artículo.

### **Artículo 35. Documentación de incidentes de seguridad**

El responsable del tratamiento de datos personales debe documentar cualquier incidente de seguridad, incluyendo los hechos relacionados a ello, sus efectos y las medidas adoptadas. Dicha documentación permite a la Autoridad Nacional de Protección de Datos Personales verificar el cumplimiento de las obligaciones referidas a esta materia.

### **Artículo 36. Obligación del encargado del tratamiento**

El encargado del tratamiento debe informar de forma inmediata al titular del banco de datos personales o responsable del tratamiento del incidente de seguridad de los datos personales de las que tenga conocimiento.

### **Artículo 37. Designación del Oficial de Datos Personales**

- 37.1. El titular del banco de datos personales o responsable y el encargado de tratamiento deben designar a un Oficial de Datos Personales cuando:
1. El tratamiento lo lleve a cabo una entidad pública, de conformidad con lo establecido en el párrafo 68.6 del artículo 68 del Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, aprobado por Decreto Supremo N° 029-2021-PCM.
  2. El titular del banco de datos o responsable del tratamiento o el encargado de tratamiento realicen tratamientos de grandes volúmenes de datos personales, en cantidad o tipo de datos, o que

21 NOTA SPIJ: En la presente edición de Normas Legales del diario oficial "El Peruano", dice: "34.6", debiendo decir: "34.7".

22 NOTA SPIJ: En la presente edición de Normas Legales del diario oficial "El Peruano", dice: "34.7", debiendo decir: "34.8".

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.

3. El titular del banco de datos o responsable de tratamiento o el encargado del tratamiento realicen actividades principales o de giro de negocio que comprendan el tratamiento de datos sensibles.
- 37.2. Un grupo empresarial puede nombrar un único Oficial de datos personales siempre que sea fácil contactarlo desde cada establecimiento.
- 37.3. Cuando el titular del banco de datos o el responsable del tratamiento sea una autoridad u organismo público, se puede designar un único Oficial de datos personales para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.
- 37.4. El titular del banco de datos o el responsable o encargado del tratamiento debe publicar los datos de contacto del Oficial de datos personales en un lugar visible que permita a los titulares de datos personales tomar conocimiento de ello.
- 37.5. Los datos de contacto del Oficial de datos personales designado, y cualquier actualización, deben ser comunicados a la Autoridad Nacional de Protección de Datos Personales dentro de los 15 días siguientes a la designación o actualización respectiva.

### **Artículo 38. Perfil del Oficial de datos personales**

- 38.1. El Oficial de datos personales es designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos y práctica en materia de protección de datos personales, debidamente acreditados, lo cual le debe permitir desempeñar eficientemente las funciones del artículo 39 del presente Reglamento.
- 38.2. El Oficial de datos personales puede ser una persona que desempeñe otras funciones en la empresa, entidad pública, sin que sea necesario que desempeñe con exclusividad las funciones vinculadas a su designación, pudiendo incluso ser una persona externa a la organización privada.

## **Artículo 39. Funciones del Oficial de Datos Personales**

39.1. El Oficial de datos personales tiene como mínimo las siguientes funciones:

1. Informar y asesorar al titular del banco de datos personales o al responsable del tratamiento y a los empleados que se ocupen del tratamiento de los datos personales respecto de las obligaciones que les incumben en virtud de la Ley, el presente Reglamento y de otras disposiciones de protección de datos.
2. Verificar e informar sobre el cumplimiento de lo dispuesto en la Ley, el presente Reglamento y de otras disposiciones de protección de datos personales, así como del cumplimiento de las políticas del titular del banco de datos o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la sensibilización y formación del personal que participa en las operaciones de tratamiento, y las auditorías que se realicen.
3. Cooperar, en lo que resulte pertinente, con la Autoridad Nacional de Protección de Datos Personales para el desempeño de sus fines y atribuciones.
4. Actuar como punto de contacto de la Autoridad Nacional de Protección de Datos Personales para cuestiones relativas al tratamiento de datos personales.

39.2 El Oficial de datos personales desempeña sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento de datos personales, teniendo en cuenta la naturaleza, el alcance, el contexto y fines de tal tratamiento.

## **Artículo 40. Evaluación de impacto relativo a la protección de datos personales**

40.1. De manera facultativa y previa al tratamiento de datos personales, el titular del banco de datos o responsable del tratamiento puede realizar la Evaluación de impacto relativa a la protección de datos personales, especialmente cuando se trate de datos sensibles, datos con fines de crear perfiles personales, datos de personas en especial situación de vulnerabilidad como niños, niñas y adolescentes, personas pertenecientes a pueblos indígenas en situación de aislamiento y/o contacto inicial o personas con discapacidad; o cuando se realice

tratamiento de grandes volúmenes de datos u otros supuestos determinados por la Autoridad Nacional de Protección de Datos Personales.

- 40.2. La evaluación de impacto relativo a la protección de datos personales se puede elaborar tomando como referencia la guía, lineamientos y procedimientos establecidos en la NTP-ISO/IEC 27005 y la NTP-ISO 31000 en su edición vigente u otros estándares relacionados con el análisis y la evaluación de riesgos para la protección de datos personales.
- 40.3. La Autoridad Nacional de Protección de Datos Personales emite las disposiciones complementarias que resulten pertinentes para la realización de la Evaluación de impacto relativo a la protección de datos personales.

#### **Artículo 41. Procedimiento de disociación**

- 41.1. La disociación es el procedimiento que impide la identificación o que no hace identificable al titular de los datos personales. Este procedimiento es reversible.
- 41.2. El responsable o encargado del tratamiento de datos personales debe elegir la técnica adecuada al momento de realizar el procedimiento de disociación, atendiendo siempre al tipo de datos objeto de tratamiento, el número de titulares de datos y el factor de riesgo (gravedad, la probabilidad, las consecuencias para el responsable y el titular) y los que la Autoridad Nacional determine para tal efecto.
- 41.3. La Autoridad Nacional de Protección de Datos Personales aprueba las disposiciones complementarias u orientativas para la realización del procedimiento de disociación y de anonimización.

#### **Artículo 42. Obligación de inscripción**

- 42.1. Las personas naturales o jurídicas del sector privado o entidades públicas que creen, modifiquen o cancelen bancos de datos personales están obligadas a tramitar la inscripción de dichos actos ante el Registro Nacional de Protección de Datos Personales.
- 42.2. El Registro Nacional de Protección de Datos Personales es la unidad de almacenamiento destinada a contener principalmente la información sobre los bancos de datos personales de titularidad pública o privada y tiene por finalidad dar publicidad de la inscripción de dichos bancos

de tal forma que sea posible ejercer los derechos de acceso a la información, rectificación, cancelación, oposición y otros regulados en la Ley y el presente Reglamento.

### **Artículo 43. Actos y documentos inscribibles en el Registro Nacional**

- 43.1. Son objeto de inscripción en el Registro Nacional de Protección de Datos Personales con arreglo a lo dispuesto en la Ley y en este título:
1. Los bancos de datos personales de la administración pública, con las excepciones previstas en la Ley y el presente Reglamento.
  2. Los bancos de datos personales de administración privada, con la excepción prevista en el numeral 1 del artículo 3 de la Ley.
  3. Las sanciones, medidas cautelares o correctivas impuestas por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales conforme a la Ley y el presente Reglamento.
- 43.2. Cualquier persona puede consultar la información a que se refiere el artículo 34 de la Ley y cualquier otra contenida en el Registro Nacional.
- 43.3. La inscripción de los actos precitados en el Registro Nacional de Protección de Datos Personales es gratuita, incluyendo la modificación y cancelación de la inscripción de acuerdo a lo señalado en el presente Reglamento.

### **Artículo 44. Modificación o cancelación de bancos de datos personales en el Registro Nacional de Inscripción de bancos de datos personales**

- 44.1. La inscripción de un banco de datos personales de la administración pública o privada en el Registro Nacional de Inscripción de bancos de datos personales debe mantenerse actualizada en todo momento.
- 44.3. <sup>23</sup>Los titulares de los bancos de datos personales o responsables de su tratamiento, comunican la modificación o cancelación que se realice a la inscripción del banco de datos inscritos ante el Registro Nacional de Protección de Datos Personales presentando la solicitud vía formulario de cancelación o modificación dirigida a la Dirección de Protección de Datos Personales.

---

23 NOTA SPIJ: En la presente edición de Normas Legales del diario oficial "El Peruano", dice: "44.3", debiendo decir: "44.2".

## **Artículo 45. Procedimiento**

- 45.1. Los titulares de los bancos de datos personales solicitan la inscripción de los bancos de datos ante el Registro Nacional de Protección de Datos Personales, vía formulario, ante la Dirección de Protección de Datos Personales.
- 45.2. El procedimiento de inscripción es de aprobación automática y se rige conforme las disposiciones establecidas en el artículo 31 de la Ley N° 27444, Ley del Procedimiento Administrativo General o norma que lo sustituya.

## **CAPÍTULO VI MEDIDAS DE SEGURIDAD**

### **Artículo 46. Seguridad para el tratamiento de datos a través de medios digitales**

Las plataformas, sitios web, aplicaciones móviles, servicios digitales y los sistemas informáticos que son empleados para realizar tratamiento de datos personales deben tener documentado e implementado lo siguiente:

1. El control de acceso a los datos personales que incluye:
  - a) Gestión de accesos desde el registro de un usuario hasta su eliminación o baja, incluyendo eventualidades periódicas como periodos vacacionales o permisos esporádicos.
  - b) Procedimientos de identificación y autenticación.
  - c) Gestión de los privilegios asignados a dicho usuario, incluyendo la verificación periódica de los mismos, que debe ser ejecutado periódicamente en un intervalo mínimo de tiempo semestral.
  - d) Mecanismos de autenticación del usuario ante el sistema que implica la asignación de uso de usuario-contraseña, uso de certificados digitales, tokens, entre otros.
2. El monitoreo y revisión periódica de las medidas de seguridad y los planes de capacitación del personal, dependiendo de sus roles y responsabilidades, respecto al tratamiento de datos personales que efectúan.

3. La generación y el mantenimiento de registros que provean evidencia de las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones referidas a procesamiento, visualización, modificación, eliminación, importación y exportación de datos personales.

Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, almacenamiento, transferencia, destrucción una vez que los registros ya no sean útiles y generarse y/o ejecutarse de manera periódica. Dichos registros deben conservarse por un periodo mínimo de dos (2) años.

Los registros de interacción lógica correspondientes a trazabilidad de las acciones realizadas por los operadores de los sistemas empleados para realizar el tratamiento de los datos personales deben generarse de manera continua y deben encontrarse disponibles de manera inmediata.

4. Las medidas de seguridad que impidan al personal no autorizado la generación de copias o la reproducción de documentos digitales que contengan datos personales. En el caso de uso de sistemas, aplicaciones de mensajería instantánea, uso de cuentas de correo electrónico y/o redes sociales no institucionales, estos deben ser debidamente aprobados y formalmente establecidos, a efectos de evitar generar riesgos y transferencias no autorizadas de datos personales.

#### **Artículo 47. Documento de Seguridad**

- 47.1. El responsable del tratamiento de datos personales debe contar con un documento de seguridad el cual debe ser aprobado formalmente y contar con fecha cierta. El documento de seguridad debe estar actualizado y contener como mínimo los procedimientos de gestión de accesos, la gestión de privilegios y la verificación periódica de los privilegios asignados referentes a los sistemas de información, incluyendo, plataformas tecnológicas, aplicaciones móviles, motores de bases de datos, entre otros, empleados para realizar el tratamiento de datos personales. Puede tomar como referencia los requisitos y controles indicados en la NTP-ISO/IEC 27001 vigente o alguna mejor práctica o estándar ampliamente reconocido en su sector. En el caso de las entidades públicas aplican lo dispuesto en las normas de gobierno digital y seguridad digital vigentes.

- 47.2. El documento de seguridad es de obligatorio cumplimiento para el personal con acceso a los sistemas de información. El responsable de su elaboración debe determinar las medidas necesarias para que el personal conozca adecuadamente las consecuencias de su incumplimiento y aplique las medidas de seguridad necesarias para su sustento.
- 47.3. El documento de seguridad debe contener políticas internas para la gestión y el tratamiento de los datos personales que tomen en cuenta el contexto y el ciclo de vida de los datos personales, es decir su obtención, uso y posterior supresión. Asimismo, debe elaborar un inventario de datos personales y de los sistemas empleados para el tratamiento debiendo especificar si se trata datos sensibles.

#### **Artículo 48. Conservación, respaldo y recuperación de los datos personales**

- 48.1. En los ambientes en los que se procese, almacene o transmita la información se debe diseñar e implementar como mínimo los siguientes controles de seguridad:
1. Controles para mantener las áreas seguras.
  2. Controles para mantener los equipos seguros dentro y fuera de las instalaciones.
  3. Controles para garantizar la generación de copias de respaldo seguras y continuas y verificación de integridad de las mismas.
- 48.2. El responsable del tratamiento de datos personales puede tomar como referencia las recomendaciones indicadas en la “NTP-ISO/IEC 27001:2022 Tecnología de la información. Técnicas de Seguridad. Sistemas de Seguridad de la información. Requisitos” en la edición que se encuentre vigente.

#### **Artículo 49. Controles para mantener las áreas seguras**

- 49.1. Los controles para mantener las áreas seguras son los siguientes:
1. Perímetros de seguridad que protegen áreas donde se realice el tratamiento de datos personales.
  2. Controles apropiados de ingreso para asegurar que se le permita el acceso solo al personal autorizado.

3. Sistema contra desastres naturales, ataque maliciosos o accidentes.
4. Procedimientos para el trabajo en áreas seguras.
5. Control de puntos de acceso, áreas de despacho, carga y otros donde personas no autorizadas pueden ingresar al local, y de ser el caso aislar las instalaciones de procesamiento de la información para evitar el acceso no autorizado.

### **Artículo 50. Controles para mantener los equipos seguros dentro y fuera de las instalaciones**

- 50.1. Los controles para mantener los equipos seguros dentro y fuera de las instalaciones son los siguientes:
1. Ubicación y protección de equipos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.
  2. Protección de equipos contra fallas de electricidad y otras alteraciones causadas por desperfectos en los servicios de suministro.
  3. Protección de interceptación, interferencia y/o daño del cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte.
  4. Imposibilidad de retirar equipos, información o software sin la autorización previa.
  5. Asegurar, antes de su disposición o reutilización, que los equipos que contengan medios de almacenamiento de datos sensibles, hayan sido eliminados o sobre escritos.
  6. Asegurar que los equipos informáticos cuenten con protección apropiada en caso sean desatendidos por los usuarios.
  7. Implementación de una política de escritorio y pantalla limpios de papeles y de medios de almacenamiento removibles, para las instalaciones de procesamiento de la información.

### **Artículo 51. Controles para garantizar la generación de copias de respaldo seguras y continuas y verificación de integridad de las mismas**

- 51.1. Las copias de respaldo se realizan con una frecuencia semanal como mínimo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos personales. Dicho procedimiento debe contar con las medidas de seguridad para su almacenamiento, transferencia y destrucción si fuese el caso.
- 51.2. Se debe verificar la integridad de los datos almacenados en las copias de respaldo, incluyendo, de ser el caso, la recuperación completa ante una interrupción o daño que garantice el retorno al estado en el que se encontraba al momento en que se produjo la interrupción o daño.

### **Artículo 52. Transferencia lógica o electrónica de los datos personales**

El intercambio de datos personales desde los ambientes de procesamiento o almacenamiento hacia cualquier destino fuera de las instalaciones físicas de la entidad, solo procede con la autorización del titular del banco de datos personales y se realiza utilizando los medios de transporte autorizados por el mismo, implementando las medidas necesarias (entre las que se encuentran el cifrado de datos, uso de firmas y certificados digitales, checksum de verificación, entre otros) para evitar el acceso no autorizado, pérdida o corrupción durante el tránsito hacia su destino.

### **Artículo 53. Almacenamiento de documentación no automatizada**

- 53.1. Los armarios, archivadores u otros elementos en los que se almacenen datos personales contenidos en documentos no automatizados son protegidos con puertas dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Las áreas en las que se encuentran los datos personales permanecen cerradas cuando no sea preciso el acceso a los documentos. Todas las llaves o mecanismos de apertura deben ser asignadas de manera formal, y de ser el caso, deben contar con procedimientos de traspaso y asignación.
- 53.2. Si por las características de los locales que se dispusiera no fuera posible mantener cerradas las áreas donde se encuentran los armarios, archivadores u otros elementos en los que se almacenen documentos no automatizados con datos personales, se deben adoptar las medidas alternativas, conforme a las directivas de seguridad brindadas por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

#### **Artículo 54. Copia o reproducción de documentación automatizada y no automatizada**

- 54.1. La generación de copias o la reproducción de los documentos que contienen datos personales, únicamente pueden ser realizadas bajo el control del personal autorizado.
- 54.2. Debe procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

#### **Artículo 55. Acceso a la documentación**

- 55.1. El acceso a la documentación se limita exclusivamente al personal autorizado.
- 55.2. Se deben establecer mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
- 55.3. El acceso de personas no incluidas en el párrafo anterior debe quedar adecuadamente registrado.

#### **Artículo 56. Traslado de documentación no automatizada**

Siempre que se proceda al traslado físico de la documentación contenida en un banco de datos, debe adoptarse medidas dirigidas a impedir el acceso no autorizado, el mal uso, la manipulación y alteración de los datos personales objeto de traslado.

#### **Artículo 57. Prestaciones de servicios sin acceso a datos personales**

- 57.1. El responsable o el encargado de la información o tratamiento debe implementar los mecanismos o medidas de seguridad adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.
- 57.2. Cuando se trate de personal ajeno, el contrato de prestación de servicios recoge expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

### **Artículo 58. Determinación de fecha cierta de documentos**

La fecha cierta de los documentos presentados por los administrados como medios probatorios debe ser determinada conforme a la valoración probatoria realizada por el órgano competente, para la cual se considera los siguientes criterios alternativos:

1. Que el documento haya sido presentado ante funcionario o notario público; o,
2. Que el documento se haya difundido a través de un medio público de fecha determinada o determinable; o,
3. Que existan otros medios técnicos idóneos que generen convicción sobre ello.

## **CAPÍTULO VII CÓDIGOS DE CONDUCTA**

### **Artículo 59. Alcances de los Códigos de conducta**

- 59.1. Los códigos de conducta son un mecanismo de responsabilidad proactiva que permite demostrar el cumplimiento de las obligaciones establecidas en la Ley y el presente Reglamento para el tratamiento de datos personales. Los Códigos de conducta tienen carácter voluntario.
- 59.2. Los códigos de conducta de carácter sectorial pueden referirse a la totalidad o a parte de los tratamientos llevados a cabo por el sector, debiendo ser formulados por organizaciones representativas del mismo.
- 59.3. Los códigos de conducta promovidos por una empresa o grupo empresarial deben referirse a la totalidad de los tratamientos llevados a cabo por los mismos.
- 59.4. La implementación del Código de Conducta, debidamente acreditada de manera previa al inicio del procedimiento administrativo sancionador, conforme a los requisitos regulados en el presente Reglamento, se considera atenuante de responsabilidad.

### **Artículo 60. Contenido**

- 60.1. Los códigos de conducta deben redactarse en términos claros y accesibles.

60.2. Los códigos de conducta se adecuan a lo establecido en la Ley e incluyen como mínimo los siguientes aspectos:

1. La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.
2. Las disposiciones para el cumplimiento de los principios de protección de datos personales a los tratamientos sometidos al código de conducta.
3. El establecimiento de procedimientos que faciliten el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición de los afectados.
4. La determinación de las transferencias nacionales e internacionales de datos personales que, en su caso, se prevean con indicación de las garantías que deban adoptarse.
5. Las acciones de fomento y difusión en materia de protección de datos personales dirigidas a quienes los traten.
6. Mecanismos para asegurar la confidencialidad de los datos personales por parte de quienes los traten.
7. Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código de conducta.
8. Cláusulas para la obtención del consentimiento de los titulares de los datos personales al tratamiento o transferencia de sus datos personales.
9. Cláusulas para informar a los titulares de los datos personales del tratamiento.
10. Formatos para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.
11. En caso de que se realice el tratamiento de datos personales por encargo, se presenta formatos de cláusulas para la contratación del encargado del tratamiento, conforme lo establece la Ley y el presente Reglamento.

## TÍTULO II DERECHOS DEL TITULAR DE DATOS PERSONALES

### CAPÍTULO I DISPOSICIONES GENERALES

#### **Artículo 61. Carácter personal**

Los derechos de información, acceso, rectificación, cancelación, oposición y tratamiento objetivo de datos personales sólo pueden ser ejercidos por el titular de datos personales, sin perjuicio de las normas que regulan la representación.

#### **Artículo 62. Ejercicio de los derechos del titular de datos personales**

El ejercicio de alguno o algunos de los derechos no excluye la posibilidad de ejercer alguno o algunos de los otros, ni puede ser entendido como requisito previo para el ejercicio de cualquiera de ellos.

#### **Artículo 63. Legitimidad para ejercer los derechos**

63.1. El ejercicio de los derechos contenidos en el presente título se realiza:

1. Por el titular de datos personales, acreditando su identidad y presentando copia del Documento Nacional de Identidad o documento equivalente. El empleo de la firma digital conforme a la normatividad vigente sustituye la presentación del Documento Nacional de Identidad y su copia.
2. Mediante representante legal acreditado como tal.
3. Mediante representante expresamente facultado para el ejercicio del derecho, adjuntando la copia de su Documento Nacional de Identidad o documento equivalente, y del título que acredite la representación.

63.2. Cuando el titular del banco de datos personales sea una entidad pública, puede acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, conforme al artículo 115 de la Ley N° 27444, Ley del Procedimiento Administrativo General u otra que la sustituya.

63.2.<sup>24</sup>En caso se opte por el procedimiento señalado en el artículo 65 del presente Reglamento, la acreditación de la identidad del titular se sujeta a lo dispuesto en dicha disposición.

---

24 NOTA SPIJ: En la presente edición de Normas Legales del diario oficial "El Peruano", dice: "63.2", debiendo decir: "63.3".

#### **Artículo 64. Requisitos de la solicitud**

El ejercicio de los derechos se lleva a cabo mediante solicitud dirigida al titular del banco de datos personales o responsable del tratamiento o ante el encargado de tratamiento, si como consecuencia del encargo se establece en el contrato o relación jurídica que los vincule a la obligación de atender las solicitudes o se considere un responsable de tratamiento por administrar la base de datos personales, la misma que debe contener:

1. Nombres y apellidos del titular del derecho y acreditación de los mismos, y en su caso de su representante conforme al artículo precedente.
2. Petición concreta que da lugar a la solicitud.
3. Domicilio, o dirección que puede ser electrónica, a efectos de las notificaciones que correspondan.
4. Fecha y firma del solicitante.
5. Documentos que sustenten la petición, de ser el caso.
6. Pago de la contraprestación, tratándose de entidades públicas siempre que lo tengan previsto en sus procedimientos de fecha anterior a la vigencia del presente Reglamento.

#### **Artículo 65. Servicios de atención al público**

- 65.1. Cuando el titular del banco de datos personales o responsable del tratamiento disponga de servicios de cualquier naturaleza para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o productos ofertados, puede también atender las solicitudes para el ejercicio de los derechos comprendidos en el presente título a través de dichos servicios, siempre que los plazos no sean mayores a los establecidos en el presente Reglamento.
- 65.2. En este caso, la identidad del titular de datos personales se considera acreditada por los medios establecidos por el titular del banco de datos personales o responsable del tratamiento para la identificación de aquel, siempre que se acredite la misma, conforme a la naturaleza de la prestación del servicio o producto ofertado.

## **Artículo 66. Recepción y subsanación de la solicitud**

- 66.1. Todas las solicitudes presentadas deben ser recibidas dejándose constancia de su recepción por parte del titular del banco de datos personales o responsable del tratamiento o encargado de tratamiento, cuando así corresponda.
- 66.2. En caso de que la solicitud no cumpla con los requisitos del artículo 63, el titular del banco de datos personales o responsable de su tratamiento, en un plazo de cinco (5) días, contado desde el día siguiente de la recepción de la solicitud, formula las observaciones que no puedan ser salvadas de oficio, invitando al titular a subsanarlas dentro de un plazo máximo de cinco (5) días. Transcurrido el plazo señalado sin que ocurra la subsanación se tiene por no presentada la solicitud.
- 66.3. Las entidades públicas aplican el artículo 126 de la Ley N° 27444, Ley del Procedimiento Administrativo General u otra que la sustituya, sobre observaciones a la documentación presentada.
- 66.4. Cuando la solicitud del ejercicio del derecho es presentada ante el encargado de tratamiento de datos personales, este debe trasladarlo en un plazo máximo de tres (3) días al titular del banco de datos o responsable del tratamiento a fin de que se atienda la solicitud correspondiente.
- 66.5. Cuando la solicitud del ejercicio del derecho es presentada ante el encargado de tratamiento de datos personales, siendo quien cumple el encargo con la base de datos del titular del banco de datos o responsable del tratamiento, debe recepcionar la solicitud y trasladarla de inmediato a fin de que se atienda el derecho del titular de los datos personales, conforme establece el párrafo 65.1 del presente artículo, y además debe comunicarlo al titular del dato personal.

## **Artículo 67. Facilidades para el ejercicio del derecho**

- 67.1. El titular del banco de datos personales o responsable del tratamiento o encargado de tratamiento cuando corresponda, está obligado a establecer un procedimiento sencillo para el ejercicio de los derechos. Independientemente de los medios o mecanismos que la Ley y el presente Reglamento establezcan para el ejercicio de los derechos del titular de datos personales, el titular del banco de datos personales o el responsable del tratamiento o encargado de tratamiento puede

ofrecer mecanismos que faciliten el ejercicio de tales derechos en beneficio del titular de datos personales.

- 67.2. Para efectos de la contraprestación que debe abonar el titular de datos personales para el ejercicio de sus derechos ante la administración pública se aplica lo dispuesto en el primer párrafo del artículo 26 de la Ley.
- 67.3. El ejercicio por el titular de datos personales de sus derechos ante los bancos de datos personales de administración privada es de carácter gratuito, salvo lo establecido en normas especiales de la materia. En ningún caso el ejercicio de estos derechos implica ingreso adicional para el titular del banco de datos personales o responsable del tratamiento o encargado de tratamiento ante el cual se ejercen.
- 67.4. No se puede establecer como medios para el ejercicio de los derechos ninguno que implique el cobro de una tarifa adicional al solicitante o cualquier otro medio que suponga un costo excesivo en el caso de bancos de datos personales de entidades públicas.

#### **Artículo 68. Forma de la respuesta para el ejercicio del derecho**

- 68.1. El titular del banco de datos personales o responsable del tratamiento o encargado cuando corresponda, debe responder a la solicitud en la forma y plazo establecido en el presente Reglamento, con independencia de que figuren o no datos personales del titular de los mismos en los bancos de datos personales que administre.
- 68.2. La respuesta al titular de datos personales debe presentarse en forma clara, legible, comprensible y de fácil acceso.
- 68.3. En caso de ser necesario el empleo de claves o códigos, debe proporcionarse los significados correspondientes.
- 68.4. Corresponde al titular del banco de datos personales o responsable del tratamiento la prueba del cumplimiento del deber de respuesta, debiendo conservar los medios para hacerlo. Lo señalado también es de aplicación, en lo que fuera pertinente, para acreditar la realización de lo establecido en el segundo párrafo del artículo 20 de la Ley.

#### **Artículo 69. Plazos de respuesta para el ejercicio del derecho**

- 69.1. El plazo máximo de respuesta del titular del banco de datos personales o responsable o encargado del tratamiento cuando corresponda,

ante el ejercicio del derecho de información, es de ocho (08) días contados desde el día siguiente de la presentación de la solicitud.

69.2. El plazo máximo para la respuesta del titular del banco de datos personales o responsable o encargado del tratamiento cuando corresponda, ante el ejercicio del derecho de acceso es de veinte (20) días contados desde el día siguiente de la presentación de la solicitud por el titular de datos personales.

69.3. Tratándose del ejercicio de los otros derechos como los de rectificación, cancelación u oposición, el plazo máximo de respuesta del titular del banco de datos personales o responsable o encargado del tratamiento cuando corresponda, es de diez (10) días contados desde el día siguiente de la presentación de la solicitud.

## **Artículo 70. Requerimiento de información o documentación adicional**

70.1. En el caso que la información proporcionada en la solicitud sea insuficiente o errónea de forma que no permita su atención, el titular del banco de datos personales o responsable del tratamiento, cuando corresponda, puede requerir dentro de los siete (7) días siguientes de recibida la solicitud, información o documentación adicional al titular de los datos personales para atenderla.

70.2. En un plazo de diez (10) días de recibido el requerimiento, contado desde el día siguiente de la recepción del mismo, el titular de datos personales debe acompañar la documentación adicional que estime pertinente para fundamentar su solicitud. En caso contrario, se tiene por no presentada dicha solicitud.

70.3. El plazo aplicable para brindar la respuesta se suspende hasta que el titular de datos personales atienda el requerimiento de información o documentación adicional.

## **Artículo 71. Ampliación de los plazos**

71.1. Salvo el plazo establecido para el ejercicio del derecho de información, los plazos que correspondan para la respuesta o la atención de los demás derechos, pueden ser ampliados una sola vez, y por un plazo igual, como máximo, siempre y cuando las circunstancias lo justifiquen.

71.2. La justificación de la ampliación del plazo debe comunicarse al titular del dato personal dentro del plazo que se pretenda ampliar.

### **Artículo 72. Aplicación de disposiciones específicas**

Cuando las disposiciones aplicables a determinados bancos de datos personales, conforme a la legislación especial que los regule, establezcan un procedimiento específico para el ejercicio de los derechos regulados en el presente Título, son de aplicación tales disposiciones en cuanto ofrezcan iguales o mayores garantías al titular de los datos personales y no contravengan la Ley y el presente Reglamento.

### **Artículo 73. Denegación parcial o total ante el ejercicio de un derecho**

La respuesta total o parcialmente negativa por parte del titular del banco de datos personales o del responsable del tratamiento ante la solicitud de un derecho debe estar debidamente justificada e indicar al titular de datos personales que puede recurrir ante la Dirección de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de acción del hábeas data, conforme al artículo 24 de la Ley.

## **CAPÍTULO II DISPOSICIONES ESPECIALES**

### **Artículo 74. Derecho a la información**

- 74.1. El titular de datos personales tiene derecho, en vía de acceso, a que se le brinde toda la información señalada en el artículo 18 de la Ley. La respuesta debe contener los extremos previstos en el artículo 18 antes mencionado.
- 74.2. Para la respuesta al ejercicio del derecho a la información, es de aplicación, en lo que fuere pertinente, los artículos 77 y 78 del presente Reglamento.

### **Artículo 75. Derecho de acceso**

- 75.1. El titular de datos personales tiene derecho a que se le comunique de forma clara, expresa e indubitablemente con lenguaje sencillo lo siguiente:
1. Sus datos personales objeto de tratamiento;
  2. La forma en que sus datos personales fueron recopilados;
  3. Las razones que motivaron la recopilación de los datos personales;
  4. La indicación de a solicitud de quién se realizó la recopilación; y,

5. Las transferencias realizadas o que se prevén hacer con los datos personales.

75.2. Al amparo del derecho de acceso no se puede obtener información o documentación que, aunque corresponda al titular del dato personal, no se encuentre estrictamente comprendida dentro de los supuestos previstos en el párrafo 75.1.

## **Artículo 76. Portabilidad de datos personales**

76.1. Como manifestación del derecho de acceso, el titular del dato puede solicitar los datos personales sobre sí mismo, que haya facilitado a un responsable o titular de banco de datos, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable o titular de banco de datos personales cuando:

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

76.2. Al ejercer la portabilidad, el titular del dato tiene derecho a que sus datos se transmitan directamente de un responsable o titular del banco de datos a otro cuando sea técnicamente posible lo que no incluye su ejercicio imponga una carga financiera excesiva, técnica excesiva o irrazonable al responsable o encargado del tratamiento.

76.3. El titular del banco de datos personales o responsable del tratamiento que considere que no cuenta con la posibilidad técnica precitada debe poder acreditar tal situación ante un eventual requerimiento de la Autoridad Nacional de Protección de Datos Personales en el marco de un procedimiento trilateral de tutela, cuando así corresponda.

76.4. Los datos derivados, inferidos o contruidos a partir de datos personales pueden ser objeto de portabilidad siempre que el titular del banco de datos personales o el responsable del tratamiento así lo determinen. Se considera dato derivado, inferido o contruido aquel dato que ha sido sometido, por lo menos, a un proceso de personalización, categorización o elaboración de perfiles.

76.5. La portabilidad que este artículo reconoce no afecta negativamente a los derechos de terceros.

76.6. La portabilidad no se aplica al tratamiento necesario para el cumplimiento de las competencias o funciones conferidas a las entidades públicas.

76.7. La Autoridad Nacional de Protección de Datos Personales emite las disposiciones complementarias necesarias para la correcta aplicación de la portabilidad de datos personales.

### **Artículo 77. Medios para el cumplimiento del derecho de acceso**

77.1. La información correspondiente al derecho de acceso, a opción del titular de los datos personales, puede suministrarse por escrito, por medios electrónicos, telefónicos, de imagen u otro idóneo para tal fin.

77.2. El titular de los datos personales puede optar por alguna de las siguientes formas:

1. Visualización en sitio.
2. Escrito, copia, fotocopia o facsímil.
3. Transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la seguridad y recepción de la información.
4. Cualquier otra forma o medio que sea adecuado a la configuración o implantación material del banco de datos personales o a la naturaleza del tratamiento, establecido por el titular del banco de datos personales o responsable del tratamiento.

77.3. Cualquiera sea la forma a emplear, el acceso debe ser en formato claro, legible e inteligible, sin utilizar claves o códigos que requieran de dispositivos mecánicos para su adecuada comprensión y en su caso acompañada de una explicación. El acceso debe ser en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.

77.4. Sin perjuicio de lo anterior, con el objeto de usar los medios de comunicación más ecológicos disponibles en cada caso, el responsable del tratamiento puede acordar con el titular el uso de medios de reproducción de la información distintos a los establecidos en el presente Reglamento.

### **Artículo 78. Contenido de la información**

La información que, con ocasión del ejercicio del derecho de acceso, se ponga a disposición del titular de los datos personales, debe ser amplia y comprender lo indicado en el artículo 75 del presente Reglamento, aun cuando el requerimiento solo comprenda un aspecto de dicha información. El informe no puede revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

### **Artículo 79. Actualización**

79.1. Es derecho del titular de datos personales, en vía de rectificación, actualizar aquellos datos que han sido modificados a la fecha del ejercicio del derecho.

79.2. La solicitud de actualización debe señalar los datos personales a que se refiere, así como la modificación que haya de realizarse en ellos, acompañando la documentación que sustente la procedencia de la actualización solicitada.

### **Artículo 80. Rectificación**

80.1. Es derecho del titular de datos personales que se modifiquen los datos que resulten ser inexactos, erróneos o falsos.

80.2. La solicitud de rectificación deberá indicar a qué datos personales se refiere, así como la corrección que haya de realizarse en ellos, acompañando la documentación que sustente la procedencia de la rectificación solicitada.

### **Artículo 81. Inclusión**

81.1. Es derecho del titular de datos personales que, en vía de rectificación, sus datos sean incorporados a un banco de datos personales, así como que al tratamiento de sus datos personales se incorpore aquella información faltante que la hace incompleta, omitida o eliminada en atención a su relevancia para dicho tratamiento.

81.2. La solicitud de inclusión debe indicar los datos personales a que se refiere, así como la incorporación que haya de realizarse en ellos, acompañando la documentación que sustente la procedencia e interés fundado para el mismo.

## **Artículo 82. Supresión o cancelación**

- 82.1. El titular de los datos personales puede solicitar la supresión o cancelación de sus datos personales cuando estos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados, cuando hubiere vencido el plazo establecido para su tratamiento, cuando ha revocado su consentimiento para el tratamiento y en los demás casos en los que no están siendo tratados conforme a la Ley y al presente Reglamento.
- 82.2. La solicitud de supresión o cancelación puede referirse a todos los datos personales del titular contenidos en un banco de datos personales o solo a alguna parte de ellos.
- 82.3. Dentro de lo establecido por el artículo 20 de la Ley y el numeral 3 del artículo III del presente Reglamento, la presentación de la solicitud de supresión al responsable del tratamiento implica el cese en el tratamiento de los datos personales a partir de un bloqueo de los mismos en tanto se evalúe su posterior eliminación.

## **Artículo 83. Comunicación de la supresión o cancelación**

El titular del banco de datos personales o responsable del tratamiento debe documentar ante el titular de los datos personales haber cumplido con lo solicitado e indicar las transferencias de los datos suprimidos, identificando a quién o a quiénes fueron transferidos, así como la comunicación de la supresión correspondiente.

## **Artículo 84. Improcedencia de la supresión o cancelación**

La supresión no procede cuando los datos personales deban ser conservados en virtud de razones históricas, estadísticas o científicas de acuerdo con la legislación aplicable o, en su caso, en las relaciones contractuales entre el responsable y el titular de los datos personales, que justifiquen el tratamiento de los mismos.

## **Artículo 85. Protección en caso de denegatoria de supresión o cancelación**

Siempre que sea posible, según la naturaleza de las razones que sustenten la denegatoria prevista en el artículo precedente, se deben emplear medios de disociación o anonimización para continuar el tratamiento.

## **Artículo 86. Oposición**

- 86.1. El titular de datos personales tiene derecho a oponerse en cualquier momento, a efectos de que no se lleve a cabo el tratamiento de sus

datos personales o se cese en el mismo, cuando no hubiere prestado su consentimiento para su recopilación por haber sido tomados de fuente de acceso al público.

- 86.2. Aun cuando hubiera prestado consentimiento, el titular de datos personales tiene derecho a oponerse al tratamiento de sus datos, si acredita la existencia de motivos fundados y legítimos relativos a una concreta situación personal que justifiquen el ejercicio de este derecho.
- 86.3. En caso de que la oposición resulte justificada el titular del banco de datos personales o responsable de tratamiento debe proceder al cese del tratamiento que ha dado lugar a la oposición.
- 86.4. Salvo que exista relación contractual previa que sustente dicho tratamiento, cuando los datos personales son tratados para fines de publicidad y prospección comercial, incluido la elaboración de perfiles, el titular de datos personales puede ejercer su derecho de oposición, en cualquier momento, de acuerdo con los requisitos del presente Reglamento.
- 86.5. Cuando los datos personales son tratados en internet, el ejercicio de derecho de oposición puede incluir la desindexación de los datos personales.

## **Artículo 87. Derecho al tratamiento objetivo de datos personales**

- 87.1. 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 incluyendo aquellas que se basen únicamente en tratamientos automatizados destinados a evaluar, analizar o predecir, sin intervención humana, determinados aspectos personales del mismo, en particular, su rendimiento profesional, situación económica, estado de salud, orientación o identidad sexual, fiabilidad o comportamiento, entre otros, debiéndose considerar las excepciones contempladas en el artículo 23 de la Ley.
- 87.2. Para garantizar el ejercicio del derecho al tratamiento objetivo, de conformidad con lo establecido en el artículo 23 de la Ley, cuando se traten datos personales como parte de un proceso de toma de decisiones sin participación del titular de los datos personales, el titular del banco de datos personales o responsable del tratamiento debe informárselo a la brevedad posible, sin perjuicio de lo regulado para el ejercicio de los demás derechos en la Ley y el presente Reglamento.

### **CAPÍTULO III**

#### **PROCEDIMIENTO DE TUTELA**

##### **Artículo 88. Procedimiento de tutela directa**

- 88.1. El ejercicio de los derechos regulados por la Ley y el presente Reglamento se inicia con la solicitud que el titular de los datos personales debe dirigir directamente al titular del banco de datos personales o responsable del tratamiento.
- 88.2. El titular del banco de datos personales o responsable del tratamiento debe dar respuesta, en los plazos previstos en el presente Reglamento, expresando lo correspondiente a cada uno de los extremos de la solicitud. Transcurrido el plazo sin haber recibido la respuesta el solicitante puede considerar denegada su solicitud.
- 88.3. La denegatoria o la respuesta insatisfactoria habilitan al solicitante a iniciar el procedimiento administrativo ante la Dirección de Protección de Datos Personales.

##### **Artículo 89. Requisitos para el inicio del procedimiento trilateral de tutela**

El procedimiento trilateral de tutela de los derechos del titular de los datos personales se sujeta a lo dispuesto en el presente Reglamento y en la Ley N° 27444, Ley del Procedimiento Administrativo General u otra que la sustituya, en lo que le sea aplicable. Sin perjuicio de ello, la solicitud del titular de los datos personales debe cumplir con los siguientes requisitos:

1. La solicitud de inicio del procedimiento administrativo de tutela o reclamación debe contener los requisitos conforme a la Ley N° 27444, Ley de Procedimiento Administrativo General u otra que la sustituya.
2. El cargo de la solicitud que previamente envió al titular del banco de datos personales o responsable del tratamiento para obtener, directamente, la tutela de sus derechos.
3. El documento que contenga la respuesta del titular del banco de datos personales o responsable del tratamiento que, a su vez, contenga la denegatoria de su pedido o la respuesta que considere no satisfactoria, de haberla recibido.
4. Documentos que acrediten la afectación del derecho del titular del dato personal conforme a las condiciones reguladas en la Ley y el presente Reglamento, cuando así corresponda.

### **Artículo 90. Contestación a la reclamación**

Cuando la Dirección de Protección de Datos Personales haya admitido a trámite la reclamación, se corre traslado al reclamado y se otorga un plazo de quince (15) días sujetándose a lo dispuesto por el artículo 223 de la Ley N° 27444, Ley de Procedimiento Administrativo General u otra que la sustituya.

### **Artículo 91. Plazo para resolver**

- 91.1. El plazo máximo en que debe resolverse el procedimiento trilateral de tutela es de treinta (30) días, contado desde el día siguiente de recibida la contestación del reclamado o desde el vencimiento del plazo para formularla, y puede ampliarse hasta por un máximo de treinta (30) días adicionales, atendiendo a la complejidad del caso.
- 91.2. En caso se realice acciones de fiscalización a requerimiento de la Dirección de Protección de Datos Personales, se suspende el plazo previsto para resolver hasta que se reciba el informe correspondiente.

### **Artículo 92. Impugnación**

- 92.1. Contra la resolución del procedimiento trilateral de tutela solo procede el recurso de apelación conforme con lo establecido en el artículo 227 de la Ley N° 27444, Ley del Procedimiento Administrativo General u otro que la sustituya.
- 92.2. El recurso de apelación se presenta ante la Dirección de Protección de Datos Personales, la cual debe emitir la concesión del recurso de apelación. Posteriormente, la Dirección de Protección de Datos Personales debe elevar el expediente administrativo a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales en el plazo de dos (02) días de haberse notificado la concesión antes mencionada.
- 92.3. La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, dentro del plazo de quince (15) días de recibido el expediente administrativo, corre traslado de la apelación a la otra parte, la cual debe presentar su absolucón en un plazo máximo de quince (15) días.
- 92.4. Recibida la absolucón precitada o vencido el plazo establecido para tal efecto, el recurso de apelación es resuelto por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de

Datos Personales en un plazo máximo de treinta (30) días. Dicha resolución agota la vía administrativa.

#### **Artículo 93. Medidas cautelares**

Las medidas cautelares proceden en cualquier etapa del procedimiento trilateral de tutela ante la Dirección de Protección de Datos Personales, sujetándose a lo dispuesto en la Ley N° 27444, Ley del Procedimiento Administrativo General u otra que la sustituya, en lo que le sea aplicable.

#### **Artículo 94. Acciones de fiscalización**

Para mejor resolver, la Dirección de Protección de Datos Personales puede requerir a la Dirección de Fiscalización e Instrucción la realización de acciones de fiscalización, lo cual se debe efectuar dentro de los cinco (5) días siguientes de recibido tal requerimiento.

## **TÍTULO III INFRACCIONES Y SANCIONES**

### **CAPÍTULO I FISCALIZACIÓN**

#### **Artículo 95. Objeto**

La actividad de fiscalización tiene por objeto la realización de un conjunto de actos y diligencias de investigación, supervisión, control o inspección sobre el cumplimiento de las obligaciones en materia de protección de datos personales, prohibiciones y otras limitaciones exigibles a los administrados que realizan tratamiento de datos personales, derivados de una norma legal o reglamentaria, contratos con el Estado u otra fuente jurídica, bajo un enfoque de cumplimiento normativo, de prevención del riesgo, de gestión del riesgo y tutela de los bienes jurídicos protegidos.

#### **Artículo 96. Inicio de la actividad de fiscalización**

96.1. La actividad de fiscalización se inicia siempre de oficio como consecuencia de:

1. Iniciativa directa de la Dirección de Fiscalización e Instrucción; o,
2. Por denuncia de cualquier entidad pública, persona natural o jurídica.

96.2. En todos los casos, la Dirección de Fiscalización e Instrucción requiere al titular del banco de datos personales, al encargado o a quien resulte responsable, información relativa al tratamiento de datos personales o la documentación necesaria.

96.3. Para efectos de la actividad fiscalizadora, la Dirección de Fiscalización e Instrucción está facultada para ejecutar las actividades dispuestas en el artículo 228-B de la Ley N° 27444, Ley del Procedimiento Administrativo General u otro que la sustituya.

### **Artículo 97. Tipos de actividad de fiscalización**

La actividad de fiscalización se clasifica en:

1. **Presencial:** Acción de fiscalización que se realiza fuera de las sedes de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en presencia del titular del banco de datos personales, el encargado o quien resulte responsable o sus representantes.
2. **En gabinete:** Acción de fiscalización que se realiza desde las sedes de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales y que implica el acceso y evaluación a través de medios digitales a las actividades que realiza el titular del banco de datos personales, el encargado o quien resulte responsable del tratamiento de datos personales.

### **Artículo 98. Reconducción**

En caso de que, de la denuncia presentada, se advierta que no se dirige a los objetivos de una fiscalización, sino a la tutela de derechos, se reconduce la misma a una reclamación en el marco de un procedimiento trilateral de tutela.

### **Artículo 99. Fe pública**

En el ejercicio de las actividades de fiscalización, el personal de la Dirección de Fiscalización e Instrucción está dotado de fe pública para constatar la veracidad de los hechos en relación con los trámites a su cargo.

### **Artículo 100. Requisitos de la denuncia**

La denuncia debe indicar lo siguiente:

1. Nombre del denunciante y el domicilio para efectos de recibir las notificaciones conforme con lo señalado en el artículo 20 de la Ley N° 27444.

2. Relación de los hechos en los que basa su denuncia y los documentos que la sustenten.
3. Nombre y domicilio del denunciado o, en su caso, datos para su ubicación.

### **Artículo 101. Forma de la denuncia**

- 101.1. La denuncia puede presentarse en soporte físico o según los formularios publicados en el Portal Institucional del Ministerio de Justicia y Derechos Humanos.
- 101.2. Cuando la denuncia se presente por medios digitales, a través del sistema que establezca la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, se entiende que se acepta que las notificaciones sean efectuadas por dicho sistema o a través de otros medios electrónicos generados por este.
- 101.3. El denunciante puede solicitar que se mantenga la reserva de su identidad.

### **Artículo 102. Requerimiento de información**

Cuando se formule denuncia, la Dirección de Fiscalización e Instrucción puede solicitar la documentación que estime oportuna al denunciante para el desarrollo de la fiscalización.

### **Artículo 103. Acción de fiscalización presencial**

- 103.1. La acción de fiscalización presencial se realiza sin previo aviso, salvo en determinadas circunstancias y para garantizar la eficacia de la fiscalización. La Dirección de Fiscalización e Instrucción, cuando estime conveniente, en un plazo razonable, comunica al fiscalizado la fecha y hora en que se efectúa la acción de fiscalización.
- 103.2. La acción de fiscalización presencial puede incluir diversas visitas para obtener los elementos de convicción necesarios. Luego de la primera visita inopinada, de ser el caso, las siguientes visitas se notifican previamente al administrado fiscalizado.
- 103.3. Las visitas de fiscalización requieren el levantamiento del acta correspondiente, en la que se deja constancia de las actuaciones practicadas durante dicha visita. Dicha acta debe ser suscrita por el personal fiscalizador, el administrado o el personal que participó en la

diligencia. En caso estos últimos, se nieguen a recibir o firmar el acta, se deja constancia de ello en el acta, no afectando su validez. La firma del fiscalizado no supone su conformidad con el contenido, sino tan sólo su participación y la recepción de la misma.

103.4. El acta se elabora por duplicado y se entrega una copia al administrado. El acta puede incluir la manifestación que los participantes consideren que conviene a su derecho.

103.5. En el caso no se lleve a cabo la visita de fiscalización por obstrucción y obstaculización del administrado o de su personal, se elabora el acta respectiva dejando constancia del motivo que impidió se lleve a cabo.

#### **Artículo 104. Identificación del personal fiscalizador**

104.1. Al iniciar la visita, el personal fiscalizador debe exhibir credencial vigente con fotografía, expedida por la Dirección de Fiscalización e Instrucción que lo acredite como tal.

104.2. El personal que lleve a cabo las visitas de fiscalización debe estar provisto de orden escrita con firma autógrafa del funcionario, de la que deja copia, con cargo, a la persona que atendió la visita.

104.3. En la orden debe precisarse el lugar o los lugares en donde se encuentra la entidad pública o privada o la persona natural que se fiscaliza, o donde se encuentren los bancos de datos personales objeto de fiscalización, el objeto genérico de la visita y las disposiciones legales que lo fundamenten.

#### **Artículo 105. Contenido de las actas de fiscalización**

En las actas de fiscalización se debe hacer constar:

1. Nombre, denominación o razón social del fiscalizado.
2. Hora, día, mes y año en que se inicie y concluya la fiscalización.
3. Los datos que identifiquen plenamente el lugar donde se realizó la fiscalización, tales como calle, avenida, pasaje, número, distrito, código postal, la entidad pública o privada en que se encuentre ubicado el lugar en que se practicó la fiscalización, así como el número telefónico u otra forma de comunicación disponible con el fiscalizado.

4. Tipo de acción de fiscalización.
5. Número y fecha de la orden de fiscalización que la motivó.
6. Nombre y cargo de la persona que atendió a los fiscalizadores.
7. Datos y detalles relativos a la actuación.
8. Declaración del fiscalizado si lo solicitase.
9. Requerimiento de información efectuado y el plazo otorgado para su entrega, de ser el caso.
10. Nombre y firma de quienes intervinieron en la fiscalización, incluyendo quienes la hubieran llevado a cabo.

#### **Artículo 106. Obstrucción a la fiscalización**

Si el fiscalizado se niega directamente a colaborar u observa una conducta obstructiva, demorando injustificadamente su colaboración, planteando cuestionamientos no razonables a la labor fiscalizadora, desatendiendo las indicaciones de los fiscalizadores o cualquier otra conducta similar o equivalente, debe dejarse constancia de ello en el acta, con precisión del acto o los actos obstructivos y de su reiteración, de ser el caso.

#### **Artículo 107. Observaciones en el acto de fiscalización o posteriores**

Sin perjuicio de que los fiscalizados puedan formular observaciones en el acto de la fiscalización y manifestar lo que a su derecho convenga en relación con los hechos contenidos en el acta, también pueden hacerlo por escrito dentro del término de los cinco (5) días siguientes a la fecha de realización de la acción de fiscalización.

#### **Artículo 108. Informe de fiscalización**

- 108.1. La fiscalización concluye con la emisión de un informe que puede contener:
  1. Constancia de conformidad de la actividad desarrollada por el administrado.
  2. La recomendación de mejoras o correcciones de la actividad desarrollada por el administrado.
  3. La advertencia de la existencia de incumplimientos no susceptibles de ameritar la determinación de responsabilidades administrativas.

4. La recomendación del inicio de un procedimiento con el fin de determinar las responsabilidades administrativas que correspondan.
  5. Disposición de adopción de medidas correctivas, bajo apercibimiento de recomendar inicio de procedimiento sancionador.
- 108.2. El informe de la conclusión de la fiscalización debe ser elaborado en un plazo máximo de noventa (90) días, este plazo se inicia desde la fecha en que la Dirección de Fiscalización e Instrucción recibe la denuncia o da inicio de oficio a las actuaciones de fiscalización. El plazo establecido puede ser ampliado por una sola vez y hasta por un periodo de cuarenta y cinco (45) días, por decisión motivada, atendiendo a la complejidad de la materia fiscalizada.

### **Artículo 109. Improcedencia de medios de impugnación**

En contra de cualquiera de las formas de conclusión de la actividad de fiscalización que expide la Dirección de Fiscalización e Instrucción no procede la interposición de recurso alguno, la contradicción de su contenido y cualquier forma de defensa respecto de él se hacen valer en el trámite del procedimiento administrativo sancionador, de ser el caso.

## **CAPÍTULO II PROCEDIMIENTO SANCIONADOR**

### **Artículo 110. Autoridades del procedimiento sancionador**

Para efectos de la aplicación de las normas sobre el procedimiento administrativo sancionador establecido en la Ley, las autoridades son las siguientes:

1. La Dirección de Fiscalización e Instrucción es competente para conducir y desarrollar la fase de investigación y es responsable de llevar a cabo las actuaciones necesarias para determinar las circunstancias de la comisión, de actuación de pruebas, imputar cargos de los actos contrarios a lo establecido en la Ley y el presente Reglamento, y emitir el Informe Final de Instrucción, según corresponda.
2. La Dirección de Protección de Datos Personales es competente para resolver en primera instancia sobre la existencia de infracción e imposición de sanciones y de dictar medidas cautelares y correctivas tendientes a la protección de los datos personales, así como resolver el recurso de reconsideración interpuesto contra sus resoluciones, según corresponda.

3. La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales ejerce funciones como segunda y última instancia administrativa del procedimiento administrativo sancionador y su decisión agota la vía administrativa.

### **Artículo 111. Inicio del procedimiento sancionador**

- 111.1. El procedimiento sancionador se inicia con la notificación de la resolución de imputación de cargos a los administrados, la cual es realizada por la Dirección de Fiscalización e Instrucción, de conformidad con lo dispuesto en el numeral 3 del artículo 234 de la Ley N° 27444, Ley de Procedimiento Administrativo General u otro que la sustituya.
- 111.2. El denunciante puede interponer recurso de apelación contra la resolución que declara el archivo o la improcedencia total o parcial de su denuncia.

### **Artículo 112. Contenido de la resolución de inicio del procedimiento sancionador**

- 112.1. La Dirección de Fiscalización e Instrucción notifica la resolución de imputación de cargos que contiene lo siguiente:
  1. La identificación de la autoridad competente de imponer la sanción, identificando la norma que otorga dicha competencia.
  2. Los hechos que motivan el inicio del procedimiento administrativo sancionador, que incluye la manifestación de los hechos que se atribuyen al administrado y de la calificación de las infracciones que tales hechos puedan constituir.
  3. La identificación del administrado a quien se le abre procedimiento.
  4. La sanción o sanciones, que en su caso se pudieran imponer.
  5. El plazo para presentar los descargos y pruebas.
  6. Las normas que tipifican los actos u omisiones como infracción administrativa.
- 112.2. A la notificación de la resolución de imputación de cargos se le anexa el Informe de fiscalización.

### **Artículo 113. Presentación de descargos y pruebas**

- 113.1. El administrado en un plazo máximo de quince (15) días, contado a partir del día siguiente de la notificación correspondiente puede presentar su descargo, en el cual puede pronunciarse concretamente respecto de cada uno de los hechos que se le imputan de manera expresa, afirmándolos, negándolos, señalando que los ignora por no ser propios o exponiendo como ocurrieron, según sea el caso. Asimismo, puede presentar los medios probatorios correspondientes.
- 113.2. En los descargos, el administrado puede reconocer su responsabilidad de forma expresa y por escrito, cuya evaluación es considerada como un supuesto de atenuación de responsabilidad para efectos del cálculo de la sanción.

### **Artículo 114. Actuaciones para la instrucción de los hechos**

Vencido el plazo de los quince (15) días para la presentación del descargo, con o sin él, la Dirección de Fiscalización e Instrucción realiza de oficio todas las actuaciones necesarias para el examen de los hechos y puede disponer visitas de fiscalización o de presentación de medios probatorios, si no las hubiera realizado antes, con la finalidad de recabar la información que sea necesaria o relevante para determinar, en su caso, la existencia de infracciones susceptibles de sanción.

### **Artículo 115. Informe Final de Instrucción**

- 115.1. La Dirección de Fiscalización e Instrucción emite el Informe Final de Instrucción, en un plazo máximo de cincuenta (50) días, este plazo inicia desde la fecha en que se notifica la resolución de inicio del procedimiento sancionador. El plazo establecido puede ser ampliado por una vez y hasta por un periodo de cincuenta (50) días. En el informe de instrucción se determina de forma motivada las conductas que se consideren constitutivas de infracción, la norma que prevé la imposición de sanción, la propuesta de sanción que corresponda o el archivo del procedimiento, según sea el caso.
- 115.2. Si luego de la evaluación correspondiente, la Dirección de Fiscalización e Instrucción concluye que no existen infracciones, debe dejar constancia de ello en el Informe Final de Instrucción, en el que recomienda a la Dirección de Protección de Datos Personales se declare el archivo del procedimiento administrativo sancionador.
- 115.3. Cuando se determine la existencia de responsabilidad administrativa

de una o más infracciones, la Dirección de Fiscalización e Instrucción notifica el informe al administrado otorgándole un plazo de cinco (5) días, contado desde el día siguiente de la notificación, para que presente sus descargos ante la Dirección de Protección de Datos Personales. El informe no constituye un acto impugnabile.

### **Artículo 116. Resolución del procedimiento sancionador**

- 116.1. La resolución que emite la Dirección de Protección de Datos Personales, puede acoger o no la recomendación del Informe Final de Instrucción, y debe encontrarse debidamente motivada y pronunciarse respecto de los descargos y a los hechos imputados a fin de determinar la responsabilidad del administrado, la sanción aplicable y las medidas correctivas, de ser el caso.
- 116.2. La resolución del procedimiento administrativo sancionador es notificada a las partes del procedimiento, así como al denunciante cuando el procedimiento se haya originado por alguna acción de fiscalización debido a una denuncia.

### **Artículo 117. Concurso de infracciones**

- 117.1. Cuando una misma conducta o hecho califique como más de una infracción se aplica la multa determinada para la infracción de mayor gravedad, conforme al numeral 6 del artículo 230 de la Ley N° 27444, Ley del Procedimiento Administrativo General u otro que la sustituya.
- 117.2. Cuando varias conductas o hechos califiquen como infracciones independientes, se aplica la suma de las multas determinadas previamente y de manera individualizada, hasta un máximo del doble de la sanción aplicable por la infracción más grave.

### **Artículo 118. Impugnación**

- 118.1. El recurso de reconsideración se debe sustentar en nueva prueba y es resuelto por la Dirección de Protección de Datos Personales en un plazo que no excede de los quince (15) días. En caso de que la Dirección de Protección de Datos Personales determine que el recurso de reconsideración es improcedente por no sustentarse en prueba nueva, debe encauzarlo como recurso de apelación, según corresponda.

- 118.2. El recurso de apelación se presenta ante el mismo órgano que expidió la resolución que se apela, el que lo eleva a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales junto con el expediente. El recurso de apelación debe ser resuelto en un plazo no mayor de treinta (30) días contado a partir de la recepción del expediente administrativo.
- 118.3. Las resoluciones emitidas por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales que resuelven los recursos de apelación agotan la vía administrativa. No cabe interposición de recurso alguno en la vía administrativa y únicamente puede presentarse demanda contenciosa administrativa según la legislación de la materia.

### **Artículo 119. Audiencia de informe oral**

- 119.1. En el marco de los procedimientos de su competencia, la Dirección de Protección de Datos Personales y la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales pueden, por decisión propia o a solicitud de parte y en atención a su evaluación del caso concreto, programar la realización de la audiencia de informe oral.
- 119.2. La audiencia de informe oral puede ser presencial o virtual, según determine el órgano competente en atención a las circunstancias de cada caso en concreto. En caso de ser virtual, se debe dejar registrada por el órgano a cargo de la audiencia, en video, audio o mediante cualquier otro medio que permita dejar constancia de su realización. Una copia es archivada en el expediente administrativo correspondiente.
- 119.3. En la audiencia solo pueden participar y hacer uso de la palabra los representantes o apoderados de los administrados, quienes deben identificarse como tales antes del inicio de la audiencia de informe oral.

### **Artículo 120. Sobre la confidencialidad de la información**

- 120.1. Se considera confidencial aquella información que posee dicha naturaleza conforme al régimen previsto en la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, que haya sido presentada por las partes o terceros en el marco de un procedimiento de competencia de la Autoridad Nacional de Protección de Datos Personales, o generada por la misma en el trámite de la investigación propia del ejercicio de la potestad sancionadora.

- 120.2. De manera enunciativa y no limitativa, se considera información confidencial el secreto bancario, comercial, industrial, tributario o bursátil; así como aquella que afecte la intimidad personal y familiar.
- 120.3. La información debe ser de uso exclusivo de los servidores públicos encargados del trámite del procedimiento. Dicha información no debe ser puesta en conocimiento de las demás partes del procedimiento ni de terceros; por lo cual, la Autoridad Nacional de Protección de Datos Personales puede aplicar procedimientos de disociación y/o anonimización, según corresponda.

### **CAPÍTULO III MEDIDAS ADMINISTRATIVAS**

#### **Artículo 121. Medidas de carácter provisional y cautelares**

- 121.1. Una vez iniciado el procedimiento sancionador, la Dirección de Protección de Datos Personales, a solicitud de la Dirección de Fiscalización e Instrucción, puede disponer la adopción de medidas de carácter provisional que aseguren la eficacia de la resolución final que pudiera recaer en el referido procedimiento, con observancia de las normas aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General u otra que la sustituya.
- 121.2. La Dirección de Protección de Datos Personales, mediante decisión motivada, puede dictar medida cautelar, sustentándose en la verosimilitud de la existencia de una infracción administrativa, peligro en la demora y la razonabilidad de la medida, a fin de salvaguardar el derecho de protección de datos personales.

#### **Artículo 122. Medidas correctivas**

- 122.1. La medida correctiva es la medida dictada por la Dirección de Protección de Datos Personales, sin perjuicio de la sanción administrativa que corresponda, destinada a revertir, corregir o disminuir, en la medida de lo posible, el efecto nocivo que la conducta infractora hubiera producido al titular del dato personal.
- 122.2. La Dirección de Protección de Datos Personales puede dictar las siguientes medidas correctivas:

1. Cese de tratamiento de datos personales obtenidos de forma desproporcional y/o sin consentimiento.
2. Eliminación de datos que fueron obtenidos sin el consentimiento del titular del dato personal.
3. Acciones para revertir o disminuir en lo posible el efecto nocivo de la conducta infractora sobre el titular del dato personal.
4. Atención inmediata del derecho solicitado por el titular del dato personal.
5. Otras que se deriven del ordenamiento vigente en materia de protección de datos personales.

## **CAPÍTULO IV SANCIONES**

### **Artículo 123. Graduación del monto de la sanción administrativa de multa**

- 123.1. Para graduar la sanción a imponerse en el caso concreto debe observarse el principio de razonabilidad de la potestad sancionadora reconocido en el numeral 3 del artículo 230 de la Ley N° 27444, Ley del Procedimiento Administrativo General u otra norma que la sustituya.
- 123.2. La determinación de las multas se realiza conforme con lo establecido en la Metodología para el cálculo de multas, aprobada por Resolución Ministerial N° 0326-2020-JUS o norma que la sustituya.

### **Artículo 124. Límite al monto de la sanción administrativa de multa**

- 124.1. Conforme a lo establecido en el segundo párrafo del artículo 39 de la Ley, el administrado puede acreditar en el descargo de la imputación de cargos el monto de ingreso bruto anual que percibió el año anterior a la fecha en la que cometió la infracción, a través de declaraciones juradas de la Superintendencia Nacional de Aduanas y de Administración Tributaria, estados financieros u otro documento de naturaleza similar.
- 124.2. En caso el administrado acredite que no esté percibiendo ingresos, remite a la Dirección de Fiscalización e Instrucción la información necesaria para que se efectúe la estimación de los ingresos que proyecta percibir.

### **Artículo 125. Atenuantes de responsabilidad administrativa**

Se consideran atenuantes de responsabilidad las siguientes:

- 125.1. El reconocimiento expreso y por escrito de la infracción cometida, el cual debe ser efectuado de manera clara, precisa y sin ambigüedades o contradicciones.
- 125.2. La colaboración con la Autoridad Nacional y la adopción medidas de enmienda que permiten mitigar los efectos de la conducta infractora, después de la notificación de imputación de cargos. Tales medidas deben ser debidamente acreditadas.
- 125.3. La implementación debidamente acreditada y de manera previa al inicio del procedimiento administrativo sancionador del Código de Conducta, conforme a los requisitos regulados en el presente Reglamento.
- 125.4. La implementación debidamente acreditada y de manera previa al inicio del procedimiento administrativo sancionador de la Evaluación de impacto relativa a la protección de datos personales respecto del tratamiento cuestionado, conforme a los requisitos regulados en el presente Reglamento.

### **Artículo 126. Mora en el pago de las multas**

- 126.1. El administrado que no realiza el pago oportuno de las multas incurre en mora automática, en consecuencia, el monto de las multas impagas devenga interés moratorio que se aplica diariamente desde el día siguiente de la fecha del vencimiento del plazo de cancelación de la multa hasta la fecha de pago inclusive, multiplicando el monto de la multa impaga por la Tasa de Interés Moratoria (TIM) diaria vigente.
- 126.2. La Tasa de Interés Moratoria (TIM) diaria vigente resulta de dividir la Tasa de Interés Moratoria (TIM) vigente entre treinta (30).

### **Artículo 127. Beneficio de pronto pago de la multa**

- 127.1. El administrado puede acogerse al beneficio de pronto pago mediante la cancelación de la multa dentro del plazo establecido por la Dirección de Protección de Datos Personales en la resolución emitida en primera instancia, siempre que no se interponga recurso de apelación contra tal resolución y, en consecuencia, esta quede consentida.

127.2. El beneficio del pronto pago corresponde a una reducción del 40% respecto al importe de la multa impuesta.

127.3. Para que surta efecto el beneficio de pronto pago se deben cumplir las condiciones mencionadas en el presente Reglamento y, adicionalmente, se debe comunicar tal circunstancia a la Dirección de Protección de Datos Personales adjuntando el comprobante del depósito bancario correspondiente.

### **Artículo 128. Ejecución coactiva de la multa**

La ejecución de la sanción de multa se rige por la ley de la materia referida al procedimiento de ejecución coactiva.

### **Artículo 129. Registro de sanciones, medidas cautelares y correctivas**

La Dirección de Protección de Datos Personales tiene a su cargo el Registro Nacional de Protección de Datos Personales, en el cual se inscriben los sancionados por incumplimiento de la Ley y el presente Reglamento, las medidas cautelares y medidas correctivas, lo cual es publicado en la sede digital del Ministerio de Justicia y Derechos Humanos, ubicada en la Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano (Gob.pe).

### **Artículo 130. Aplicación de multas coercitivas**

130.1. En caso de incumplimiento de medidas correctivas y medidas cautelares, la Dirección de Protección de Datos Personales impone multas coercitivas, de manera automática y sin necesidad de requerimiento previo, de acuerdo con la siguiente graduación:

1. Por infracciones leves, la multa coercitiva debe ser de hasta dos (2) Unidades Impositivas Tributarias.
2. Por infracciones graves, la multa coercitiva debe ser no menor de dos (2) hasta seis (6) Unidades Impositivas Tributarias.
3. Por infracciones muy graves, la multa coercitiva debe ser no menor de seis (6) hasta diez (10) Unidades Impositivas Tributarias.

130.2. En caso de persistir en el incumplimiento de cualquiera de los mandatos a los que se refiere el párrafo 130.1, se puede imponer una nueva multa coercitiva, duplicando sucesivamente el monto de la última multa impuesta hasta el límite de cien (100) Unidades Impositivas Tributarias (UIT).

- 130.3. La multa que corresponda debe ser pagada dentro del plazo de cinco (5) días, vencido el cual se ordena su cobranza coactiva.
- 130.4. Contra la imposición de una multa coercitiva no procede la interposición de recurso impugnativo.
- 130.5. La Autoridad Nacional de Protección de Datos Personales aprueba las disposiciones necesarias para regular la aplicación de las multas coercitivas.

## **CAPÍTULO V INFRACCIONES**

### **Artículo 131. Infracciones**

Las infracciones a la Ley o al presente Reglamento se califican como leves, graves y muy graves, y se sancionan con multa de acuerdo con el artículo 39 de la citada Ley.

### **Artículo 132. Infracciones leves**

Son infracciones leves, las siguientes:

1. Realizar tratamiento de datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos.
2. No modificar o rectificar los datos personales objeto de tratamiento cuando se tenga conocimiento de su carácter inexacto o incompleto.
3. No suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios, pertinentes o adecuados para la finalidad para la cual fueron recopilados o cuando hubiese vencido el plazo para su tratamiento. En estos casos, no se configura la infracción cuando medie procedimiento de anonimización o disociación.
4. No inscribir o actualizar en el Registro Nacional de Protección de Datos Personales los actos establecidos en el artículo 34 de la Ley.
5. 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.

6. Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia.
7. Atender fuera de plazo el ejercicio material de los derechos del titular de datos personales, cuando legalmente proceda.
8. No comunicar el flujo transfronterizo de datos personales a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales para su inscripción en el Registro Nacional de Protección de Datos Personales.
9. No designar al Oficial de Datos Personales, cuando así corresponda.

### **Artículo 133. Infracciones graves**

Son infracciones graves, las siguientes:

1. No atender, impedir u obstaculizar el ejercicio material de los derechos del titular de datos personales.
2. No cumplir con el deber de informar o informar de forma incompleta de tres a más condiciones del tratamiento de los datos personales a los titulares de datos personales, de acuerdo con lo establecido en el artículo 18 de la Ley.
3. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la Ley y su Reglamento.
4. Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia, y generando con ello un perjuicio al titular del dato personal o una exposición no autorizada de sus datos personales.
5. Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia.
6. Realizar tratamiento de datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos.
7. Utilizar los datos personales obtenidos lícitamente para finalidades

distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación.

8. Negar o demorar injustificadamente a la Autoridad Nacional de Protección de Datos Personales el ingreso a las instalaciones objeto de la fiscalización.
9. Negarse injustificadamente a proporcionar a la Autoridad Nacional de Protección de Datos Personales la información o la documentación relativa al tratamiento de datos personales que esta le requiera en el marco de una fiscalización o procedimiento administrativo en curso.
10. Obstruir el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales.
11. Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley.
12. No comunicar a la Autoridad Nacional de Protección de Datos Personales un incidente de seguridad de datos personales cuando así corresponda conforme a lo previsto en el artículo 34 del presente Reglamento.
13. 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.

#### **Artículo 134. Infracciones muy graves**

Son infracciones muy graves, las siguientes:

1. Realizar tratamiento de datos personales mediante medios fraudulentos, desleales o ilícitos.
2. Suministrar documentos o información falsa o inexacta a la Autoridad Nacional de Protección de Datos Personales.
3. No cumplir con las medidas correctivas o medidas cautelares ordenadas en un procedimiento trilateral de tutela, pese al apercibimiento efectuado previamente.
4. 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.

### **Artículo 135. Reincidencia**

- 135.1. Se considera que existe reincidencia en la comisión de una infracción, cuando se cometen los mismos actos u omisiones que dieron lugar a una infracción anterior, siempre que el tiempo transcurrido entre la fecha de la resolución de sanción de los actos u omisiones que dieron lugar a la infracción inmediata anterior quede firme, o haya causado estado, y la fecha de realización de los mismos actos u omisiones que dan lugar a la comisión de una nueva infracción sea igual o menor a un (1) año.
- 135.2. Para efectos de la reincidencia se consideran también las infracciones que no fueron sancionadas debido a un concurso de infracciones según el numeral 6 del artículo 230 de la Ley N° 27444, Ley de Procedimiento Administrativo General u otra que la sustituya.
- 135.3. La reincidencia es considerada como un factor agravante al momento de la determinación de la multa.

## **DISPOSICIONES COMPLEMENTARIAS FINALES**

### **Primera. Vigencia**

El presente Reglamento entra en vigencia a partir de los 120 días calendario siguientes de su publicación en el diario oficial El Peruano.

Las disposiciones previstas para el titular del banco de datos personales, responsable o encargado de tratamiento que se encuentren comprendidos en los supuestos previstos en los numerales 2 y 3 del párrafo 37.1 del artículo 37 del presente Reglamento, referidas a la designación del Oficial de datos personales, entran en vigencia de modo progresivo, de acuerdo al siguiente cronograma:

Titular del banco de datos personales, responsable o encargado de tratamiento de datos personales	Fecha de entrada en vigencia y carácter obligatorio
Para empresas con ventas anuales superiores a 2300 UIT	1 año después de la fecha de publicación del presente Reglamento
Para empresas medianas con ventas anuales superiores a 1700 UIT y hasta el monto máximo de 2300 UIT	2 años después de la fecha de publicación del presente Reglamento
Para pequeñas empresas con ventas anuales superiores a 150 UIT y hasta el monto máximo de 1700 UIT	3 años después de la fecha de publicación del presente Reglamento
Para microempresas con ventas anuales hasta el monto máximo de 150 UIT y otros equivalentes	4 años después de la fecha de publicación del presente Reglamento

La disposición prevista en el artículo 76, referida la Portabilidad de Datos Personales, surte efecto a partir de los 6 meses posteriores a la entrada en vigencia del presente Reglamento.

### **Segunda. Normas complementarias**

La Autoridad Nacional de Protección de Datos Personales emite las normas complementarias para la aplicación del presente Reglamento.

La Autoridad Nacional de Protección de Datos Personales emite disposición o lineamiento referido a la obligación de notificar incidente de seguridad de datos personales, para la imputación e imposición de sanción como consecuencia de un incumplimiento en el marco de un procedimiento administrativo sancionador.

### **Tercera. Interoperabilidad entre entidades públicas**

La definición, los alcances y el contenido de la interoperabilidad, así como los lineamientos para su aplicación y funcionamiento en concordancia con las normas de protección de datos personales, son competencia de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en su calidad de Ente Rector del Sistema Nacional de Transformación Digital.

La interoperabilidad entre entidades se regula, en cuanto a su implementación, de acuerdo a las disposiciones establecidas en la Ley de Gobierno Digital y su Reglamento, aprobados mediante Decreto Legislativo N° 1412 y Decreto Supremo N° 029-2021-PCM, respectivamente; y, en el marco de lo dispuesto por el párrafo 76.2 del artículo 76 de la Ley N° 27444, Ley del Procedimiento Administrativo General u otra que la sustituya.

#### **Cuarta. Plataforma “Yo cuido mis datos personales”**

Créase la plataforma digital “Yo cuido mis datos personales” que tiene como finalidad que la Autoridad Nacional de Protección de Datos Personales brinde atención al ciudadano, en vía de reclamación, cuando no se atiende, se atiende parcialmente o se deniegue el ejercicio de los derechos establecidos en la Ley N° 29733, Ley de Protección de Datos Personales, así como para la presentación de denuncias de parte por presuntos actos contrarios a la normativa de protección de datos personales.

La plataforma es administrada por la Autoridad Nacional de Protección de Datos Personales.

La Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros pone a disposición de la Autoridad Nacional de Protección de Datos Personales las capacidades de la Plataforma Nacional de Gobierno Digital (PNGD) para la implementación de la plataforma digital “Yo cuido mis datos personales”.

#### **Quinta. Competencias y promoción de la cultura de protección de datos personales en el uso de servicios digitales**

El Ministerio de Justicia y Derechos Humanos a través de la Autoridad Nacional de Protección de Datos Personales, en coordinación con la Secretaría de Gobierno y Transformación Digital, en su calidad de ente rector, promueven acciones para el desarrollo de la cultura de protección de datos personales de los ciudadanos en el entorno digital para el acceso y uso de servicios digitales.

#### **Sexta. Absolución de consultas en materia de protección de datos personales**

La Autoridad Nacional de Protección de Datos personales absuelve consultas sobre protección de datos personales y el sentido de las normas vigentes, en los términos previstos en el numeral 10 del artículo 33 de la Ley en el plazo de 30 días.

## **DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS**

### **PRIMERA. Conductas infractoras cometidas previo a la entrada en vigencia del presente Reglamento**

Las conductas infractoras cometidas previo a la entrada en vigencia del presente Reglamento, conforme a lo establecido en la Primera Disposición Complementaria Final, se rigen por lo dispuesto por el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales aprobada por el Decreto Supremo 003-2013-JUS.

### **SEGUNDA. Actividades de fiscalización y procedimientos en trámite**

Las actividades de fiscalización y los procedimientos administrativos iniciados a la entrada en vigencia del presente Reglamento y que se encuentren en trámite se rigen conforme a las disposiciones del Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales aprobada por Decreto Supremo 003-2013-JUS.



---

**CRITERIOS INTERPRETATIVOS  
AUTORIDAD NACIONAL DE PROTECCIÓN  
DE DATOS PERSONALES - ANPD**

---



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

## **TRATAMIENTO DE DATOS PERSONALES DE ESPECIAL INTERÉS: PROSPECCIÓN COMERCIAL- SPAM**

- Pronunciamiento : Opinión Consultiva N° 01-2022-DGTAIPD
- Asunto : Sobre el alcance de la autorización de primer contacto para solicitar el consentimiento para el uso de datos con fines de publicidad
- Entidad Consultante : Dirección de Fiscalización del Instituto Nacional de Defensa de la Competencia y de la Protección de la propiedad Intelectual - INDECOPI
- Criterio :
  1. Un responsable de tratamiento que obtenga datos de forma lícita, puede utilizarlos una sola vez para solicitar el consentimiento para tratamiento de datos con fines de publicidad y/o prospección comercial de forma general y no por tipo de producto o servicio.
  2. El proveedor es el responsable del tratamiento de los datos personales en el proceso de prospección de sus productos y/o servicios, sea cual fuere el medio utilizado, siendo las empresas contratadas para contactar al titular del dato personal las que cumplen el rol de encargadas, debido a que dicho proceso se lleva a cabo para satisfacer el interés comercial del proveedor; con ello, decide sobre el desarrollo de las actividades de dicho tratamiento y la finalidad, relacionada esta con dicho interés.
  3. El proveedor debe ejercer diligentemente el control sobre las actividades de prospección realizadas por terceros, a fin de garantizar la licitud y evitar cualquier daño ilícito o riesgo a los derechos de las personas. Para ello, debe establecer canales para la atención de derechos ARCO dirigidos por los receptores, mantener un contacto regular y permanente con las empresas que efectúan las comunicaciones, y asegurar que estas informen de forma inmediata cualquier denegatoria o falta de consentimiento, especialmente en el caso de llamadas telefónicas, en las que dicha voluntad suele manifestarse de forma directa e inmediata. Asimismo, el proveedor debe poder demostrar en todo momento que realiza estas acciones de control y que obtiene el consentimiento válido, siendo responsable por las conductas de las empresas que realizan las comunicaciones.
- Disponible en : <https://acortar.link/WLP0Vc>

## **PRINCIPIO DE CONSENTIMIENTO: ACTUALIZACIÓN DE LOS DATOS PERSONALES DE AFILIADOS DE LAS AFP**

- Pronunciamiento : Opinión Consultiva N° 005-2022-JUS/DGTAIPD
- Asunto : Sobre actualización de base de datos de AFPs.
- Entidad Consultante : Entidad privada
- Criterio : 1. Los datos identificativos y el dato de contacto referido al domicilio pueden ser tratados sin el consentimiento del titular de los datos por parte de las AFPs, de acuerdo a lo dispuesto en el artículo 14, numeral 5 de la LPDP. Otros datos personales sólo podrán ser utilizados por estas administradoras con el consentimiento o autorización de los afiliados.
2. Las AFPs se encuentran obligadas a mantener actualizada la información personal de sus afiliados, la cual deberán utilizar solo para los fines autorizados por el titular del dato personal o por ley.
- Disponible en : <https://acortar.link/XDtPBm>

## **HABILITACIÓN LEGAL PARA EL TRATAMIENTO DE DATOS PERSONALES: ACCESO A DATOS PERSONALES POR PARTE DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA**

- Pronunciamiento : Opinión Consultiva N° 010-2022-JUS/DGTAIPD
- Asunto : Sobre el acceso a la base de datos del Registro Nacional de Sanciones contra Servidores Civiles.
- Entidad Consultante : Gerencia de Desarrollo del Sistema de Recursos Humanos de la Autoridad Nacional del Servicio Civil
- Criterio :
  1. Una entidad pública no requiere consentimiento del titular del dato personal para acceder a información personal en el marco del ejercicio de competencias otorgadas por ley. Sin embargo, debe de respetar los demás principios y obligaciones para el tratamiento de datos personales.
  2. La CGR se encuentra legitimada para acceder a la información y documentación sobre las operaciones de las entidades sujetas al ámbito de control gubernamental, aunque sea secreta, siendo necesaria esta para su función.
  3. Las declaraciones juradas de intereses no contienen información sobre las sanciones no vigentes impuestas a funcionarios públicos, por lo que no es necesario –por regla general– que la CGR tenga acceso a dicha información para el cumplimiento de las funciones reservadas a ella vinculadas a determinar si los intereses declarados por el sujeto obligado en la Ley N° 31227 son compatibles con el ejercicio de sus funciones, y otros aspectos de relevancia que deriven de los mismos establecidos en las disposiciones reglamentarias de la presente ley. Ello sin perjuicio de que pueda acceder a la información en el marco de otras acciones de control.
  4. No se aprecia una habilitación legal expresa en la Quinta Disposición Complementaria Final de la Ley N° 31227 para acceder a información sobre sanciones no vigentes del Registro Nacional de Sanciones contra Servidores Civiles.
- Disponible en : <https://n9.cl/2n4e5>

## **PRINCIPIO DE CONSENTIMIENTO: TRATAMIENTO DE DATOS PERSONALES EFECTUADO CON FINALIDADES RELATIVAS A LA PREVENCIÓN DE LAVADO DE ACTIVOS**

Pronunciamiento	: Opinión Consultiva N° 006-2022-JUS/DGTAIPD
Asunto	: Sobre uso tratamiento de datos para la prevención de delitos y cumplimiento regulatorio
Entidad Consultante	: Entidad privada
Criterio	: <ol style="list-style-type: none"><li>1. Los sujetos obligados a informar a la UIF-Perú, conforme la Ley N° 27693, pueden utilizar información obtenida de fuentes accesibles al público para el cumplimiento de sus obligaciones sin necesidad de solicitar el consentimiento del titular del dato personal.</li><li>2. Los sujetos obligados a informar a la UIF-Perú, conforme la Ley N° 27693, pueden compartir entre las empresas que formen parte del grupo económico al que pertenecen información de sus clientes para el cumplimiento de sus obligaciones relacionadas a la prevención del delito de lavado de activos y financiamiento del terrorismo, así como el cumplimiento regulatorio. Se debe establecer las medidas necesarias para garantizar la confidencialidad de la información que se comparte y que no es pública, y solo deberá ser utilizada para la finalidad mencionada.</li><li>3. Las personas jurídicas con la finalidad de evitar responsabilidad por los delitos previstos en los artículos 384, 397, 397-A, 398 y 400 del Código Penal, en los artículos 1, 2, 3 y 4 del Decreto Legislativo N° 1106, Decreto Legislativo de lucha eficaz contra el Lavado de Activos y otros delitos relacionados a la minería ilegal y el crimen organizado y en el artículo 4-A del Decreto Ley N° 25475, Decreto Ley que establece la penalidad para los delitos de terrorismo, pueden establecer medidas para la mitigación de riesgos, para lo cual pueden realizar tratamiento de datos de fuentes accesibles al público sin consentimiento del titular del dato personal.</li><li>4. No se puede señalar de forma general que todo tratamiento cuya finalidad, a criterio de una persona</li></ol>

jurídica, sea la prevención de lavado de activos se enmarca en las excepciones establecidas en el artículo 14 de la LPDP, puesto que si bien hay una finalidad que puede ser legítima, el tratamiento puede resultar desproporcional, por lo que debe evaluarse caso por caso.

Disponible en : <https://n9.cl/fmnzu>

## **PRINCIPIO DE PROPORCIONALIDAD: RECOPIACIÓN DE DATOS PERSONALES MEDIANTE SISTEMAS DE VIDEOVIGILANCIA**

Pronunciamiento	: Opinión Consultiva N° 07-2022-JUS/DGTAIPD
Asunto	: Sobre uso de sistemas de videovigilancia en caso de denuncias de hostigamiento sexual en instituciones educativas.
Entidad Consultante	: Entidad privada
Criterio	: <ol style="list-style-type: none"><li>1. Mediante el uso de las cámaras de videovigilancia se realiza una captación de información que contiene datos personales, tales como las imágenes y voces de una persona, siendo aplicable la LPDP y su reglamento, a fin de garantizar el derecho fundamental a la protección de datos personales, a través de un adecuado tratamiento, tanto por las entidades públicas, como por las instituciones pertenecientes al sector privado.</li><li>2. Es proporcional la instalación de cámaras de videovigilancia en aulas de una institución educativa ante denuncias recurrentes o sospechas razonables respecto a la comisión de un delito como el acoso u hostigamiento sexual, a fin de proteger el legítimo interés del titular del dato personal.</li><li>3. En caso de optar por la instalación de cámaras o videocámaras deberán respetar, adicionalmente los principios de calidad y seguridad; así como dar cumplimiento a las disposiciones y obligaciones establecidas en la LPDP, su reglamento y la Directiva.</li></ol>
Disponible en	: <a href="https://n9.cl/zye9v">https://n9.cl/zye9v</a>

## **PRINCIPIO DE PROPORCIONALIDAD: USO DE SOFTWARE DE PREVENCIÓN DE ACCESO A PORNOGRAFÍA INFANTIL ENTRE TRABAJADORES**

- Pronunciamiento : Opinión Consultiva N° 035-2022-DGTAIPD
- Asunto : Sobre instalación de software con finalidad de prevención de comisión del delito de pornografía infantil
- Entidad Consultante : Entidad privada
- Criterio : 1. La instalación y uso del software en las computadoras de la empresa que son asignadas a sus trabajadores no requiere de consentimiento en tanto el tratamiento de datos personales del empleador para fines de control y fiscalización laboral se exceptúa de la obligatoriedad de la obtención previa del consentimiento por parte del titular del dato personal (trabajadores), por estar enmarcado en la ejecución de una relación contractual (numeral 5 del artículo 14 de la LPDP).
2. No obstante, el empleador se encuentra obligado a informar de manera clara y expresa acerca de la existencia de esta herramienta y/o software de detección de actividades ilícitas, así como los supuestos en los que el mismo se activa y qué datos personales e información respecto al trabajador en dicha situación, el empleador, y el encargado de tratamiento, de ser el caso, tendrían acceso, así como los alcances previstos para dicho tratamiento.
3. El empleador puede utilizar el software como una forma de ejercicio de su poder de dirección y de control/fiscalización laboral siempre que el tratamiento de los datos personales vinculados al uso del mismo sea proporcional a la finalidad del tratamiento, la cual debe ser expresada de forma clara y precisa.
4. Corresponde a cada responsable de tratamiento de datos personales cumplir con las obligaciones previstas en la LPDP y su reglamento, partiendo especialmente de la interpretación de los principios rectores de finalidad, proporcionalidad, seguridad y confidencialidad, para efectos de

la implementación y ejecución de medidas informáticas de control y/o fiscalización laboral.

5. El desarrollo de la presente consulta se encuentra limitado únicamente al supuesto consultado de prevención del delito de pornografía infantil, no debiendo extenderse como una regla general para justificar cualquier acción que pueda ser ejercida por los empleadores en virtud de su poder de dirección.

Disponible en : <https://goo.su/cVfD>

## **TRATAMIENTO DE DATOS PERSONALES DE ESPECIAL INTERÉS: EJERCICIO DEL DERECHO DE ACCESO A DATOS PERSONALES OBTENIDOS POR SISTEMAS DE VIDEOVIGILANCIA**

- Pronunciamiento : Opinión Consultiva N° 008-2022-JUS/DGTAIPD
- Asunto : Sobre el derecho de acceso en sistemas de videovigilancia.
- Entidad Consultante : Entidad privada
- Criterio : 1. Para el ejercicio de derecho de acceso a datos recopilados a través de sistemas de videovigilancia resulta facultativa la entrega de una imagen actualizada del titular del dato personal, siendo necesaria para la visualización en sitio solo si a partir de la imagen del DNI, o de la información con la que cuenta el titular del banco de datos o responsable de tratamiento, no se puede reconocer a la persona por diversas circunstancias.
2. La alternativa de “acceso mediante un escrito” prevista en el literal a) del artículo 6.31.2 de la Directiva, implica que el titular del dato personal presente una solicitud escrita a la dirección física o electrónica que aparece en el cartel o documento informativo del titular del banco de datos personales o responsable del tratamiento, y este a su vez emita una respuesta detallando los datos requeridos por el titular del dato personal que son objeto de tratamiento, sin afectar derechos de terceros; es decir, el titular del dato personal es quien define qué datos personales requiere.
3. La alternativa de “entrega de las imágenes, videos o audios” regulada en el literal b) del artículo 6.31.2 de la Directiva, que dispone la entrega de un CD en blanco o en dispositivo análogo por parte del titular del dato personal para la grabación de su información, debe ser entendida como una alternativa económica para facilitar el derecho de acceso; lo cual no impide que si existen otros mecanismos similares acordes con el avance de la tecnología, con las medidas de seguridad apropiadas, que faciliten y beneficien al titular del dato personal para ejercer su derecho de acceso, pueden ejecutarse siempre y cuando el titular del dato personal este de acuerdo.
- Disponible en : <https://n9.cl/0r9mx>

## **DEBER DE CONFIDENCIALIDAD: PUBLICACION DE DATOS PERSONALES DE DEUDORES FINANCIEROS**

Pronunciamiento	:	Opinión Consultiva N° 015-2022-DGTAIPD
Asunto	:	Sobre publicación de lista de deudores de entidad financiera.
Entidad Consultante	:	Caja de Pensiones Militar Policial
Criterio	:	<ol style="list-style-type: none"><li>1. Las actividades de tratamiento de datos personales como la difusión (sin importar el medio), deben ceñirse a los principios y obligaciones de la LPDP y su reglamento, tales como los principios de consentimiento, proporcionalidad, finalidad y el deber de confidencialidad.</li><li>2. El Código Civil y el Código Procesal Civil establecen la forma en que se debe notificar en caso de proceso de cobranza, por lo que la CPMP deberá seguir dichas disposiciones para la cobranza de deudas, lo que no incluye la publicación de la lista de deudores en la página web de la entidad.</li></ol>
Disponible en	:	<a href="https://n9.cl/9suhn">https://n9.cl/9suhn</a>

## **HABILITACIÓN LEGAL PARA EL TRATAMIENTO DE DATOS PERSONALES: LEGITIMACIÓN DE ACCESO A DATOS SENSIBLES POR PARTE DEL MINISTERIO PÚBLICO**

- Pronunciamiento : Opinión Consultiva N° 026-2022-DGTAIPD
- Asunto : Sobre atención de requerimientos de información realizados por el Ministerio Público vinculados a datos personales sensibles.
- Entidad Consultante : Secretaría General del Ministerio de Salud
- Criterio : 1. Para el tratamiento de datos personales sensibles se requiere obligatoriamente el consentimiento válido y por escrito de sus titulares, salvo medie ley autoritativa al respecto o se configure uno o más de los supuestos de excepción contemplados en el artículo 14 de la LPDP.
2. Los fiscales no pueden tener acceso a información confidencial, como aquella vinculada a datos personales sensibles, sin que medie autorización legal, salvo supuestos de habilitación legal específica, como aquella contenida en el artículo 5 de la Ley N° 26626.
- Disponible en : <https://n9.cl/65cavj>

## **TRATAMIENTO DE DATOS PERSONALES DE ESPECIAL INTERÉS: TRATAMIENTO DE LOS DATOS PERSONALES DE SALUD**

- Pronunciamiento : Opinión Consultiva N° 027-2022-JUS/DGTAIPD
- Asunto : Sobre consentimiento para el tratamiento de datos personales sensibles
- Entidad Consultante : Entidad privada
- Criterio : 1. No debe confundirse el consentimiento que se brinda en virtud de lo dispuesto por la LPDP y su reglamento referido al tratamiento de datos personales, con el consentimiento informado para procedimientos médicos que, por su objeto referido a la autorización de procedimientos médicos o quirúrgicos, rebasa el ámbito de aplicación de las disposiciones normativas sobre protección de datos personales, con lo cual la forma de obtener este consentimiento debe de responder a las normas propias sobre la materia.
2. Los centros médicos deben de velar por el principio de calidad y el deber de confidencialidad de los datos personales, por lo que deben implementar los mecanismos necesarios para identificar de forma certera a los titulares de datos personales.
- Disponible en : <https://n9.cl/gypfiu>

## **REQUERIMIENTO DE DATOS PARSONALES DE SALUD (HISTORIA CLÍNICA) POR UN TRIBUNAL ARBITRAL**

- Pronunciamiento : Opinión Consultiva N° 041-2022-JUS/DGTAIPD
- Asunto : Sobre requerimiento de historia clínica por parte de un Tribunal Arbitral
- Entidad Consultante : Entidad privada
- Criterio :
  1. Para el tratamiento de datos personales sensibles se requiere obligatoriamente el consentimiento válido y por escrito de sus titulares, salvo que medie ley autoritativa al respecto o se configure uno o más de los supuestos de excepción contemplados en el artículo 14 de la LPDP.
  2. Los árbitros pueden solicitar a las partes que presenten pruebas, incluyendo aquellas que contienen información sensible, en aquellos casos que dicha información sea estrictamente necesaria para resolver determinada controversia, teniendo en cuenta el principio de proporcionalidad.
  3. El centro de salud que es parte del procedimiento arbitral puede presentar las historias clínicas que sean estrictamente necesarias para la solución de la controversia como medio probatorio sin necesidad de solicitar el consentimiento del titular del dato, conforme el artículo 14, numeral 13, de la LPDP, en el marco del ejercicio de su derecho de prueba.
  4. Las partes y el tribunal arbitral deben de guardar la confidencialidad de los datos personales a los que tengan acceso en el marco del procedimiento arbitral.
  5. Una historia clínica disociada puede ser entregada sin consentimiento del titular del dato personal, dado que no permite identificar al titular del dato personal.
- Disponible en : <https://shre.ink/xpxk>

## **TRATAMIENTO DE DATOS PERSONALES DE ESPECIAL INTERÉS: ENTREGA DE DATOS PERSONALES RELATIVOS A LA AFILIACIÓN SINDICAL**

Pronunciamiento	: Opinión Consultiva N° 042-2022-DGTAIPD
Asunto	: Sobre entrega de listas de afiliados a una organización sindical a congresistas y a entidades públicas
Entidad Consultante	: Secretaría General del Ministerio de Trabajo y Promoción del Empleo
Criterio	: <ol style="list-style-type: none"><li>1. Los datos vinculados a la afiliación sindical de una persona resultan de especial protección al ser considerados datos sensibles, debido a su particular relevancia para la intimidad y ejercicio de otros derechos y libertades fundamentales del titular, motivo por el cual no pueden ser tratados sin consentimiento válido y por escrito de su titular.</li><li>2. No obstante, existen limitaciones y/o excepciones a la obligación de obtención del consentimiento para el tratamiento de datos personales, como aquellos contemplados en los numerales 1 y 13 del artículo 14 de la LPDP, esto es, cuando la recopilación de los mismos sea para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias, así como las facultades de un Congresista que representa a una Comisión Investigadora del Congreso establecidas a nivel constitucional.</li><li>3. Únicamente, podrán acceder a datos personales sensibles aquellos funcionarios que para el ejercicio de sus competencias establecidas por ley requieran de dicha información, debiendo sustentar y/o justificar dicha necesidad de acceso, así como delimitar su pedido a lo estrictamente necesario frente a la entidad responsable del tratamiento de los datos personales.</li><li>4. El régimen de las excepciones al acceso regulado en la Ley de Transparencia y Acceso a la Información Pública resulta oponible a los pedidos de información que se realizan en el marco del deber de colaboración o en el ejercicio de las competencias encomendadas a otras entidades. La excepcionalidad del acceso no será aplicable a las entidades que, conforme a la Constitución Política del Perú y a la citada Ley se encuentran habilitadas para conocer información excluida del dominio público.</li></ol>
Disponible en	: <a href="https://n9.cl/njuwk">https://n9.cl/njuwk</a>

## **TRATAMIENTO DE DATOS PERSONALES DE ESPECIAL INTERÉS: PERSONAS DESAPARECIDAS Y UBICADAS**

- Pronunciamiento : Opinión Consultiva N° 001-2023-DGTAIPD
- Asunto : Sobre protección de datos personales en el marco de la difusión de alertas de emergencia de personas reportadas como desaparecidas y de publicación de información de personas ubicadas
- Entidad consultante : Dirección General de Seguridad Democrática del Ministerio del Interior
- Criterios : 1. No se requiere el consentimiento para la publicación referida a una persona reportada como desaparecida en diversos medios de instituciones privadas. Dicha publicación solo debe contener detalles relevantes para su búsqueda, teniendo en cuenta el principio de proporcionalidad.
2. Una vez ubicada la persona reportada como desaparecida, debe indicarse dicha situación en la fuente original, a fin de que sea conocida por quienes han compartido la noticia.
3. La información sobre la ubicación de una persona desaparecida no debe contener detalles que vulneren innecesariamente la intimidad o privacidad de la persona, y debe mantenerse durante un periodo razonable, teniendo en cuenta los principios de proporcionalidad y finalidad.
- Disponible en: : <https://bit.ly/48dIT6q>

## **TRATAMIENTO DE DATOS PERSONALES DE ESPECIAL INTERÉS: DATOS DE INGRESOS ECONÓMICOS ENTREGADOS POR EMPLEADORES A ORGANIZACIONES SINDICALES**

- Pronunciamiento : Opinión Consultiva N° 007-2023-DGTAIPD
- Asunto : Sobre entrega de boletas de pago en el marco de un procedimiento de negociación colectiva
- Entidad consultante : Persona natural
- Criterios : 1. Los empleadores podrán entregar boletas de pago y/o escala salarial a una organización sindical, sin solicitar el consentimiento de los titulares de datos personales, siempre que su tratamiento tenga por finalidad funciones sindicales (defensa de derechos e intereses de los trabajadores, a través de la negociación y su posterior convención colectiva) y aplicando la disociación y/o anonimización de los datos personales que no sean necesarios para tal finalidad, contenidos en los documentos a entregar.
2. Se debe tener en cuenta los principios de finalidad y proporcionalidad, en virtud de los cuales deben entregarse únicamente los datos necesarios y relevantes, no excesivos a la finalidad determinada reconocida para la cual éstos son entregados (defensa de derechos e intereses de los trabajadores, a través de la negociación y su posterior convención colectiva), no debiendo extenderse el tratamiento de los mismos a finalidades distintas a la mencionada.
- Disponible en : <https://bit.ly/42lxoaD>

## **HABILITACIÓN LEGAL PARA EL TRATAMIENTO DE DATOS PERSONALES: PUBLICIDAD DE PERSONAL DOCENTE CONDENADO Y SEPARADO DE ACUERDO CON LA LEY N° 29988**

Pronunciamiento	: Opinión Consultiva N° 030-2023-JUS/DGTAIPD
Asunto	: Sobre la publicidad de la relación de personal condenado y separado por los delitos señalados en la Ley N° 29988, Ley que establece medidas extraordinarias para el personal docente y administrativo de instituciones educativas públicas y privadas, implicado en delitos de terrorismo, apología del terrorismo, delitos de violación de la libertad sexual y delitos de tráfico ilícito de drogas; crea el Registro de personas condenadas o procesadas por delito de terrorismo, apología del terrorismo, delitos de violación de la libertad sexual y tráfico ilícito de drogas y modifica los artículos 36 y 38 del Código Penal
Entidad consultante	: Oficina General de Transparencia, Ética Pública y Anticorrupción del Ministerio de Educación
Criterios	: <ol style="list-style-type: none"><li>1. La información sobre antecedentes penales de una persona no es pública, incluyendo la información de las personas que están impedidas de prestar servicios de docencia por estar condenadas por los delitos señalados en la Ley N° 29988. Por lo que, solo puede ser conocida por las autoridades competentes señaladas en la propia norma.</li><li>2. Para la publicación de personas impedidas de prestar servicios de docencia por estar condenadas por los delitos señalados en la Ley N° 29988, se requiere una modificación a esa misma ley para otorgarle el carácter público; lo que debe presumir un análisis previo y conforme de constitucionalidad, en procura de implementar la publicidad de los antecedentes penales de las personas que hayan cometido los delitos señalados en la referida Ley, como medida precautoria para evitar su contratación en el sector Educación, y el impacto que dicha medida traería en las posibilidades de reinserción social de este colectivo.</li></ol>
Disponible en	: <a href="https://bit.ly/4nYv3dT">https://bit.ly/4nYv3dT</a>

## **HABILITACIÓN LEGAL PARA EL TRATAMIENTO DE DATOS PERSONALES: ACCESO A LA INFORMACIÓN SOBRE CLASIFICACIÓN SOCIOECONÓMICA CONTENIDA EN EL PADRÓN GENERAL DE HOGARES**

Pronunciamiento	:	Opinión Consultiva N° 022-2023-DGTAIPD
Asunto	:	Sobre la protección de datos personales contenidos en el Padrón General de Hogares y el acceso de las entidades públicas a la información de la clasificación socioeconómica
Entidad consultante	:	Dirección General de Focalización e Información del Ministerio de Desarrollo e Inclusión Social
Criterios:	:	<ol style="list-style-type: none"><li>1. La clasificación socioeconómica (CSE), al formar parte de la información de un potencial beneficiario/ usuario que se registra en el Padrón General de Hogares – PGH, juntamente con sus nombres completos u otros datos personales, permite identificarlo como tal, por lo que sí tiene calidad de dato personal, cuyo tratamiento debe estar sujeto a la observancia de la LPDP y su reglamento.</li><li>2. Únicamente podrán tener acceso a la clasificación de hogares vinculada a datos personales contenidos en el PGH, sin consentimiento de los titulares de datos, aquellas entidades que se encuentren bajo el marco de actuación del Sistema Nacional de Focalización en el marco de intervenciones públicas focalizadas aprobadas por las comisiones interministeriales de asuntos sociales.</li><li>3. El MIDIS, como entidad encargada del PGH, debe garantizar el cumplimiento de los principios de la LPDP, tales como el principio de finalidad, proporcionalidad, así como el deber de confidencialidad de los datos que permiten identificar a un titular de datos personales plenamente como potencial beneficiario de un bien o servicio de una intervención pública focalizada que considere como requisito de elegibilidad la CSE, en tanto contiene este dato personal en su registro.</li><li>4. El MIDIS puede proporcionar información disociada o estadística respecto a la clasificación de hogares.</li></ol>
Disponible en	:	<a href="https://bit.ly/4mJqTFC">https://bit.ly/4mJqTFC</a>

## **LIMITES AL TRATAMIENTO DE DATOS PERSONALES A LAS ENTIDADES PÚBLICAS: REGISTRO DE INFORMACIÓN MIGRATORIO Y CERTIFICADO DE MOVIMIENTO MIGRATORIO**

Pronunciamiento	:	Opinión Consultiva N° 001-2024-DGTAIPD
Asunto	:	Sobre el tratamiento de datos personales contenidos en el Registro de Información Migratoria y en el Certificado de Movimiento Migratorio
Entidad consultante	:	Oficina de Asesoría Jurídica de la Superintendencia Nacional de Migraciones
Criterios	:	<ol style="list-style-type: none"><li>1. Uno de los supuestos de excepción del artículo 14 de la Ley N° 29733, Ley de Protección de Datos Personales, desarrollado en el artículo 17 de su reglamento, alude a la existencia de una fuente de acceso público respecto de la cual los datos personales puedan ser extraídos para determinados tratamientos. Además de la lista que el citado artículo reglamentario recoge, la normativa prevé la existencia de otras que, por mandato de norma con rango legal, existan. No es el caso del RIM, ni por inclusión en dicho listado ni por existir norma con rango legal entre las analizadas que así lo reconozca; por lo que no se le puede considerar fuente de acceso público.</li><li>2. El tratamiento de datos personales realizado por la Superintendencia Nacional de Migraciones referido al suministro de la información contenida en el Certificado de Movimiento Migratorio a terceros distintos al titular de los datos personales (sin contar con el consentimiento de estos) no está amparado en la Ley N° 29733, Ley de Protección de Datos Personales, ni en su Reglamento.</li></ol>
Disponible en	:	<a href="https://n9.cl/rx45uw">https://n9.cl/rx45uw</a>

## **TRATAMIENTO DE DATOS PERSONALES DE ESPECIAL INTERÉS: DATOS PERSONALES RELATIVOS A LA AFILIACIÓN SINDICAL Y OTROS DE MIEMBROS DE UN SINDICATO DE TRABAJADORES**

Pronunciamiento	: Opinión Consultiva N° 002-2024-JUS/DGTAIPD
Asunto	: Sobre la confidencialidad de los datos personales referido a la “afiliación sindical” y de los miembros de los sindicatos
Entidad consultante	: Persona natural
Criterios	: <ol style="list-style-type: none"><li>1. La información referida a la afiliación sindical constituye un dato personal sensible que ostenta una especial protección por la incidencia que tiene en la intimidad personal, el ejercicio de libertades y derechos fundamentales de su titular, como es el derecho a la libertad sindical, que, de ser expuesto deliberadamente, pueden tener repercusiones graves en su esfera personal y laboral.</li><li>2. La relación de afiliados a una organización sindical con indicación de su DNI revela la pertenencia del trabajador a un sindicato (afiliación sindical), el cual es un aspecto exclusivo del trabajador y resulta ser un dato sensible. Por ende, el artículo 17 inciso 5 del TUO de la LTAIP lo excluye del acceso.</li><li>3. El correo y número telefónico de los afiliados a una organización sindical es información excluida del acceso, conforme al artículo 17 inciso 5 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.</li></ol>
Disponible en	: <a href="https://n9.cl/j4mj4">https://n9.cl/j4mj4</a>

**TRATAMIENTO DE DATOS PERSONALES DE ESPECIAL INTERÉS: DATOS PERSONALES DE PARIENTES DE FUNCIONARIOS Y SERVIDORES PÚBLICOS BENEFICIARIOS DE SEGUROS CONTRATADOS PARA ESTOS, INCLUYENDO MENORES DE EDAD**

- Pronunciamento : Opinión Consultiva N° 008-2024-JUS/DGTAIPD
- Asunto : Sobre el carácter público del monto, periodicidad de pago y beneficiarios de la contratación de seguros privados o programas de salud por las entidades para sus funcionarios públicos y familiares con cargo a recursos públicos
- Entidad consultante : Funcionario Responsable de Acceso a la Información Pública de la Superintendencia Nacional de Salud
- Criterios : 1. La identidad de los funcionarios y servidores públicos beneficiarios de los programas de asistencia médica o seguros privados contratados con recursos públicos no está protegida por el artículo 17 inciso 5 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, tampoco la identidad y el vínculo de parentesco de sus familiares beneficiarios, ya que, existe un interés público en vigilar la correcta ejecución del gasto público y el cumplimiento de los requisitos para gozar de este beneficio como, por ejemplo, ser cónyuge, concubino/concubina, hijo/hija con cierta edad u otras exigencias determinadas por la entidad. En el caso de hijo/hija menor de edad debiera aplicarse, en la eventualidad de una entrega de información por mediar una solicitud de acceso a la información pública, un mecanismo o procedimiento de disociación de datos personales respecto a sus nombres.
2. En aplicación del artículo 17 inciso 6 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, el artículo 4 de la Constitución y el artículo IX del Título Preliminar del Código de los Niños y Adolescentes, la identificación de los familiares menores de edad de los funcionarios públicos, que sean beneficiarios de los programas de asistencia médica o seguros privados contratados con recursos públicos, constituye información confidencial. Sin embargo, esta excepción no comprende al vínculo de parentesco propiamente como, por ejemplo, ser hijo o hija u otra información relativa al cumplimiento de los requisitos exigidos por la entidad para acceder al beneficio en mención.
- Disponible en : <https://n9.cl/d4o34>

## **TRATAMIENTO DE DATOS PERSONALES DE ESPECIAL INTERÉS: DATOS PERSONALES DE PROFESORES DE COLEGIOS PRIVADOS**

Pronunciamiento	: Opinión Consultiva N° 009-2024-JUS/DGTAIPD
Asunto	: Consulta sobre entrega de copia de títulos profesionales y/o pedagógicos de la plana docente de instituciones educativas privadas ante la solicitud de terceros
Entidad consultante	: Persona natural
Criterios	: <ol style="list-style-type: none"><li>1. Para el tratamiento de datos personales se requiere obligatoriamente el consentimiento válido de sus titulares, salvo medie ley autoritativa al respecto o se configure uno o más de los supuestos de excepción contemplados en el artículo 14 de la Ley N° 29733, Ley de Protección de Datos Personales, siendo de aplicación al presente caso los numerales 7 y 8.</li><li>2. Los colegios privados se encuentran facultados legalmente para entregar información respecto a sus profesores y docentes (acerca de los diplomas que acrediten los grados académicos y títulos otorgados por las universidades, instituciones y escuelas de educación superior universitarios) como parte de las características del servicio público de educación que prestan.</li><li>3. Cualquier solicitud de acceso a información distinta sobre el personal docente debe contar con el consentimiento previo, informado, expreso e inequívoco de su titular; máxime tratándose de datos personales propios de su esfera privada. Dicho consentimiento no es necesario recabarse si se aplica algún procedimiento de disociación que impida el conocimiento de estos datos que yacen en documentación que es, por naturaleza, pública, y que favorezca la entrega parcial de la información.</li></ol>
Disponible en	: <a href="https://shre.ink/SWr5">https://shre.ink/SWr5</a>

**LIMITES AL TRATAMIENTO DE DATOS PERSONALES A LAS ENTIDADES PÚBLICAS: TRATAMIENTO DE DATOS PERSONALES REALIZADO POR MEDIO DE LA PLATAFORMA SISTEMA ELECTRÓNICO DE CONTRATACIONES DEL ESTADO – SEACE**

Pronunciamiento	:	Opinión Consultiva N° 016-2024-JUS/DGTAIPD
Asunto	:	Sobre el Sistema Electrónico de Contrataciones del Estado y la transversalidad del régimen de excepciones de la Ley N° 29733, Ley de Protección de Datos Personales, y la obligación de implementar una política
Entidad consultante	:	Persona natural
Criterios	:	<ol style="list-style-type: none"><li>1. El supuesto regulado en el artículo 17, numeral 5, del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública cautela los datos personales de las personas naturales cuya publicidad pueda afectar su intimidad personal o familiar, por lo que, no comprende la información de las personas jurídicas ni los datos de sus representantes legales. Distinto es el caso de una persona natural con o sin negocio, pues no pierde dicho carácter por el hecho de contar con un negocio.</li><li>2. La plataforma del SEACE debe contar con una política de privacidad que informe sobre los tratamientos de datos que se realizan con los datos recopilados a través de la misma, conforme lo dispuesto por el artículo 18 de la Ley N° 29733, Ley de Protección de Datos Personales. Así, de corresponder, debe adecuarse; para lo cual se tiene en la Guía práctica para la Observancia del Deber de Informar y en la orientación que a este respecto puede brindar la Autoridad Nacional de Protección de Datos Personales, una vía para hacerlo.</li></ol>
Disponible en	:	<a href="https://shre.ink/SWri">https://shre.ink/SWri</a>

## **SOBRE DEFINICIÓN DE DATOS PERSONALES: TRATAMIENTO DE PLACAS DE RODAJE COMO DATO PERSONAL**

- Pronunciamento : Opinión Consultiva N° 017-2024-JUS/DGTAIPD
- Asunto : Sobre la accesibilidad a la placa de rodaje de un vehículo, a propósito de la inaplicación del numeral 5 del artículo 17 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública y ejercicio del derecho de acceso regulado por la Ley N° 29733, Ley de Protección de Datos Personales
- Entidad consultante : Unidad de Atención a la Ciudadanía y Gestión Documental de la Autoridad de Transporte Urbano para Lima y Callao
- Criterios : 1. La placa de rodaje de los vehículos constituye un dato personal; sin embargo, al estar sujeto tanto a publicidad registral como contenida en fuentes accesibles al público es de carácter público; por ende, no le resulta aplicable la excepción del numeral 5 del artículo 17 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública y puede ser entregada en el marco de una solicitud de acceso a la información pública.
2. Las solicitudes para acceder a información propia como las boletas de pago, legajo y/o órdenes de servicios pueden tramitarse por el procedimiento de acceso a la información pública si el requirente invoca el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública o su reglamento, o no acredita ni motiva algún interés particular. Por ende, la entrega de la información corresponderá a aquella que sea de acceso público. En caso acredite y/o justifique algún interés particular, corresponde tramitarlo bajo el procedimiento diseñado para la petición administrativa o por las normativas específicas que regulan la entrega a su titular, cuya identificación precisa exceden las competencias.
3. Si una persona requiere copia de sus boletas de pago, su legajo y/u órdenes de servicios, es decir, información propia y que le atañe, acreditando y/o

justificando algún interés particular en acceder, corresponderá tramitarlo, en principio, bajo el procedimiento diseñado para el ejercicio del derecho de petición administrativa o las normas específicas que regulan la entrega a su titular como, por ejemplo, la legislación laboral, en el caso de las boletas de pago, o las normas de contratación pública, en el caso de las órdenes de servicios.

Disponible en : <https://acortar.link/PTgWKG>

## **TRATAMIENTO DE DATOS PERSONALES DE ESPECIAL INTERÉS: DATOS PERSONALES DE SALUD EN CERTIFICADOS DE TRABAJO**

- Pronunciamiento : Opinión Consultiva N° 018-2024-JUS/DGTAIPD
- Asunto : Sobre la confidencialidad de la información contenida en los certificados médicos, así como la información referida al descanso médico y el rol del Médico de Control
- Entidad consultante : Funcionario Responsable de Transparencia y Acceso a la Información Pública de la Unidad de Gestión Educativa Local N° 15
- Criterios : 1. El certificado médico contiene información relativa al acto médico realizado por un profesional de salud, donde se describen las acciones realizadas, el diagnóstico efectuado y el tratamiento a seguir, por tanto, contiene información relacionada a la salud; en consecuencia, se encuentra comprendido en el supuesto de excepción regulado en el artículo 17, numeral 5 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
2. El médico de control se encuentra legitimado para acceder a la información contenida en un Certificado Médico en el marco de una acción de validación, para lo cual no requiere contar con el consentimiento del titular de los datos personales. Sin embargo, debe observar los demás principios y obligaciones para el tratamiento de datos personales señalados en la Ley N° 29733, Ley de Protección de Datos Personales.
- Disponible en : <https://n9.cl/eysfy>

**LIMITES AL TRATAMIENTO DE DATOS PERSONALES A LAS ENTIDADES PÚBLICAS: TRATAMIENTO DE DATOS PERSONALES DE SALUD POR ÓRGANO DESCONCENTRADO DEL MINISTERIO DE SALUD**

- Pronunciamiento : Opinión Consultiva N° 008-2025-DGTAIPD
- Asunto : Sobre la transferencia de datos al Centro de Epidemiología, Prevención y Control de Enfermedades, órgano desconcentrado del Ministerio de Salud, para la implementación del Registro Nacional de Cáncer
- Entidad consultante : Centro de Epidemiología, Prevención y Control de Enfermedades del Ministerio de Salud
- Criterios : 1. Para el adecuado cumplimiento de sus funciones [realizar vigilancia epidemiológica sin duplicar registros], delimitadas por las normas legales (Decreto Legislativo N° 1161 y Ley N° 31336), el Centro de Epidemiología, Prevención y Control de Enfermedades requiere recopilar datos de los pacientes diagnosticados con cáncer, específicamente el DNI, apellidos y nombres, dirección domiciliaria, teléfono de contacto y en el caso de menores de edad, el DNI, nombres, apellidos y número de teléfono de la persona responsable.
2. Dicha información [en tanto necesaria e indispensable para el cumplimiento de sus funciones] permitirá que se cuente con cifras certeras respecto al estado situacional del cáncer en el Perú, de tal forma que se puedan realizar las investigaciones necesarias, se cuente con estadística y se puedan implementar las políticas públicas pertinentes.
3. Por lo tanto, para dicho tratamiento no se requiere el consentimiento del titular del dato personal.
- Disponible en : <https://n9.cl/7apan>

## **PRINCIPIO DE CONSENTIMIENTO: CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES RECOPIADOS EN EVENTOS PÚBLICOS**

Pronunciamiento	: Opinión Consultiva N° 012-2025-DGTAIPD
Asunto	: Sobre tratamiento de datos personales en eventos públicos
Entidad consultante	: Gerencia de Asesoría Jurídica del Organismo Supervisor de la Inversión en Energía y Minería - Osinergmin
Criterios	: <ol style="list-style-type: none"><li>1. Para difundir datos personales recopilados en un evento público, como una feria de libro, se requiere el consentimiento previo, libre expreso e informado del titular del dato personal, salvo se usen máscaras de privacidad.</li><li>2. Se considera que se cumple con la obligación de obtener el consentimiento expreso cuando la conducta del titular del dato personal permite de forma indubitable conocer que el titular del dato está dando su consentimiento para ser grabado, por ejemplo, posando ante la cámara de un medio de comunicación.</li></ol>
Disponible en	: <a href="https://n9.cl/fb0bru">https://n9.cl/fb0bru</a>

## ÍNDICE

• Prólogo .....	7
• Presentación .....	9
• Resolución Viceministerial .....	11
• Guía del Lector .....	13

### COMPENDIO DE PROTECCIÓN DE DATOS PERSONALES: NORMATIVA Y CRITERIOS INTERPRETATIVOS RELEVANTES

#### COMPENDIO NORMATIVO

1. LEY N° 29733 – Ley de protección de datos personales .....	19
2. DECRETO SUPREMO N° 003-2013-JUS – Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.....	55

#### CRITERIOS INTERPRETATIVOS

##### 2022

• Opinión Consultiva N° 001-2022-2022-DGTAIPD – Sobre el alcance de la autorización de primer contacto para solicitar el consentimiento para el uso de datos con fines de publicidad.....	128
• Opinión Consultiva N° 005-2022-JUS/DGTAIPD – Sobre actualización de base de datos de AFPs.....	129
• Opinión Consultiva N° 010-2022-JUS/DGTAIPD – Sobre el acceso a la base de datos del Registro Nacional de Sanciones contra Servidores Civiles .....	130
• Opinión Consultiva N° 006-2022-JUS/DGTAIPD – Sobre uso tratamiento de datos para la prevención de delitos y cumplimiento regulatorio .....	131
• Opinión Consultiva N° 007-2022-JUS/DGTAIPD – Sobre uso de sistemas de videovigilancia en caso de denuncias de hostigamiento sexual en instituciones educativas .....	133
• Opinión Consultiva N° 035-2022-DGTAIPD – Sobre instalación de software con finalidad de prevención de comisión del delito de pornografía infantil .....	134
• Opinión Consultiva N° 008-2022-JUS/DGTAIPD – Sobre el derecho de acceso en sistemas de videovigilancia.....	136
• Opinión Consultiva N° 015-2022-DGTAIPD – Sobre publicación de lista de deudores de entidad financiera .....	137

- Opinión Consultiva N° 026-2022-DGTAIPD - Sobre atención de requerimientos de información realizados por el Ministerio Público vinculados a datos personales sensibles..... 138
- Opinión Consultiva N° 027-2022-JUS/DGTAIPD - Sobre consentimiento para el tratamiento de datos personales sensibles..... 139
- Opinión Consultiva N° 041-2022-JUS/DGTAIPD - Sobre requerimiento de historia clínica por parte de un Tribunal Arbitral..... 140
- Opinión Consultiva N° 042-2022-DGTAIPD - Sobre entrega de listas de afiliados a una organización sindical a congresistas y a entidades públicas..... 141

## 2023

- Opinión Consultiva N° 001-2023-DGTAIPD - Sobre protección de datos personales en el marco de la difusión de alertas de emergencia de personas reportadas como desaparecidas y de publicación de información de personas ubicadas ..... 142
- Opinión Consultiva N° 007-2023-DGTAIPD - Sobre entrega de boletas de pago en el marco de un procedimiento de negociación colectiva..... 143
- Opinión Consultiva N° 030-2023-JUS/DGTAIPD - Sobre la publicidad de la relación de personal condenado y separado por los delitos señalados en la Ley N° 29988, Ley que establece medidas extraordinarias para el personal docente y administrativo de instituciones educativas públicas y privadas, implicado en delitos de terrorismo, apología del terrorismo, delitos de violación de la libertad sexual y delitos de tráfico ilícito de drogas; crea el Registro de personas condenadas o procesadas por delito de terrorismo, apología del terrorismo, delitos de violación de la libertad sexual y tráfico ilícito de drogas y modifica los artículos 36 y 38 del Código Penal..... 144
- Opinión Consultiva N° 022-2023-DGTAIPD - Sobre la protección de datos personales contenidos en el Padrón General de Hogares y el acceso de las entidades públicas a la información de la clasificación socioeconómica ..... 145

## 2024

- Opinión Consultiva N° 001-2024-DGTAIPD - Sobre el tratamiento de datos personales contenidos en el Registro de Información Migratoria y en el Certificado de Movimiento Migratorio..... 146
- Opinión Consultiva N° 002-2024-JUS/DGTAIPD - Sobre la confidencialidad de los datos personales referido a la “afiliación sindical” y de los miembros de los sindicatos ..... 147
- Opinión Consultiva N° 008-2024-JUS/DGTAIPD - Sobre el carácter público del monto, periodicidad de pago y beneficiarios de la contratación de seguros privados o programas de salud por las entidades para sus funcionarios públicos y familiares con cargo a recursos públicos..... 148
- Opinión Consultiva N° 009-2024-JUS/DGTAIPD - Consulta sobre entrega de copia de títulos profesionales y/o pedagógicos de la plana docente de instituciones educativas privadas ante la solicitud terceros..... 149
- Opinión Consultiva N° 016-2024-DGTAIPD - Sobre el Sistema Electrónico de Contrataciones del Estado y la transversalidad del régimen de excepciones de la

Ley N° 29733, Ley de Protección de Datos Personales, y la obligación de implementar una política.....150

- Opinión Consultiva N° 017-2024-JUS/DGTAIPD - Sobre la accesibilidad a la placa de rodaje de un vehículo, a propósito de la inaplicación del numeral 5 del artículo 17 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública y ejercicio del derecho de acceso regulado por la Ley N° 29733, Ley de Protección de Datos Personales..... 151
- Opinión Consultiva N° 018-2024-JUS/DGTAIPD - Sobre la confidencialidad de la información contenida en los certificados médicos, así como la información referida al descanso médico y el rol del Médico de Control .....153

**2025**

- Opinión Consultiva N° 008-2025-DGTAIPD - Sobre la transferencia de datos al Centro de Epidemiología, Prevención y Control de Enfermedades, órgano desconcentrado del Ministerio de Salud, para la implementación del Registro Nacional de Cáncer .....154
- Opinión Consultiva N° 012-2025-DGTAIPD - Sobre tratamiento de datos personales en eventos públicos.....155

Índice .....156



**Dirección General de Desarrollo Normativo y Calidad Regulatoria**  
**Dirección de Sistematización Jurídica y Difusión**

Scipión Llona 350 Miraflores, Lima 18  
Teléfono: (511) 204-8020  
<https://www.gob.pe/minjus>  
<https://spijweb.minjus.gob.pe>