NORMAS LEGALES
ACTUALIZADAS

Editora Perú

DIARIO OFICIAL DEL BICENTENARIO
El Peruano

# LEY DE PROTECCIÓN DE DATOS PERSONALES

Ley Nº 29733

# REGLAMENTO DE LA LEY Nº 29733, LEY DE PROTECCIÓN DE DATOS PERSONALES

Decreto Supremo Nº 003-2013-JUS

# LEY DE PROTECCIÓN DE DATOS PERSONALES

## LEY Nº 29733

EL PRESIDENTE DE LA REPÚBLICA

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 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 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". ***(*) Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

**"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 modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

## 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.

**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".

***(*) Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

## 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 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 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 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".

***(*) Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

**"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.

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 autentificación 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". ***(*) Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

**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.

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". ***(*) Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

**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.

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 27806, Ley de Transparencia y Acceso a la Información Pública, o la que haga sus veces**".** ***(*) Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

**"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". ***(*) Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

**"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". ***(*) Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

**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.

**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 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". ***(*) Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

**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 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.

**"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***". (*) Artículo modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

## TÍTULO IV

## "OBLIGACIONES DEL TITULAR Y DEL ENCARGADO DE TRATAMIENTO DE DATOS PERSONALES"

***(*) Denominación modificada por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

**"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.
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***". (*) Artículo modificado por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

## 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 modificado por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 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, cuyo texto es el siguiente:***

**"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 de los principios rectores establecidos en esta Ley." ***(*) Artículo modificado por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

## 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 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces, así como de potestad coactiva, de conformidad con la Ley 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 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".

***(*) Artículo modificado por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

**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 Nº 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". ***(*) Artículo modificado por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, publicado el 7 de enero de 2017.***

**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 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 27444, 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 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 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 28706 , Ley de Transparencia y Acceso a la Información Pública, constituye dato sensible conforme a los alcances de esta Ley.(*)

**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.

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

# REGLAMENTO DE LA LEY Nº 29733 LEY DE PROTECCIÓN DE DATOS PERSONALES

## DECRETO SUPREMO Nº 003-2013-JUS

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, el artículo 2 numeral 6 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, la Ley Nº 29733, Ley de Protección de Datos Personales, tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en la Constitución Política del Perú;

Que, el artículo 32 de la acotada Ley Nº 29733, dispone que el Ministerio de Justicia y Derechos Humanos asume la Autoridad Nacional de Protección de Datos Personales;

Que, la Primera Disposición Complementaria Final de la Ley Nº 29733, dispuso que se constituya una Comisión Multisectorial, presidida por la Autoridad Nacional de Protección de Datos Personales, para la elaboración del correspondiente Reglamento;

Que, la Comisión Multisectorial conformada mediante Resolución Suprema Nº 180-2011-PCM ha elaborado el proyecto de Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales, el que ha sido prepublicado conforme a ley, recibiéndose los aportes de la ciudadanía y comunidad en general;

Que, en tal sentido, corresponde aprobar el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales;

De conformidad con lo establecido por la Ley Nº 29733, Ley de Protección de Datos Personales; la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo; y la Ley Nº 29809, Ley de Organización y Funciones del Ministerio de Justicia y Derechos Humanos;

DECRETA:

**Artículo 1.- Aprobación**

Apruébese el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales, que consta de VI Títulos, ciento treinta y un (131) Artículos, tres (03) Disposiciones Complementarias Finales y tres (03) Disposiciones Complementarias Transitorias, que forma parte integrante del presente Decreto Supremo.

**Artículo 2.- Publicación**

El presente Decreto Supremo y el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales, aprobado por el artículo precedente, deberán ser publicados en el Portal Institucional del Ministerio de Justicia y Derechos Humanos (www.minjus.gob.pe).

**Artículo 3.- Vigencia**

El Reglamento aprobado entrará en vigencia en el plazo de treinta (30) días hábiles contados a partir del día siguiente de la publicación del presente Decreto Supremo en el Diario Oficial El Peruano.

**Artículo 4.- Refrendo**

El presente Decreto Supremo será refrendado por la Ministra de Justicia y Derechos Humanos.

Dado en la Casa de Gobierno, en Lima, a los veintiún días del mes de marzo del año dos mil trece.

OLLANTA HUMALA TASSO
Presidente Constitucional de la República

EDA A. RIVAS FRANCHINI
Ministra de Justicia y Derechos Humanos

# REGLAMENTO DE LA LEY Nº 29733 LEY DE PROTECCIÓN DE DATOS PERSONALES

## Índice


| | |
|---|---|
| **TÍTULO I** | Disposiciones generales. |
| **TÍTULO II** | Principios rectores. |
| **TÍTULO III** | Tratamiento de datos personales. |
| **Capítulo I** | Consentimiento. |
| **Capítulo II** | Limitaciones al consentimiento. |
| **Capítulo III** | Transferencia de datos personales. |
| **Capítulo IV** | Tratamientos especiales de datos personales. |
| **Capítulo V** | Medidas de seguridad. |
| **TÍTULO IV** | Derechos del titular de datos personales. |
| **Capítulo I** | Disposiciones generales. |
| **Capítulo II** | Disposiciones especiales. |
| **Capítulo III** | Procedimiento de tutela. |
| **TÍTULO V** | Registro Nacional de Protección de Datos Personales. |
| **Capítulo I** | Disposiciones generales. |
| **Capítulo II** | Procedimiento de inscripción. |
| **Capítulo III** | Procedimiento de inscripción de los códigos de conducta. |
| **TÍTULO VI** | Infracciones y sanciones. |
| **Capítulo I** | Procedimiento fiscalizador. |
| **Capítulo II** | Procedimiento sancionador. |
| **Capítulo III** | Sanciones. |

**Disposiciones Complementarias Finales y Transitorias**

## TÍTULO I

### Disposiciones generales

**Artículo 1.- Objeto.**

El presente reglamento tiene por objeto desarrollar la Ley Nº 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, tanto por las entidades públicas, como por las instituciones pertenecientes al sector privado. Sus disposiciones constituyen normas de orden público y de cumplimiento obligatorio.

**Artículo 2.- Definiciones.**

Para los efectos de la aplicación del presente reglamento, sin perjuicio de las definiciones contenidas en la Ley, complementariamente, se entiende las siguientes definiciones:

**1. Banco de datos personales no automatizado:** Conjunto de datos de personas naturales no computarizado 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 por la que el encargado del banco de datos personales impide el acceso de terceros a los datos y éstos no pueden ser objeto de tratamiento, 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 previsto 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 de un banco de datos.

**4. Datos personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables 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 el grado de discapacidad y su información genética.

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

**7. Días:** Días hábiles.

**8. Dirección General de 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.

**9. Emisor o exportador de datos personales:** Es el titular del banco de datos personales o aquél que resulte responsable del tratamiento situado en el Perú que realice, conforme a lo dispuesto en el presente reglamento, una transferencia de datos personales a otro país.

**10. Encargado del tratamiento:** Es quien realiza el tratamiento de los datos personales, pudiendo ser el propio titular del banco de datos personales o el encargado del banco de datos personales u otra persona 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 de datos personales por orden del responsable del tratamiento cuando este se realice sin la existencia de un banco de datos personales.

**11. 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 o encargado del banco de datos personales, o como tercero.

**12. Rectificación:** Es aquella acción genérica destinada a afectar o modificar un banco de datos personales ya sea para actualizarlo incluir información en él o específicamente rectificar su contenido con datos exactos.

**13. Repertorio de jurisprudencia:** Es el banco de resoluciones judiciales o administrativas que se organizan como fuente de consulta y destinadas al conocimiento público.

**14. Responsable del tratamiento:** Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.

**15. Tercero:** Es toda persona natural, persona jurídica de derecho privado o entidad pública, distinta del titular de datos personales, del titular o encargado del banco de datos personales y del responsable del tratamiento, incluyendo a quienes tratan los datos bajo 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 3.- Ámbito de aplicación.**

El presente reglamento es de aplicación al tratamiento de los datos personales contenidos en un banco de datos personales o destinados a ser contenidos en bancos de datos personales.

Conforme a lo dispuesto por el numeral 6 del artículo 2 de la Constitución Política del Perú y el artículo 3 de la Ley, el presente reglamento se aplicará a toda modalidad de tratamiento de datos personales, ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado e independientemente del soporte en el que se encuentren.

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.

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 4.- Excepciones al ámbito de aplicación.**

Las disposiciones de este reglamento no serán de aplicación a:

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 contenidos o destinados a ser contenidos en bancos de datos personales de la administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de competencias asignadas por ley a las respectivas entidades públicas siempre que tengan por objeto:

2.1 La defensa nacional.
2.2 La seguridad pública y,
2.3 El desarrollo de actividades en materia penal para la investigación y represión del delito.

**Artículo 5.- Ámbito de aplicación territorial.**

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 del tratamiento no esté establecido en territorio peruano, pero le resulte aplicable la legislación peruana, por disposición contractual o del derecho internacional; y
4. El titular del banco de datos personales o quien resulte responsable no esté 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.

Para estos efectos, el responsable deberá proveer los medios que resulten necesarios para el efectivo cumplimiento de las obligaciones que imponen la Ley y el presente reglamento y designará un representante o implementar los mecanismos suficientes para estar en posibilidades de cumplir de manera efectiva, en territorio peruano, con las obligaciones que impone la legislación peruana.

Cuando el titular del banco de datos personales o quien resulte el responsable del tratamiento no se encuentre establecido en territorio peruano, pero el encargado del tratamiento lo esté, a este último le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el presente reglamento.

En el caso de personas naturales, el establecimiento se entenderá 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.

Tratándose de personas jurídicas, se entenderá 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 entenderá 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.

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

## TÍTULO II

### Principios rectores

**Artículo 6.- Principios rectores.**

El titular del banco de datos personales, o en su caso, quien resulte responsable del tratamiento, debe cumplir con los principios rectores de la protección de datos personales, de conformidad con lo establecido en la Ley, aplicando los criterios de desarrollo que se establecen en el presente título del reglamento.

**Artículo 7.- Principio de consentimiento.**

En atención al principio de consentimiento, el tratamiento de los datos personales es lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco. No se admiten fórmulas de consentimiento en las que éste no sea expresado de forma directa, como aquellas en las que se requiere presumir, o asumir la existencia de una voluntad que no ha sido expresa. Incluso el consentimiento prestado con otras declaraciones, deberá manifestarse en forma expresa y clara.

**Artículo 8.- Principio de finalidad.**

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

Tratándose de banco de datos personales que contengan datos sensibles, su creación solo puede justificarse si su finalidad además de ser legítima, es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales.

Los profesionales que realicen el tratamiento de algún dato personal, además de estar limitados por la finalidad de sus servicios, se encuentran obligados a guardar secreto profesional.

**Artículo 9.- Principio de calidad.**

En atención al principio de calidad, los datos contenidos en un banco de datos personales,

deben ajustarse con precisión a la realidad. Se presume que los datos directamente facilitados por el titular de los mismos son exactos.

**Artículo 10.- Principio de seguridad.**

En atención al principio de seguridad, en el tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley o al presente reglamento, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

## TÍTULO III

## Tratamiento de datos personales

### Capítulo I

### Consentimiento

Artículo 11.- Disposiciones generales sobre el consentimiento para el tratamiento de datos personales.

El titular del banco de datos personales o quien resulte como responsable del tratamiento, deberá 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.

La solicitud del consentimiento deberá 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 artículo siguiente sobre las características del consentimiento.

Cuando se solicite el consentimiento para una forma de tratamiento que incluya o pueda incluir la transferencia nacional o internacional de los datos, el titular de los mismos deberá ser informado de forma que conozca inequívocamente tal circunstancia, además de la finalidad a la que se destinarán sus datos y el tipo de actividad desarrollada por quien recibirá los mismos.

**Artículo 12.- Características del consentimiento.**

Además de lo dispuesto en el artículo 18 de la Ley y en el artículo precedente del presente reglamento, la obtención del consentimiento debe ser:

**1. Libre:** Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales.

La entrega de obsequios o el otorgamiento de beneficios al titular de los datos personales con ocasión de su consentimiento no afectan la condición de libertad que tiene para otorgarlo, salvo en el caso de menores de edad, en los supuestos en que se admite su consentimiento, en que no se considerará libre el consentimiento otorgado mediando obsequios o beneficios.

El condicionamiento de la prestación de un servicio, o la advertencia o 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.

**2. Previo:** Con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron.

**3. Expreso e Inequívoco:** Cuando el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento.

Se considera que el consentimiento expreso se otorgó verbalmente cuando el titular lo exterioriza oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral.

Se considera consentimiento escrito a aquél que otorga el titular mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por el ordenamiento jurídico que queda o pueda ser impreso en una superficie de papel o similar.

La condición de expreso no se limita a la manifestación verbal o escrita.

En sentido restrictivo y siempre de acuerdo con lo dispuesto por el artículo 7 del presente reglamento, se considerará consentimiento expreso a aquel que se manifieste mediante la conducta del titular que evidencie que ha consentido inequívocamente, dado que de lo contrario su conducta, necesariamente, hubiera sido otra.

Tratándose del entorno digital, también se considera expresa la manifestación consistente en "hacer clic", "cliquear" o "pinchar", "dar un toque", "touch" o "pad" u otros similares.

En este contexto el consentimiento escrito podrá otorgarse mediante firma electrónica, mediante escritura que quede grabada, de forma tal que pueda ser leída e impresa, o que por cualquier otro mecanismo o procedimiento establecido permita identificar al titular y recabar su consentimiento, a través de texto escrito. También podrá otorgarse mediante texto preestablecido, fácilmente visible, legible y en lenguaje sencillo, que el titular pueda hacer suyo, o no, mediante una respuesta escrita, gráfica o mediante clic o pinchado.

La sola conducta de expresar voluntad en cualquiera de las formas reguladas en el presente numeral no elimina, ni da por cumplidos, los otros requisitos del consentimiento referidos a la libertad, oportunidad e información.

**4. Informado:** Cuando al titular de los datos personales se le comunique clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos de lo siguiente:

a. 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.

b. La finalidad o finalidades del tratamiento a las que sus datos serán sometidos.

c. La identidad de los que son o pueden ser sus destinatarios, de ser el caso.

d. La existencia del banco de datos personales en que se almacenarán, cuando corresponda.

e. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.

f. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.

g. En su caso, la transferencia nacional e internacional de datos que se efectúen.

**Artículo 13.- Políticas de privacidad.**

La publicación de políticas de privacidad, de acuerdo a lo previsto en el segundo párrafo del artículo 18 de la Ley, debe entenderse como una forma de cumplimiento del deber de información que no exonera del requisito de obtener el consentimiento del titular de los datos personales.

**Artículo 14.- Consentimiento y datos sensibles.**

Tratándose de datos sensibles, el consentimiento debe ser otorgado por escrito, a través de su firma manuscrita, firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca del titular.

**Artículo 15.- Consentimiento y carga de la prueba.**

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

**Artículo 16.- Negación, revocación y alcances del consentimiento.**

El titular de los datos personales podrá 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 cumplirán los mismos requisitos observados con ocasión de su otorgamiento, pudiendo ser estos más simples, si así se hubiera señalado en tal oportunidad.

El titular de los datos personales podrá 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 podrá ser mayor a cinco (5) días.

Si la revocatoria afecta la totalidad del tratamiento de datos personales que se venía haciendo, el titular o encargado del banco de datos personales, o en su caso el responsable del tratamiento, aplicará las reglas de cancelación o supresión de datos personales.

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 17.- Fuentes accesibles al público.**

Para los efectos del artículo 2, inciso 9) de la Ley, se considerarán fuentes accesibles al 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.

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, debidamente anonimizados.

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 Nº 27806, Ley de Transparencia y Acceso a la Información Pública.

Lo dispuesto en el numeral precedente no quiere decir 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 pública accesible. La evaluación del acceso a datos personales en posesión de entidades de administración pública se hará atendiendo a las circunstancias de cada caso concreto.

El tratamiento de los datos personales obtenidos a través de fuentes de acceso público deberá respetar los principios establecidos en la Ley y en el presente reglamento.

## Capítulo III

### Transferencia de datos personales

**Artículo 18.- Disposiciones generales.**

La transferencia de datos personales implica la comunicación de datos personales dentro o fuera

del territorio nacional realizada a persona distinta al titular de los datos personales, al encargado del banco de datos personales o al encargado del tratamiento de datos personales.

Se denomina flujo transfronterizo de datos personales a la transferencia de datos personales fuera del territorio nacional.

Aquél a quien se transfieran los datos personales se obliga, por el solo hecho de la transferencia, a la observancia de las disposiciones de la Ley y del presente reglamento.

**Artículo 19.- Condiciones para la transferencia.**

Toda transferencia de datos personales requiere el consentimiento de su titular, salvo las excepciones previstas en el artículo 14 de la Ley y debe limitarse a la finalidad que la justifique.

**Artículo 20.- Prueba del cumplimiento de las obligaciones en materia de transferencias.**

Para efectos de demostrar que la transferencia se realizó conforme a lo que establece la Ley y el presente reglamento, la carga de la prueba recaerá, en todos los casos, en el emisor de datos.

**Artículo 21.- Transferencia dentro de un sector o grupo empresarial y código de conducta.**

En el caso de transferencias de datos personales dentro de grupos empresariales, sociedades subsidiarias afiliadas o vinculadas bajo el control común del mismo grupo del titular del banco de datos personales o responsable del tratamiento, o a 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 cumple con garantizar el tratamiento de datos personales, si se cuenta con un código de conducta que establezca las normas internas de protección de datos personales con el contenido previsto por el artículo 31 de la Ley, e inscrito según lo previsto por los artículos 89 a 97 del presente reglamento.

**Artículo 22.- Receptor de los datos personales.**

El receptor de los datos personales asume la condición de titular del banco de datos personales o responsable del tratamiento en lo que se refiere la Ley y el presente reglamento, y deberá realizar el tratamiento de los datos personales cumpliendo lo establecido en la información que el emisor dio de manera previa al consentimiento recabado del titular de los datos personales.

**Artículo 23.- Formalización de las transferencias nacionales.**

La transferencia deberá formalizarse mediante mecanismos que permitan demostrar que el titular del banco de datos personales o el responsable del tratamiento comunicó al responsable receptor las condiciones en las que el titular de los datos personales consintió el tratamiento de los mismos.

**Artículo 24.- Flujo transfronterizo de datos personales.**

Los flujos transfronterizos de datos personales serán posibles cuando el receptor o importador de los datos personales asuma las mismas obligaciones que corresponden al titular del banco de datos personales o responsable del tratamiento que como emisor o exportador transfirió los datos personales.

De conformidad con el artículo 15 de la Ley, además de los supuestos previstos en el primer y tercer párrafo de dicho artículo, lo dispuesto en el segundo párrafo del mismo tampoco aplica cuando se traten de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.

**Artículo 25.- Formalización del flujo transfronterizo de datos personales.**

Para los efectos del artículo precedente, el emisor o exportador podrá valerse de cláusulas contractuales 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.

**Artículo 26.- Participación de la Dirección General de Protección de Datos Personales respecto del flujo transfronterizo de datos personales.**

Los titulares del banco de datos personales o responsables del tratamiento, podrán solicitar la opinión de la Dirección General de Protección de Datos Personales respecto a si el flujo transfronterizo de datos personales que realiza o realizará cumple con lo dispuesto por la Ley y el presente reglamento.

En cualquier caso, el flujo transfronterizo de datos personales se pondrá en conocimiento de la Dirección General de Protección de Datos Personales, incluyendo la información que se requiere para la transferencia de datos personales y el registro de banco de datos.

## Capítulo IV

### Tratamientos especiales de datos personales

**Artículo 27.- Tratamiento de los datos personales de menores.**

Para el tratamiento de los datos personales de un menor de edad, se requerirá el consentimiento de los titulares de la patria potestad o tutores, según corresponda.

**Artículo 28.- Consentimiento excepcional.**

Podrá hacerse tratamiento de los datos personales de mayores de catorce y menores de dieciocho años con su consentimiento, siempre que la información proporcionada haya sido expresada en un lenguaje comprensible por ellos, salvo en los casos que la ley exija para su otorgamiento la asistencia de los titulares de la patria potestad o tutela.

En ningún caso el consentimiento para el tratamiento de datos personales de menores de edad podrá otorgarse para que accedan a actividades, vinculadas con bienes o servicios que están restringidos para mayores de edad.

**Artículo 29.- Prohibición de recopilación.**
En ningún caso se podrá recabar de un menor de edad datos 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.

Sólo podrá recabarse los datos de identidad y dirección de los padres o de los tutores con la finalidad de obtener el consentimiento a que se refiere el artículo 27 del presente reglamento.

**Artículo 30.- Fomento de la protección.**
Es obligación de todos los titulares de bancos de datos personales y 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 31.- Tratamiento de datos personales en el sector comunicaciones y telecomunicaciones.**
Los operadores de los servicios de comunicaciones o telecomunicaciones tienen la responsabilidad de velar por la confidencialidad, seguridad, uso adecuado e integridad de los datos personales que obtengan de sus abonados y usuarios, en el curso de sus operaciones comerciales. En tal sentido, no podrán 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 32.- Confidencialidad y seguridad.**
Los operadores de comunicaciones o telecomunicaciones deberán velar por la confidencialidad, seguridad y uso adecuado de cualquier dato personal obtenido como consecuencia de su actividad y adoptarán las medidas técnicas, legales y organizativas, conforme a lo establecido en la Ley y el presente reglamento, sin perjuicio de las medidas establecidas en las normas del sector de comunicaciones y telecomunicaciones que no se opongan a lo establecido en la Ley y el presente reglamento.

**Artículo 33.- Tratamiento de los datos personales por medios tecnológicos tercerizados.**
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.

Para los casos en los que en el tratamiento exista intervención humana se aplican los artículos 37 y 38.

El tratamiento de datos personales por medios tecnológicos tercerizados, sea completo o parcial, podrá 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 34.- 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 deberá considerar como prestaciones mínimas las siguientes:

1. Informar 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 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 la destrucción o la imposibilidad de acceder a los datos personales después de concluida la prestación.

**Artículo 35.- Mecanismos para la prestación del servicio de tratamiento de datos personales por medios tecnológicos tercerizados.**
El prestador del servicio deberá contar 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 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 36.- Prestación de servicios o tratamiento por encargo.**
Para efectos de la Ley, la entrega de datos personales del titular del banco de datos personales al encargado no constituye transferencia de datos personales.

El encargado del banco 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 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.

El plazo para la conservación de los datos será de dos (2) años contado desde la finalización del último encargo realizado.

Lo dispuesto en el presente artículo será aplicable, en lo que corresponda, a la subcontratación de la prestación de servicios de tratamiento de datos personales.

**Artículo 37.- Tratamiento a través de subcontratación.**

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.

Para este supuesto se requerirá de manera previa una autorización por parte del titular del banco de datos personales o responsable del tratamiento. Dicha autorización se entenderá 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. El tratamiento que haga el subcontratista se realizará en nombre y por cuenta del responsable del tratamiento, pero la carga de probar la autorización le corresponde al encargado del tratamiento.

**Artículo 38.- 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, asumirá las obligaciones del titular del banco de datos personales o encargado del tratamiento 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

### Medidas de seguridad

**Artículo 39.- Seguridad para el tratamiento de la información digital.**

Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento:

1. El control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario-contraseña, uso de certificados digitales, tokens, entre otros, y realizar una verificación periódica de los privilegios asignados, los cuales deben estar definidos mediante un procedimiento documentado a fin de garantizar su idoneidad.
2. Generar y mantener registros que provean evidencia sobre 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 relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros.

Asimismo, se deben establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales.

**Artículo 40.- Conservación, respaldo y recuperación de los datos personales.**

Los ambientes en los que se procese, almacene o transmita la información deberán ser implementados, con controles de seguridad apropiados, tomando como referencia las recomendaciones de seguridad física y ambiental recomendados en la "NTP ISO/IEC 17799 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de Seguridad de la Información." en la edición que se encuentre vigente.

Adicionalmente, se deben contemplar los mecanismos de respaldo de seguridad de la información de la base de datos personales con un procedimiento que contemple la verificación de la integridad de los datos almacenados en el respaldo, incluyendo cuando sea pertinente, la recuperación completa ante una interrupción o daño, garantizando el retorno al estado en el que se encontraba al momento en que se produjo la interrupción o daño.

**Artículo 41.- 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 procederá con la autorización del titular del banco de datos personales y se hará utilizando los medios de transporte autorizados por el mismo, tomando las medidas necesarias, entre las que se encuentran cifrado de datos, firmas digitales, información, checksum de verificación, entre otros, destinados a evitar el acceso no autorizado, pérdida o corrupción durante el tránsito hacia su destino.

**Artículo 42.- Almacenamiento de documentación no automatizada.**

Los armarios, archivadores u otros elementos en los que se almacenen documentos no automatizados con datos personales deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el banco de datos.

Si por las características de los locales que se dispusiera no fuera posible cumplir lo establecido

en el apartado anterior, se adoptarán las medidas alternativas, conforme a las directivas de la Dirección General de Protección de Datos Personales.

**Artículo 43.- Copia o reproducción.**
La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado.
Deberá 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 44.- Acceso a la documentación.**
El acceso a la documentación se limitará exclusivamente al personal autorizado.
Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo a las directivas de seguridad que emita la Dirección General de Protección de Datos Personales.

**Artículo 45.- Traslado de documentación no automatizada.**
Siempre que se proceda al traslado físico de la documentación contenida en un banco de datos, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

**Artículo 46.- Prestaciones de servicios sin acceso a datos personales.**
El responsable o el encargado de la información o tratamiento adoptarán las medidas 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.
Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá 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.

## TÍTULO IV

## Derechos del titular de datos personales

### Capítulo I

### Disposiciones generales

**Artículo 47.- 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 48.- 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 49.- Legitimidad para ejercer los derechos.**
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.
Cuando el titular del banco de datos personales sea una entidad pública, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, conforme al artículo 115 de la Ley Nº 27444, Ley del Procedimiento Administrativo General.
4. En caso se opte por el procedimiento señalado en el artículo 51 del presente reglamento, la acreditación de la identidad del titular se sujetará a lo dispuesto en dicha disposición.

**Artículo 50.- 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, la misma que contendrá:

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 51.- Servicios de atención al público.**
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, podrá 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.

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 aquél, siempre que se acredite la misma, conforme a la naturaleza de la prestación del servicio o producto ofertado.

**Artículo 52.- Recepción y subsanación de la petición.**

Deben ser recibidas todas las solicitudes presentadas, dejándose constancia de su recepción por parte del titular del banco de datos personales o responsable del tratamiento. En caso de que la solicitud no cumpla con los requisitos señalados en el artículo anterior, 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 por incumplimiento 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 tendrá por no presentada la solicitud.

Las entidades públicas aplican el artículo 126 de la Ley Nº 27444, Ley del Procedimiento Administrativo General, sobre observaciones a la documentación presentada.

**Artículo 53.- Facilidades para el ejercicio del derecho.**

El titular del banco de datos personales o responsable del tratamiento está obligado a establecer un procedimiento sencillo para el ejercicio de los derechos. Sin perjuicio de lo señalado e independientemente de los medios o mecanismos que la Ley y el presente reglamento establezcan para el ejercicio de los derechos correspondientes al titular de datos personales, el titular del banco de datos personales o el responsable del tratamiento, podrá ofrecer mecanismos que faciliten el ejercicio de tales derechos en beneficio del titular de datos personales.

Para efectos de la contraprestación que debe abonar el titular de datos personales para el ejercicio de sus derechos ante la administración pública se estará a lo dispuesto en el primer párrafo del artículo 26 de la Ley.

El ejercicio por el titular de datos personales de sus derechos ante los bancos de datos personales de administración privada será de carácter gratuito, salvo lo establecido en normas especiales de la materia. En ningún caso el ejercicio de estos derechos implicará ingreso adicional para el titular del banco de datos personales o responsable del tratamiento ante el cual se ejercen.

No se podrá 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.

**Artículo 54.- Forma de la respuesta.**

El titular del banco de datos personales o responsable del tratamiento deberá dar respuesta 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.

La respuesta al titular de datos personales deberá referirse únicamente a aquellos datos que específicamente se hayan indicado en su solicitud y deberá presentarse en forma clara, legible, comprensible y de fácil acceso.

En caso de ser necesario el empleo de claves o códigos, deberán proporcionarse los significados correspondientes.

Corresponderá 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 será 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 55.- Plazos de respuesta.**

1. El plazo máximo de respuesta del titular del banco de datos personales o responsable del tratamiento ante el ejercicio del derecho de información será de ocho (08) días contados desde el día siguiente de la presentación de la solicitud correspondiente.

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

Si la solicitud fuera estimada y el titular del banco de datos personales o responsable del tratamiento no acompañase a su respuesta la información solicitada, el acceso será efectivo dentro de los diez (10) días siguientes a dicha respuesta.

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 del tratamiento será de diez (10) días contados desde el día siguiente de la presentación de la solicitud correspondiente.

**Artículo 56.- Requerimiento de información adicional.**

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 podrá requerir dentro de los siete (7) días siguientes de recibida la solicitud, documentación adicional al titular de los datos personales para atenderla.

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 acompañará la documentación adicional que estime pertinente para fundamentar su solicitud. En caso contrario, se tendrá por no presentada dicha solicitud.

**Artículo 57.- Ampliación de los plazos.**

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, podrán ser ampliados una sola vez, y por un plazo igual, como máximo, siempre y cuando las circunstancias lo justifiquen.

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

**Artículo 58.- Aplicación de legislación específica.**

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, serán de aplicación las mismas en cuanto ofrezcan iguales o mayores garantías al titular de los datos personales y no contravengan lo dispuesto en la Ley y el presente reglamento.

**Artículo 59.- 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 del titular de datos personales, debe estar debidamente justificada y debe señalar el derecho que le asiste al mismo para recurrir ante la Dirección General de Protección de Datos Personales en vía de reclamación, en los términos del artículo 24 de la Ley y del presente reglamento.

## Capítulo II

### Disposiciones especiales

**Artículo 60.- Derecho a la información.**

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 y el numeral 4 del artículo 12 del presente reglamento.

La respuesta contendrá los extremos previstos en los artículos citados en el párrafo anterior, salvo que el titular haya solicitado la información referida sólo a alguno de ellos.

Será de aplicación para la respuesta al ejercicio del derecho a la información, en lo que fuere pertinente, lo establecido en los artículos 62 y 63 del presente reglamento.

**Artículo 61.- Derecho de acceso.**

Sin perjuicio de lo señalado en el artículo 19 de la Ley, el titular de los datos personales tiene derecho a obtener del titular del banco de datos personales o responsable del tratamiento la información relativa a sus datos personales, así como a todas las condiciones y generalidades del tratamiento de los mismos.

**Artículo 62.- Medios para el cumplimiento del derecho de acceso.**

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

El titular de los datos personales podrá optar a través de algunos o varios 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 confidencialidad, integridad 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.

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. Asimismo, el acceso debe ser en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. Sin perjuicio de lo cual, con el objeto de usar los medios de comunicación más ecológicos disponibles en cada caso, el responsable del tratamiento podrá acordar con el titular el uso de medios de reproducción de la información distintos a los establecidos en el presente reglamento.

**Artículo 63.- 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 la totalidad del registro correspondiente al titular de datos personales, aun cuando el requerimiento sólo comprenda un aspecto de dichos datos. El informe no podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

**Artículo 64.- Actualización.**

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.

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

**Artículo 65.- Rectificación.**

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

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 66.- Inclusión.**

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.

La solicitud de inclusión deberá indicar a qué datos personales 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 67.- Supresión o cancelación.**

El titular de los datos personales podrá solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando éstos 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.

La solicitud de supresión o cancelación podrá referirse a todos los datos personales del titular contenidos en un banco de datos personales o sólo a alguna parte de ellos.

Dentro de lo establecido por el artículo 20 de la Ley y el numeral 3) del artículo 2 del presente reglamento, la solicitud de supresión implica el cese en el tratamiento de los datos personales a partir de un bloqueo de los mismos y su posterior eliminación.

**Artículo 68.- Comunicación de la supresión o cancelación.**

El titular del banco de datos personales o responsable del tratamiento deberá 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 69.- Improcedencia de la supresión o cancelación.**

La supresión no procederá 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 70.- 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 párrafo precedente, se deberán emplear medios de disociación o anonimización para continuar el tratamiento.

**Artículo 71.- Oposición.**

El titular de datos personales tiene derecho a 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.

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.

En caso que la oposición resulte justificada el titular del banco de datos personales o responsable de su tratamiento deberá proceder al cese del tratamiento que ha dado lugar a la oposición.

**Artículo 72.- Derecho al tratamiento objetivo de datos personales.**

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 deberá 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 73.- Procedimiento de tutela directa.**

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, de acuerdo a las características que se regulan en los artículos precedentes del presente título.

El titular del banco de datos personales o responsable del tratamiento deberá dar respuesta, en los plazos previstos en el artículo 55 del presente reglamento, expresando lo correspondiente a cada uno de los extremos de la solicitud. Transcurrido el plazo sin haber recibido la respuesta el solicitante podrá considerar denegada su solicitud.

La denegatoria o la respuesta insatisfactoria habilitan al solicitante a iniciar el procedimiento administrativo ante la Dirección General de Protección de Datos Personales, de acuerdo al artículo 74 del presente reglamento.

**Artículo 74.- Procedimiento trilateral de tutela.**

El procedimiento administrativo de tutela de los derechos regulados por la Ley y el presente reglamento, se sujeta a lo dispuesto por los artículos 219 al 228 de la Ley Nº 27444, Ley del Procedimiento Administrativo General en lo que le sea aplicable, y será resuelto mediante resolución del Director General de Protección de Datos Personales. Contra esta resolución solo procede recurso de reconsideración, el que, una vez resuelto, agota la vía administrativa.

Para iniciar el procedimiento administrativo a que se refiere este artículo, sin perjuicio de los requisitos generales previstos en el presente reglamento, el titular de los datos personales deberá presentar con su solicitud de tutela:

1. El cargo de la solicitud que previamente envió al titular del banco de datos personales o responsable del tratamiento para obtener de él, directamente, la tutela de sus derechos.
2. El documento que contenga la respuesta del titular del banco de datos personales o responsable

**Artículo 82.- Subsanación de los defectos y archivamiento.**

Si la solicitud presentada no cumple con los requisitos exigidos por el reglamento, la Dirección de Registro Nacional de Protección de Datos Personales requerirá al solicitante que en el plazo de diez (10) días subsane la omisión. Vencido el plazo máximo, sin que el interesado haya cumplido con subsanar dicha omisión, se procederá al archivamiento de la solicitud.

**Artículo 83.- Resolución de inscripción.**

El Director de la Dirección de Registro Nacional de Protección de Datos Personales emitirá la resolución disponiendo la inscripción del banco de datos personales, siempre que se ajuste a los requisitos exigidos en la Ley y el presente reglamento.

La resolución debe consignar:

1. El código asignado por el Registro.
2. La identificación del banco de datos personales.
3. La descripción de la finalidad y usos previstos.
4. La identificación del titular del banco de datos personales.
5. La categoría de los datos personales que contiene.
6. Los procedimientos de obtención.
7. El sistema de tratamiento de los datos personales y la indicación de las medidas de seguridad.

Asimismo, se incluirán, en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el banco de datos personales y los receptores de los datos personales y del flujo transfronterizo.

Una vez inscrito el banco de datos personales en el Registro Nacional de Protección de Datos, se notificará la decisión al interesado.

La inscripción de un banco de datos personales en el Registro Nacional de Protección de Datos no exime al titular del cumplimiento del resto de las obligaciones previstas en la Ley y el presente reglamento.

**Artículo 84.- Modificación o cancelación de bancos de datos personales.**

La inscripción de un banco de datos personales deberá mantenerse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción deberá ser previamente comunicada a la Dirección de Registro Nacional de Protección de Datos Personales para su inscripción.

Cuando el titular de un banco de datos personales decida su cancelación, deberá comunicarla a la Dirección de Registro Nacional de Protección de Datos Personales, a efectos de que proceda a la cancelación de la inscripción. El solicitante precisará el destino que va a darse a los datos o las previsiones para su destrucción.

**Artículo 85.- Duración del procedimiento.**

El plazo máximo para emitir la resolución acerca de la inscripción, modificación o cancelación será de treinta (30) días.

Si en dicho plazo no se hubiese emitido resolución expresa, se entenderá inscrito, modificado o cancelado el banco de datos personales, para todos los efectos.

**Artículo 86.- Improcedencia o denegación de la inscripción.**

El Director de la Dirección de Registro Nacional de Protección de Datos emitirá resolución denegando la inscripción cuando la solicitud no cumpla con los requisitos dispuestos en la Ley y en el presente reglamento u otras disposiciones que dicte la Dirección General de Protección de Datos Personales de conformidad a las facultades legales conferidas.

La resolución debe estar debidamente motivada, con indicación expresa de las causas que impiden la inscripción, modificación o cancelación.

**Artículo 87.- Impugnación.**

Contra la resolución que deniega la inscripción proceden los recursos de reconsideración y apelación, conforme al procedimiento señalado en la Ley Nº 27444, Ley del Procedimiento Administrativo General.

**Artículo 88.- Las instancias.**

La Dirección de Registro Nacional de Protección de Datos Personales constituye la primera instancia para efectos de atender los recursos administrativos interpuestos contra la denegatoria de inscripción de un banco de datos personales. Resolverá los recursos de reconsideración y elevará los de apelación a la Dirección General de Protección de Datos Personales que resolverá en última instancia administrativa por la procedencia o improcedencia de la inscripción.

## Capítulo III

### Procedimiento de inscripción de los códigos de conducta

**Artículo 89.- Ámbito de aplicación de los códigos de conducta.**

1. Los códigos de conducta tendrán carácter voluntario.
2. Los códigos de conducta de carácter sectorial podrán referirse a la totalidad o a parte de los tratamientos llevados a cabo por el sector, debiendo ser formulados por organizaciones representativas del mismo.
3. Los códigos de conducta promovidos por una empresa o grupo empresarial deberán referirse a la totalidad de los tratamientos llevados a cabo por los mismos.

**Artículo 90.- Contenido.**

1. Los códigos de conducta deben estar redactados en términos claros y accesibles.
2. Los códigos de conducta deben estar adecuados a lo establecido en la Ley e incluir como mínimo los siguientes aspectos:

2.1. La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.

2.2. Las previsiones específicas para la aplicación de los principios de protección de datos personales.

2.3. El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley.

2.4. El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de información, acceso, rectificación, cancelación y oposición.

2.5. 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.

2.6. Las acciones de fomento y difusión en materia de protección de datos personales dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.

2.7. Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código de conducta.

3. En particular, deberá consignarse en el código:

3.1 Cláusulas para la obtención del consentimiento de los titulares de los datos personales al tratamiento o transferencia de sus datos personales.

3.2 Cláusulas para informar a los titulares de los datos personales del tratamiento, cuando los datos no sean obtenidos de los mismos.

3.3 Modelos para el ejercicio por los afectados de sus derechos de información, acceso, rectificación, cancelación y oposición.

3.4 De ser el caso, modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento.

**Artículo 91.- Inicio del procedimiento.**

El procedimiento para la inscripción en el Registro Nacional de Protección de Datos Personales de los códigos de conducta se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código de conducta.

La solicitud, además de reunir los requisitos legalmente establecidos, cumplirá los siguientes requisitos adicionales:

1. Acreditación de la representación con que cuente la persona que presente la solicitud.

2. Contenido del acuerdo, convenio o decisión por la que se aprueba en el ámbito correspondiente el contenido del código de conducta presentado.

3. En caso de que el código de conducta proceda de un acuerdo sectorial o una decisión de empresa, se adjuntará la certificación referida a la adopción del acuerdo y legitimación del órgano que lo adoptó y copia de los estatutos de la asociación, organización sectorial o entidad en cuyo marco haya sido aprobado el código.

4. En caso de códigos de conducta presentados por asociaciones u organizaciones de carácter sectorial, se adjuntará documentación relativa a su representatividad en el sector.

5. En caso de códigos de conducta basados en decisiones de empresa, se adjuntará descripción de los tratamientos a los que se refiere.

**Artículo 92.- Subsanación de los defectos.**

Analizados los aspectos sustantivos del código de conducta, si resultase necesaria la aportación de nuevos documentos o la modificación de su contenido, la Dirección de Registro Nacional de Protección de Datos Personales requerirá al solicitante que en el plazo de diez (10) días realice las modificaciones precisadas.

**Artículo 93.- Trámite.**

Transcurrido el plazo señalado en el artículo anterior, la Dirección de Registro Nacional de Protección de Datos Personales elaborará un informe sobre las características del proyecto de código de conducta que será enviado a la Dirección de Normatividad y Asistencia Legal, para que informe en el plazo de siete (07) días si cumple con lo requerido por la Ley y el presente reglamento.

**Artículo 94.- Emisión de la resolución.**

Cumplido lo establecido en los artículos precedentes, el Director de la Dirección de Registro Nacional de Protección de Datos Personales emitirá la resolución disponiendo la inscripción del código de conducta, siempre que se ajuste a los requisitos exigidos en la Ley y el presente reglamento.

**Artículo 95.- Duración del procedimiento.**

El plazo máximo para emitir la resolución será de treinta (30) días, contado desde la fecha de presentación de la solicitud ante la Dirección de Registro Nacional de Protección de Datos Personales. Si en dicho plazo no se hubiese emitido la resolución, el solicitante podrá considerar estimada su solicitud.

**Artículo 96.- Improcedencia o denegación de la inscripción.**

La denegatoria de la inscripción del código de conducta será resuelta mediante resolución del Director de la Dirección de Registro Nacional de Protección de Datos Personales, cuando dicha solicitud no cumpla con los requisitos dispuestos en la Ley, el presente reglamento y aquellas disposiciones que dicte la Dirección General de Protección de Datos Personales, en el marco de sus competencias legales y estatutarias.

Contra la resolución que deniega la inscripción proceden los recursos de reconsideración y apelación, conforme al procedimiento señalado en los artículos 87 y 88 del presente reglamento.

**Artículo 97.- Publicidad**

El Registro Nacional de Protección de Datos Personales dará publicidad al contenido de los códigos de conducta utilizando para ello medios electrónicos o telemático.

## TÍTULO VI

Infracciones y sanciones

### Capítulo I

Procedimiento fiscalizador

**Artículo 98.- Objeto.**
El procedimiento de fiscalización tendrá por objeto determinar si concurren las circunstancias que justifiquen la iniciación del procedimiento sancionador, con identificación del titular del banco de datos personales o del responsable del tratamiento y la presunta comisión de actos contrarios a la Ley y al presente reglamento.

**Artículo 99.- Inicio del procedimiento de fiscalización.**
El procedimiento de fiscalización se inicia siempre de oficio como consecuencia de:

1. Iniciativa directa de la Dirección de Supervisión y Control o del Director General de Protección de Datos Personales.
2. Por denuncia de cualquier entidad pública, persona natural o jurídica.

En ambos casos, la Dirección de Supervisión y Control requerirá 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. En el caso de las visitas de fiscalización a las sedes de las entidades públicas o privadas donde se encuentren los bancos de datos personales que administran, los fiscalizadores tendrán acceso a los mismos.

**Artículo 100.- Reconducción del procedimiento.**
En caso que, de la denuncia presentada pueda percibirse que no se dirige a los objetivos de un procedimiento de fiscalización, sino a los de la tutela de derechos, se derivará al procedimiento correspondiente.

**Artículo 101.- Fe pública.**
En el ejercicio de las funciones de fiscalización, el personal de la Dirección de Supervisión y Control estará dotado de fe pública para constatar la veracidad de los hechos en relación con los trámites a su cargo.

**Artículo 102.- Requisitos de la denuncia.**
La denuncia deberá indicar lo siguiente:

1. Nombre del denunciante y el domicilio para efectos de recibir las notificaciones.
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 103.- Forma de la denuncia.**
La denuncia podrá presentarse en soporte físico o según los formatos tipo automatizados, que se exhiban en el Portal Institucional del Ministerio de Justicia y Derechos Humanos.

Cuando la denuncia se presente por medios electrónicos a través del sistema que establezca la Dirección General de Protección de Datos Personales, se entenderá que se acepta que las notificaciones sean efectuadas por dicho sistema o a través de otros medios electrónicos generados por éste, salvo que se señale un medio distinto.

**Artículo 104.- Requerimiento de información.**
Cuando se formule denuncia, la Dirección de Supervisión y Control podrá solicitar la documentación que estime oportuna al denunciante para el desarrollo del procedimiento.

**Artículo 105.- Desarrollo de la fiscalización.**
El procedimiento de fiscalización tendrá una duración máxima de noventa (90) días, este plazo corre desde la fecha en que la Dirección de Supervisión y Control recibe la denuncia o da inicio de oficio al procedimiento y concluirá con el informe que se pronunciará sobre la existencia de elementos que sostengan o no, la presunta comisión de infracciones previstas en la Ley.

El plazo establecido podrá ser ampliado por una vez y hasta por un periodo de cuarenta y cinco (45) días, por decisión motivada, atendiendo a la complejidad de la materia fiscalizada y con conocimiento del Director General de Protección de Datos Personales.

**Artículo 106.- Programa de visitas.**
La fiscalización podrá incluir diversas visitas para obtener los elementos de convicción necesarios, las cuales se desarrollarán con un plazo máximo de diez (10) días entre cada una. Luego de la primera visita, se notificará un programa de visitas al titular del banco de datos personales o al encargado o al responsable del tratamiento y, en su caso, al denunciante.

**Artículo 107.- Identificación del personal fiscalizador.**
Al iniciar la visita, el personal fiscalizador deberá exhibir credencial vigente con fotografía, expedida por la Dirección General de Protección de Datos Personales que lo acredite como tal.

**Artículo 108.- Visitas de fiscalización.**
El personal que lleve a cabo las visitas de fiscalización deberá estar provisto de orden escrita motivada con firma autógrafa del funcionario, de la que dejará copia, con cargo, a la persona que atendió la visita.

En la orden deberá precisarse el lugar o los lugares en donde se encuentra la entidad pública o privada o la persona natural que se fiscalizará, 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 109.- Acta de fiscalización.**
Las visitas de fiscalización requieren el levantamiento del acta correspondiente, en la que quedará constancia de las actuaciones practicadas

durante la visita de verificación. Dicha acta se levantará en presencia de dos testigos propuestos por la persona con quien se entendió la diligencia. Si se hubiera negado a proponerlos o no hubieran participado los propuestos, bastará la firma de la persona con quien se entendió la diligencia o la constancia de su negativa a firmar, de ser el caso.

El acta se elaborará por duplicado y será firmada por el personal fiscalizador y quienes hayan participado en la diligencia. El acta puede incluir la manifestación que los participantes consideren que conviene a su derecho.

Se entregará al fiscalizado uno de los originales del acta de fiscalización, incorporándose el otro a los actuados.

**Artículo 110.- Contenido de las actas de fiscalización.**

En las actas de fiscalización se hará 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. Número y fecha de la orden de fiscalización que la motivó.
5. Nombre y cargo de la persona que atendió a los fiscalizadores.
6. Nombre y domicilio de las personas que participaron como testigos.
7. Datos y detalles relativos a la actuación.
8. Declaración del fiscalizado si lo solicitase.
9. Nombre y firma de quienes intervinieron en la fiscalización, incluyendo los de quienes la hubieran llevado a cabo. Si se negara a firmar el fiscalizado, su representante legal o la persona que atendió al fiscalizador, ello no afectará la validez del acta, debiendo el personal fiscalizador asentar la respectiva razón.

La firma del fiscalizado no supondrá su conformidad con el contenido, sino tan sólo su participación y la recepción de la misma.

**Artículo 111.- Obstrucción a la fiscalización.**

Si el fiscalizado se negara directamente a colaborar u observara 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, se dejará constancia en el acta, con precisión del acto o los actos obstructivos y de su naturaleza sistemática, de ser el caso.

**Artículo 112.- 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 a los hechos contenidos en el acta, también podrán hacerlo por escrito dentro del término de los cinco (5) días siguientes a la fecha en que se hubiere levantado.

**Artículo 113.- Informe.**

El procedimiento de fiscalización concluirá con el informe que expida la Dirección de Supervisión y Control, en el que determinará con carácter preliminar las circunstancias que justifiquen la instauración del procedimiento sancionador o la ausencia de ellas.

De ser el caso, se establecerán las medidas que deberá ordenarse al presunto responsable, en vía cautelar. La instrucción del procedimiento sancionador se llevará a cabo conforme a lo dispuesto por la Ley y el presente reglamento.

La determinación de la presunta responsabilidad por actos contrarios a lo establecido en la Ley y el presente reglamento contenida en el Informe, será notificada al fiscalizado y al denunciante, de ser el caso, en un plazo que no excederá de cinco (5) días.

**Artículo 114.- Improcedencia de medios de impugnación.**

En contra del informe de fiscalización que expide la Dirección de Supervisión y Control no procede la interposición de recurso alguno, la contradicción de su contenido y cualquier forma de defensa respecto de él se harán valer en el procedimiento sancionador, de ser el caso.

## Capítulo II

### Procedimiento sancionador

**Artículo 115.- Autoridades del procedimiento sancionador.**

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

1. El Director de la Dirección de Sanciones es la autoridad que instruye y resuelve, en primera instancia, sobre la existencia de infracción e imposición o no de sanciones y sobre obligaciones accesorias tendientes a la protección de los datos personales. Asimismo, 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, o no, de los actos contrarios a lo establecido en la Ley y el presente reglamento.
2. El Director General de Protección de Datos Personales resuelve en segunda y última instancia el procedimiento sancionador y su decisión agota la vía administrativa.

**Artículo 116.- Inicio del procedimiento sancionador.**

El procedimiento sancionador será promovido siempre de oficio, en atención a un informe de la Dirección de Supervisión y Control que puede obedecer a una denuncia de parte o a decisión motivada del Director General de Protección de Datos Personales.

**Artículo 117.- Rechazo liminar.**

La Dirección de Sanciones puede, mediante resolución expresa y motivada, decidir el archivamiento de los casos que no ameriten el inicio del procedimiento sancionador, no obstante el informe de la Dirección de Supervisión y Control. Contra esta decisión puede recurrir el denunciante.

**Artículo 118.- Medidas cautelares y correctivas.**

Una vez iniciado el procedimiento sancionador, la Dirección de Sanciones podrá disponer, mediante acto motivado, 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 Nº 27444, Ley del Procedimiento Administrativo General.

Asimismo, sin perjuicio de la sanción administrativa que corresponda por una infracción a las disposiciones contenidas en la Ley y el presente reglamento, se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones.

**Artículo 119.- Contenido de la resolución de inicio del procedimiento sancionador.**

1. La Dirección de Sanciones notifica la resolución de inicio del procedimiento sancionador que contendrá:
2. La identificación de la autoridad que emite la notificación.
3. La indicación del expediente correspondiente y la mención del acta de fiscalización, de ser el caso.
4. La identificación de la entidad pública o privada a quien se le abre procedimiento.
5. La decisión de abrir procedimiento sancionador.
6. El relato de los antecedentes que motivan el inicio del procedimiento 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.
7. La sanción o sanciones, que en su caso se pudieran imponer.
8. El plazo para presentar los descargos y pruebas.

**Artículo 120.- Presentación de descargos y pruebas.**

El administrado en un plazo máximo de quince (15) días, contado a partir del día siguiente de la notificación correspondiente presentará su descargo, en el cual podrá 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 podrá presentar los argumentos por medio de los cuales desvirtúe la infracción que se presuma y las pruebas correspondientes.

En caso se ofrezca prueba pericial o testimonial, se precisarán los hechos sobre los que versarán y se señalarán los nombres y domicilios del perito o de los testigos, exhibiéndose el cuestionario o el interrogatorio respectivo en preparación de las mismas. Sin estos requisitos dichas pruebas se tendrán por no ofrecidas.

**Artículo 121.- 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 Sanciones realizará de oficio todas las actuaciones necesarias para el examen de los hechos y podrá disponer una visita de fiscalización a cargo de la Dirección de Supervisión y Control, si no se hubiere hecho 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 122.- Cierre de instrucción y término del procedimiento sancionador.**

Concluidas las actuaciones instructivas, la Dirección de Sanciones emitirá resolución cerrando la etapa instructiva dentro de los cincuenta (50) días contados desde el inicio del procedimiento.

Dentro de los veinte (20) días posteriores a la notificación de la resolución de cierre de la etapa instructiva, la Dirección de Sanciones deberá resolver en primera instancia.

Podrá solicitarse informe oral dentro de los cinco (5) días posteriores a la notificación de la resolución de cierre de la etapa instructiva.

Cuando haya causa justificada, la Dirección de Sanciones podrá ampliar por una vez y hasta por un período igual, el plazo de cincuenta (50) días al que refiere el presente artículo.

La resolución que resuelve el procedimiento sancionador será notificada a todas las partes intervinientes en el procedimiento.

**Artículo 123.- Impugnación.**

Contra la resolución que resuelve el procedimiento sancionador proceden los recursos de reconsideración o apelación dentro de los quince (15) días de notificada la resolución al administrado.

El recurso de reconsideración se sustentará en nueva prueba y será resuelto por la Dirección de Sanciones en un plazo que no excederá de los treinta (30) días.

El recurso de apelación será resuelto por el Director General de Protección de Datos Personales, debiendo dirigirse a la misma autoridad que expidió el acto que se impugna, para que eleve lo actuado. El recurso de apelación deberá ser resuelto en un plazo no mayor de treinta (30) días.

## Capítulo III

### Sanciones

**Artículo 124.- Determinación de la sanción administrativa de multa.**

Las multas se determinan en función a la Unidad Impositiva Tributaria vigente a la fecha en que se cometió la infracción y cuando no sea posible establecer tal fecha, la que estuviere vigente a la fecha en que la Dirección General de Protección de Datos Personales detectó la infracción.

**Artículo 125.- Graduación del monto de la sanción administrativa de multa.**

Para graduar la sanción a imponerse debe observarse el principio de razonabilidad de la potestad sancionadora reconocido en el numeral 3 del artículo 230 de la Ley Nº 27444, Ley del Procedimiento Administrativo General, así como la condición de sancionado reincidente y la conducta procedimental del infractor.

En caso de que las infracciones continúen, luego de haber sido sancionado, debe imponerse una sanción mayor a la previamente impuesta conforme a los términos establecidos en el numeral 7 del artículo 230 de la Ley Nº 27444, Ley del Procedimiento Administrativo General.

**Artículo 126.- Atenuantes.**

La colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones acompañado de acciones de enmienda se considerarán atenuantes. Atendiendo a la oportunidad del reconocimiento y a las fórmulas de enmienda, la atenuación permitirá incluso la reducción motivada de la sanción por debajo del rango previsto en la Ley.

**Artículo 127.- Mora en el pago de las multas.**

El administrado que no realiza el pago oportuno de las multas incurre en mora automática, en consecuencia el monto de las multas impagas devengará interés moratorio que se aplicará 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. La Tasa de Interés Moratoria (TIM) diaria vigente resulta de dividir la Tasa de Interés Moratoria (TIM) vigente entre treinta (30).

**Artículo 128.- Incentivos para el pago de la sanción de multa.**

Se considerará que el sancionado ha cumplido con pagar la sanción de multa si, antes de vencer el plazo otorgado para pagar la multa, deposita en la cuenta bancaria determinada por la Dirección General de Protección de Datos Personales el sesenta por ciento (60%) de su monto. Para que surta efecto dicho beneficio deberá comunicar tal hecho a la Dirección General de Protección de Datos Personales, adjuntando el comprobante del depósito bancario correspondiente. Luego de dicho plazo, el pago sólo será admitido por el íntegro de la multa impuesta.

**Artículo 129.- Ejecución de la sanción de multa.**

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

**Artículo 130.- Registro de sanciones, medidas cautelares y correctivas.**

La Dirección de Registro Nacional de Protección de Datos Personales tendrá a su cargo el Registro de Sancionados por incumplimiento de la Ley y el presente reglamento, el Registro de Medidas Cautelares y el Registro de Medidas Correctivas, los mismos que serán publicados en el Portal Institucional del Ministerio de Justicia y Derechos Humanos.

**Artículo 131.- Aplicación de multas coercitivas**

En caso de incumplimiento de obligaciones accesorias a la sanción de multa impuesta por infracción a la Ley y el presente reglamento, la Dirección de Sanciones podrá imponer multas coercitivas de acuerdo a la siguiente graduación:

1. Por incumplimiento de obligaciones accesorias a la sanción de multa impuestas por infracciones leves, la multa coercitiva será desde cero coma dos a dos Unidades Impositivas Tributarias (0,2 a 2 UIT).
2. Por incumplimiento de obligaciones accesorias a la sanción de multa impuestas por infracciones graves, la multa coercitiva será de dos a seis Unidades Impositivas Tributarias (2 a 6 UIT).
3. Por incumplimiento de obligaciones accesorias a la sanción de multa impuestas por infracciones muy graves, la multa coercitiva será de seis a diez Unidades Impositivas Tributarias (6 a 10 UIT).

## "Capítulo IV

## Infracciones

**Artículo 132.- Infracciones**

Las infracciones a la Ley Nº 29733, Ley de Protección de Datos Personales, o su Reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada Ley.

**1. Son infracciones leves**

a) Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia.

b) Recopilar datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos.

c) No modificar o rectificar los datos personales objeto de tratamiento cuando se tenga conocimiento de su carácter inexacto o incompleto.

d) 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 media procedimiento de anonimización o disociación.

e) No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley.

f) Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento.

**2. Son infracciones graves:**

a) No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de

acuerdo a lo establecido en el Título III de la Ley Nº 29733 y su Reglamento.

b) 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 Nº 29733 y su Reglamento.

c) Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia.

d) Recopilar 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.

e) Utilizar los datos personales obtenidos lícitamente para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación.

f) Obstruir el ejercicio de la función fiscalizadora de la Autoridad.

g) Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley Nº 29733.

h) No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley Nº 29733, a pesar de haber sido requerido para ello por la Autoridad en el marco de un procedimiento sancionador.

**3. Son infracciones muy graves:**

a) Dar tratamiento a los datos personales contraviniendo las obligaciones contenidas en la Ley Nº 29733 y su Reglamento, cuando con ello se impida o se atente contra el ejercicio de otros derechos fundamentales.

b) Recopilar datos personales mediante medios fraudulentos, desleales o ilícitos.

c) Suministrar documentos o información falsa a la Autoridad.

d) No cesar en el indebido tratamiento de datos personales cuando existiese un previo requerimiento de la Autoridad como resultado de un procedimiento sancionador o de un procedimiento trilateral de tutela.

e) No cumplir con las medidas correctivas establecidas por la Autoridad como resultado de un procedimiento trilateral de tutela.

**Artículo 133.- Graduación en caso de reincidencia**

En caso de reincidencia en la comisión de dos (02) infracciones leves, en un mismo año, la tercera infracción leve se sanciona como una infracción grave.

En caso de reincidencia en la comisión de dos (02) infracciones graves, en un mismo año, la tercera infracción grave se sanciona como una infracción muy grave." ***(*) Capítulo IV incorporado por la Tercera Disposición Complementaria Modificatoria del Reglamento del Decreto Legislativo Nº 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, aprobado por Decreto Supremo N° 019-2017-JUS, publicado el 15 de setiembre de 2017.***

## Disposiciones Complementarias Finales

**Primera.- Interoperabilidad entre entidades públicas.**

La definición, los alcances y el contenido de la interoperabilidad, a que hace referencia el primer párrafo del artículo 11 del presente reglamento, así como los lineamientos para su aplicación y funcionamiento en concordancia con las normas de protección de datos personales, son competencia de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros, en su calidad de Ente Rector del Sistema Nacional de Informática. La interoperabilidad entre entidades se regulará en cuanto a su implementación en el marco de lo dispuesto por el numeral 76.2.2 del inciso 76.2 del artículo 76 de la Ley Nº 27444, Ley del Procedimiento Administrativo General.

**Segunda.- Protección de datos personales y competitividad.**

Las competencias establecidas en el presente reglamento son ejercidas por la Autoridad Nacional de Protección de Datos Personales, en concordancia con las políticas de competitividad del país establecidas por el ente correspondiente.

**Tercera.- Protección de datos personales y programas sociales.**

Conforme a lo previsto en el numeral 12 del artículo 33 de la Ley, los términos en que debe concordarse el cumplimiento de la Ley y el presente Reglamento con las normas o políticas de transparencia y fiscalización que rigen la administración de los bancos de datos vinculados con los Programas Sociales y el Sistema de Focalización de Hogares serán desarrollados mediante directiva y en coordinación con el Ministerio de Desarrollo e Inclusión Social - MIDIS.

## Disposiciones Complementarias Transitorias

**Primera.- Adecuación de bancos de datos personales.**

En el plazo de dos (2) años de la entrada en vigencia del presente reglamento, los bancos de datos personales existentes, deben adecuarse a lo establecido por la Ley y el presente reglamento, sin perjuicio de la inscripción a que se refiere la Quinta Disposición Complementaria Final de la Ley Nº 29733, Ley de Protección de Datos Personales.

**Segunda.- Facultad sancionadora.**

La facultad sancionadora de la Dirección General de Protección de Datos Personales, en relación a los bancos de datos personales existentes a la fecha de la entrada en vigencia del presente reglamento, queda suspendida hasta el vencimiento del plazo de adecuación establecido en la Primera Disposición Complementaria Transitoria.

**Tercera.- Formatos.**

La Dirección General de Protección de Datos Personales creará los formatos tipo necesarios para la tramitación de los procedimientos regulados en el presente reglamento en un plazo que no excederá de sesenta (60) días de la entrada en vigencia del presente reglamento.