INSTRUCTIVO

Para oficiales de datos personales

PERÚ Ministerio de Justicia y Derechos Humanos

Con Punche Perú

BICENTENARIO DEL PERÚ 2021 - 2024

Instructivo para oficiales de datos personales

Autoridad Nacional de Protección de Datos Personales
Mayo 2023

Calle Scipión Llona 350, Miraflores, Lima - Perú
Teléfono (511) 204 8020 anexo 2410
www.gob.pe/minjus
www.gob.pe/anpd
protegetusdatos@minjus.gob.pe

Ministro de Justicia y Derechos Humanos
Daniel Ysau Maurate Romero

Viceministro de Justicia
Walther Javier Iberos Guevara

Director General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
Eduardo Javier Luna Cervantes

Directora de Protección de Datos Personales
María Alejandra González Luna

Directora de Fiscalización e Instruccion
Olga Escudero Vílchez

Elaboración:
Este documento ha sido elaborado por el equipo de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Diseño y diagramación
Carlos Alfonso Gonzales Chingay

Presentación

Mediante la publicación del Reglamento del Decreto Legislativo Nro. 1412, Ley de Gobierno Digital, aprobado por Decreto Supremo Nro. 029-2021-PCM, se estableció la designación de un Oficial de Datos Personales a efectos de garantizar la protección de los datos personales de los ciudadanos y ciudadanas al interior de las diversas entidades de la Administración Pública.

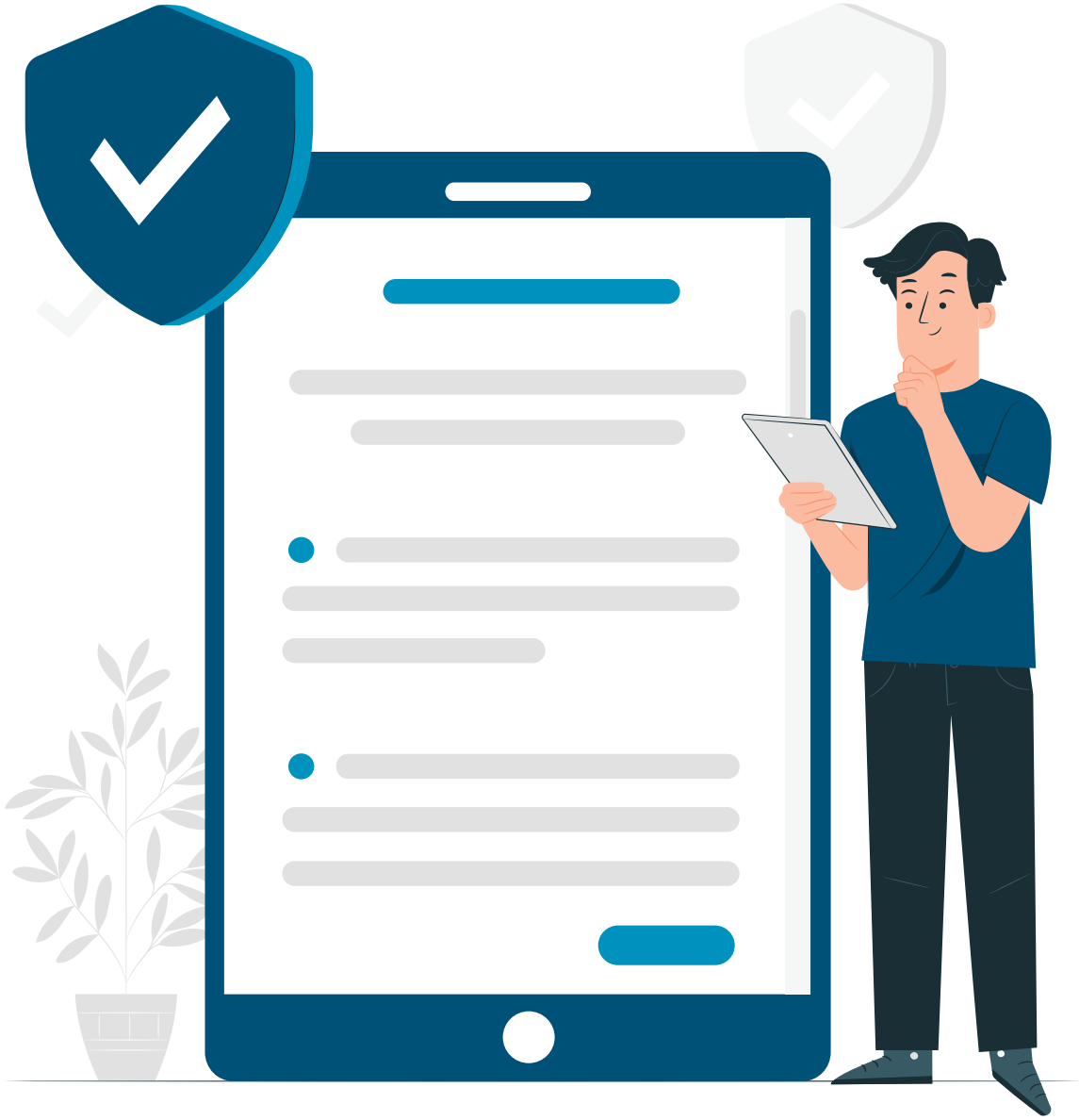
El presente documento busca informar, de manera práctica y sencilla, los alcances del rol que debe cumplir el Oficial de Datos Personales dentro de sus respectivas entidades públicas, así como brindar pautas y recomendaciones para el cumplimiento de los principios, obligaciones y derechos contemplados en la Ley N.° 29733, Ley de Protección de Datos Personales y su Reglamento, aprobado por Decreto Supremo Nro. 003-2013-JUS.

I. Siglas

ANPD	Autoridad Nacional De Protección De Datos Personales
ARCO	Acceso, Rectificación, Cancelación Y Oposición
BDP	Banco de Datos Personales
DFI	Dirección de Fiscalización e Instrucción
DP	Datos Personales
DPDP	Dirección de Protección de Datos Personales
DGTAIPD	Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
LPDP	Ley de Protección de Datos Personales
LTAIP	Ley de Transparencia y Acceso a la Información Pública
MINJUSDH	Ministerio de Justicia y Derechos Humanos
MPV	Mesa de Partes Virtual
RLPDP	Reglamento de la Ley de Protección de Datos Personales
RNPDP	Registro Nacional de Protección de Datos Personales
OC	Opinión Consultiva
ODP	Oficial de Datos Personales
PAS	Procedimiento administrativo sancionador
PIDE	Plataforma de Interoperabilidad del Estado
TBD	Titular del Banco de Datos Personales

II. Base Legal

- Constitución Política del Perú (inciso 6 del artículo 2)
- Ley Nro. 29733, Ley de Protección de Datos Personales y su Reglamento aprobado por Decreto Supremo Nro. 003-2013-JUS.
- Decreto Legislativo Nro. 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y su Reglamento aprobado por Decreto Supremo Nro. 029-2021-PCM.
- Decreto Legislativo Nro. 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 y su Reglamento aprobado por Decreto Supremo Nro. 019-2017-JUS.
- Decreto Supremo Nro. 013-2017-JUS, que aprueba el Reglamento de Organización y Funciones del MINJUSDH (artículos 70 al 71).

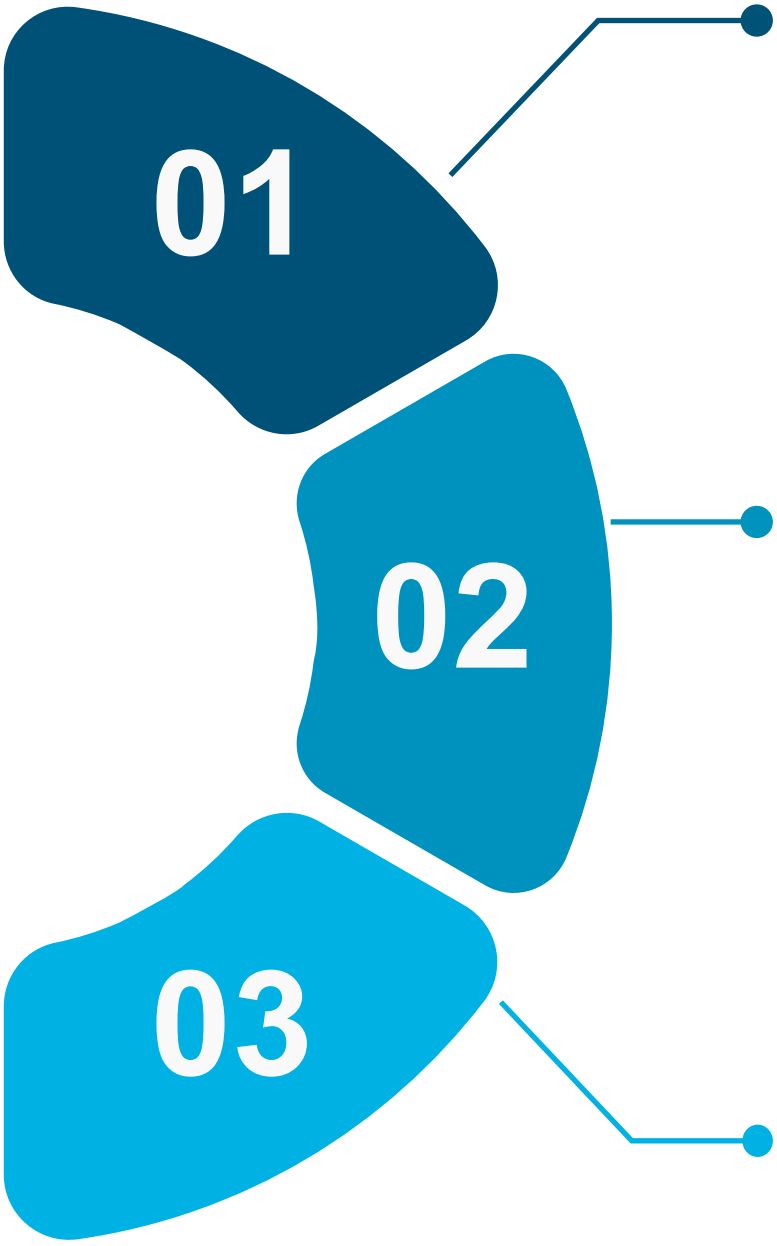


III. ¿Quién es el Oficial de Datos Personales - ODP?

El ODP es el funcionario o servidor público, responsable dentro de la entidad pública, de velar por el cumplimiento y/o atención de las normas en materia de protección de datos personales.

El ODP actúa como enlace entre la entidad pública y la Autoridad Nacional de Protección de Datos Personales.

Elección, perfil y funciones del ODP en las entidades públicas



Elección

Depende de la máxima autoridad administrativa de cada entidad.

No implica la creación de un nuevo puesto de trabajo.

Perfil

Puede recaer en el titular de la Oficina de Asesoría Jurídica o titular de la Oficina de Tecnologías de la Información o quien haga sus veces.

Conocimiento de derecho (de preferencia en materia de datos personales) y tecnologías de la información.

Funciones

Velar por el cumplimiento de las normas en materia de protección de datos personales en su entidad.

Actúa como enlace con la ANPD, para la coordinación de alguna acción necesaria en su entidad vinculada a la temática de protección de datos personales.

Coopera y sigue los lineamientos y directivas que emita la Autoridad en los ámbitos de su competencia.

Consideraciones sobre la Ley de Protección de Datos Personales y su Reglamento

IV. ¿Cuál es el ámbito de aplicación de la LPDP y su Reglamento?

Ámbito de aplicación

- DP contenidos o destinados a ser contenidos en BDP de administración pública dentro del territorio nacional.
- DP contenidos o destinados a ser contenidos en BDP de administración privada dentro de territorio nacional.

LPDP (art. 3)

Excepciones al ámbito de aplicación

Las disposiciones de la LPDP y su Reglamento no resultan aplicables cuando se trata de:

Datos personales contenidos o destinados a ser contenidos en BDP creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar. Ejemplo: Directorio familiar, álbumes de fotos, etc.

Los datos personales contenidos o destinados a ser contenidos en BDP de la administración pública, solo en tanto su tratamiento resulte necesario para el cumplimiento de competencias asignadas por ley a las entidades públicas en relación a:

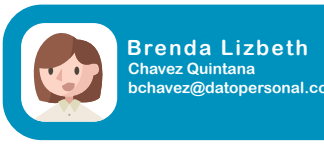
1. Defensa nacional.
2. Seguridad Pública.
3. Desarrollo de actividades en materia penal (investigación y represión del delito)

Ejemplo: Los BDP vinculados a la investigación y represión del delito de robo del Ministerio Público o la Policía Nacional del Perú.

Debes tener en cuenta que:
Aunque existan normas especiales que regulen temas relacionados a los DP dentro de las entidades públicas, ello no excluye el cumplimiento de la LPDP y su Reglamento.

V. ¿Qué es un DATO Personal?

Es toda información (numérica, alfabética, gráfica, fotográfica, acústica) que te identifica o te hace identificable



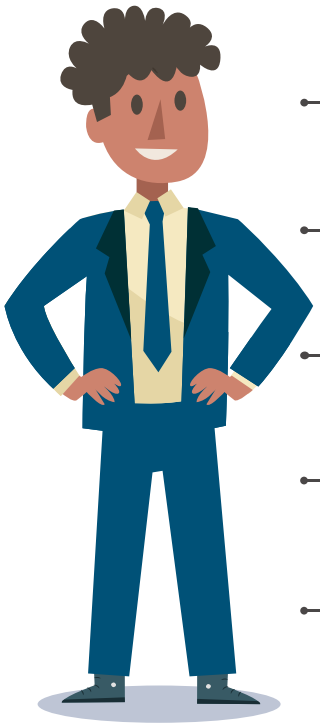
Brenda Lizbeth
Chavez Quintana
bchavez@datopersonal.com

- Sexo, Edad
- Estado Civil
- Nº de teléfono
- Dirección
- Gustos

¿Qué es un DATO Sensible?

Es toda información que derive en un dato biométrico que identifica al titular, así como datos referidos a origen racial, étnico, religioso, ingresos económicos, convicciones políticas, salud, vida sexual, afiliación sindical, entre otros.

José Carlos
Torres Gonzales
jtorres@datopersonal.com



- Ingresos Económicos
- Datos biométricos
- Datos de Salud
- Orientación sexual
- Afiliación política
- Creencia religiosa

Debes tener en cuenta que:
Personas inescrupulosas pueden suplantar o robar tu identidad. Verifica con quién compartes tus datos personales para evitar ser víctima de delitos.

VI. ¿Cuáles son los principios rectores que regulan el tratamiento de datos personales?

Los principios rectores en la normativa de datos personales sirven de pauta para guiar la conducta de quienes ejercen los derechos de protección de DP y de quienes deben cumplir las obligaciones que deriven de la LPDP y su Reglamento. Estos principios son los siguientes:

1. **Principio de consentimiento (artículo 5 de la LPDP)**

   El tratamiento de datos personales se considera lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco:

1 Libre

El consentimiento se debe obtener sin que exista error, mala fe, violencia o dolo. No se debe viciar la voluntad del titular de los datos personales.

2 Previo

El consentimiento debe pedirse antes de la recopilación de los datos personales o antes de que sean tratados de una forma distinta a la establecida en principio.

3 Expreso e inequívoco

La manifestación del consentimiento no debe dar lugar a dudas sobre su otorgamiento. Puede ser otorgada de forma verbal (presencialmente o vía tecnología); escrita (firma autógrafa, huella dactilar, otros medios permitidos) y/o alguna otra forma permitida.

4 Informado

Al titular de los datos personales se le debe comunicar en lenguaje sencillo y de forma clara, expresa e indubitablemente la información necesaria para el consentimiento.

2. Principio de finalidad y proporcionalidad (artículos 6 y 7 de la LPDP)

El principio de finalidad implica que los datos personales deben ser recopilados para una finalidad determinada (clara y sin lugar a confusión), explícita y lícita. En el caso de BDP 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 TBD.

Por su parte, el principio de proporcionalidad exige que todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

3. Principio de calidad (artículo 8 de la LPDP)

Los datos contenidos en un BDP deben ajustarse con precisión a la realidad. 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 recopiladas garantizando su seguridad. Este principio implica la necesidad de revisar y comprobar antes y después de la recopilación, la vigencia y exactitud de los datos personales.

4. Principio de seguridad (artículo 9 de la LPDP)

En el tratamiento de los datos personales deben adoptarse las medidas de seguridad necesarias a fin de evitar cualquier acto contrario a la Ley y al reglamento, incluyendo la adulteración, pérdida, desviaciones de información (intencionales o no) independientemente de la fuente de los riesgos (acción humana o medio técnico utilizado).

5 Principio de disposición de recurso (artículo 10 de la LPDP)

Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para efectuar reclamos y/o hacer valer sus derechos, cuando considere que existe una vulneración en el tratamiento de sus datos personales. Por ejemplo, las solicitudes de tutela de derechos ante la propia ANPD.

6. Principio de nivel de protección adecuado (artículo 11 de la LPDP)

En el caso del flujo transfronterizo de datos personales (transferencia internacional), resulta necesario que se garantice de forma adecuada y suficiente la protección de los datos personales que se vayan a tratar.

VII. ¿En qué casos no se requiere el consentimiento del titular de datos personales?

En lo que respecta a entidades públicas, no se requiere el consentimiento del titular de datos personales, 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. Ejemplo: La ONP recopila datos de sus aportantes para cumplir con el pago de una pensión de jubilación, conforme a ley.

2. Los datos personales se encuentran contenidos en fuentes accesibles al público. Ejemplo: El portal de transparencia estándar de una entidad pública contiene datos (nombre y DNI) de las personas que mantienen reuniones de trabajo con diversos funcionarios.

3. Los datos personales necesarios para la preparación, celebración y ejecución, celebración de un contrato en el que el titular de los datos es parte o cuando derive de una relación científica o profesional del titular. Ejemplo: Los datos incluidos en los contratos celebrados entre los trabajadores y empleadores del Estado.

4. Tratamiento de datos personales relativos a la salud, en circunstancias de emergencia, para prevenir, diagnosticar y tratar médico y quirúrgicamente al titular, en centros de salud y por profesionales de la salud, observando el secreto profesional o por razones de interés público con autorización del MINSA. Ejemplo: Las Oficinas de Recursos Humanos de las entidades públicas recolectaban datos de salud de sus trabajadores para conocer sus riesgos y comorbilidades a raíz de la emergencia sanitaria y pandemia ocurrida por el virus Covid – 19.

5. Tratamiento de datos de los miembros de entidades sin fines de lucro, cuya finalidad sea política, religiosa o sindical, siempre que se circunscriba a sus actividades y que no sean transferidos sin consentimiento. Ejemplo: La recopilación de datos de trabajadores adscritos a un sindicato que permita sus actividades propias.

6. Cuando se hubiera aplicado un procedimiento de anonimización o disociación. Ejemplo: La ANPD publica los informes y consultas que emite en el ejercicio de sus funciones, para lo cual disocia los datos de las personas que intervinieron en el procedimiento.

7. Cuando el tratamiento de datos sea para fines relacionados al sistema de prevención de lavado de activos y terrorismo, o por mandato legal. Ejemplo: El tratamiento de datos que realiza la Unidad de Inteligencia Financiera con el Ministerio Público para la detección de lavado de activos y/o financiamiento de terrorismo.

VIII. ¿Qué implica el cumplimiento del derecho de información en el tratamiento de datos personales?

Los aspectos más relevantes para cumplir con el deber de información son los siguientes:

Identidad y domicilio

Proporcionar la identificación completa del titular del banco de datos personales como: Documento Nacional de Identidad (DNI) si es una persona natural, o bien, la razón o denominación social y registro único del contribuyente (RUC), si se trata de una persona jurídica.

El domicilio se debe indicar a fin de que el titular de datos personales, si lo considera, pueda apersonarse a las instalaciones del responsable del tratamiento (debe comprender: número o lote, calle, jirón, avenida, distrito, provincia y departamento, entre otros).

Ejemplo: El Ministerio Público informa que tiene domicilio sito en la Av. Abancay, cuadra 5 S/N – Piso 1, distrito del Cercado de Lima, provincia y departamento de Lima. La información sobre los bancos de datos personales de titularidad del Ministerio Público se encuentra en su página web: https://portal.mpfn.gob.pe/convoca/politica-privacidad

Finalidad

Responde a la pregunta ¿para qué serán tratados los datos personales recabados?, es decir, cuál o cuáles serán los usos específicos que se les darán a los datos personales obtenidos. Se recomienda evitar términos o frases genéricas o inexactas, como, por ejemplo: “entre otras finalidades”, “otras modalidades análogas”, “etcétera”, que no expresen claramente las finalidades del tratamiento de los datos personales.

Ejemplo: El Registro de Banco de Datos denominado: “Registro de los nacidos vivos a nivel nacional” del Ministerio de Salud, tiene como finalidad identificar a los neonatos con su certificado de nacido vivo para la obtención del DNI y contar con una estadística para tomar en cuenta en los programas sociales del gobierno (https://www.gob.pe/9254-consultar-el-registro-nacional-de-proteccion-de-datos-personales).

El carácter obligatorio o facultativo de los datos personales otorgados

El responsable del tratamiento de los datos personales debe indicar si los datos personales que solicita son obligatorios de entregar o, por el contrario, sólo es facultativo. Asimismo, la explicación del carácter obligatorio o facultativo es ineludible cuando se trate de datos personales sensibles.

Ejemplo: Si un ciudadano solicita algún servicio de salud ante el Seguro Social de Salud (EsSalud), los datos obligatorios a solicitarle, entre otros, es su DNI a efectos de corroborar que su seguro se encuentra activo.

Consecuencia de proporcionar sus datos personales y de su negativa a hacerlo

En caso corresponda, si la recopilación de los datos personales es necesaria para el cumplimiento de las funciones públicas o de otras finalidades que inciden, o son de interés, del titular de los datos, debe informarse a su titular acerca de la obligatoriedad o no de otorgar los datos personales, así como las consecuencias de no hacerlo.

Ejemplo: El Ministerio de Educación en atribución a sus funciones, solicitó a diversas Unidades de Gestión Educativas datos personales de los padres de familia de los estudiantes, a efectos de contar con información oportuna y confiable sobre la trayectoria educativa de los mismos, sin embargo, deberá informarse si dicha información se transfiere a terceros para un uso diferente al previamente señalado.

Transferencia y destinatarios

Si realiza transmisión o suministro nacional e internacional de datos personales, es decir, si los datos personales son enviados a una persona natural o jurídica distinta del titular de los datos, dentro o fuera del Perú, se debe indicar la identidad de los destinatarios, hacia dónde y con qué finalidades se están transfiriendo los datos personales.

Ejemplo: El Ministerio de Comercio Exterior y Turismo señala que en relación al BDP denominado “Artesanos” no se realiza transferencia de datos personales a nivel internacional (flujo transfronterizo) siendo su finalidad recopilar los DP de los artesanos para promover el desarrollo de la actividad artesanal en diversas modalidades.

Banco de datos personales

Se debe indicar de manera clara y específica la denominación del banco de datos personales que almacena la información proporcionada por el titular de los datos personales.

Ejemplo: Cuando una entidad pública inscribe el banco de datos de los “trabajadores” de dicha entidad.

Tiempo de conservación de los DP

El responsable del tratamiento debe indicar el plazo durante el cual se conservarán los datos personales o los criterios utilizados para determinar ese plazo (por ejemplo, hasta que se realice determinada finalidad).

Ejemplo: Cuando una entidad pública señala que conservará los datos personales de un trabajador hasta que concluya la relación contractual entre ambas partes.

Ejercicio de los derechos ARCO

Es obligatorio informar sobre el ejercicio de los derechos de Acceso, Rectificación (actualización, inclusión), Cancelación (supresión) y Oposición; así como brindar información acerca de los canales de atención para el ejercicio de tales derechos y el procedimiento a seguir para atender las solicitudes de los titulares de los datos personales.

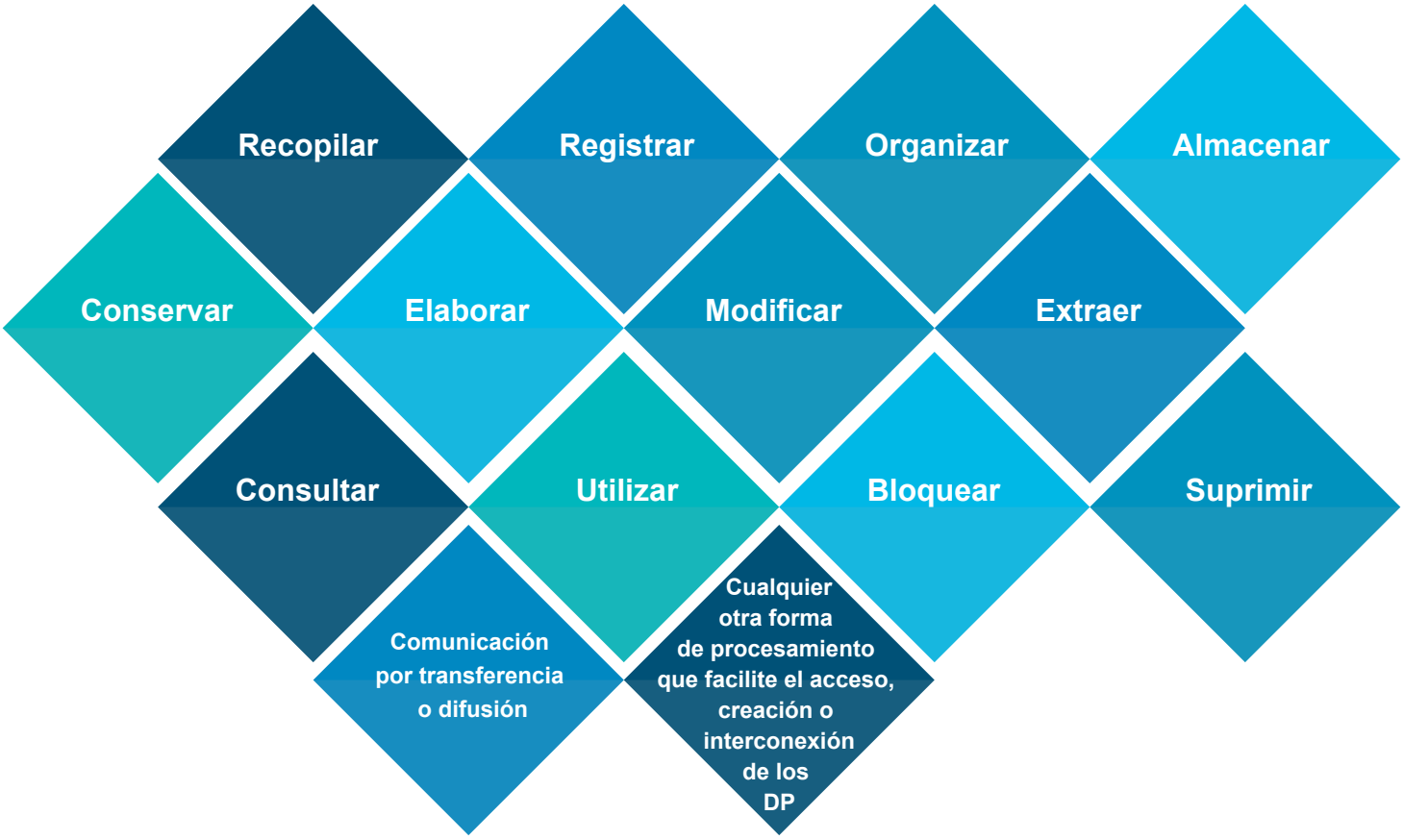
Ejemplo: El Ministerio Público señala en relación al BDP de "visitas" se podrá ejercer los derechos ARCO en la mesa de partes de la Presidencia de la Junta de Fiscales Superiores del distrito fiscal de Lima (Jirón Miroquesada N.° 220, primer piso, distrito de Cercado de Lima, provincia y departamento de Lima).

Dato importante:

La carga de la prueba sobre el cumplimiento de la obligación de solicitar el consentimiento recae en el TBD o el responsable del tratamiento de los datos personales.

Es recomendable que las entidades adopten las medidas necesarias y adecuadas para el cumplimiento de los aspectos que abarca esta obligación a fin de evitar posibles sanciones.

IX. ¿En qué consiste el tratamiento de datos personales?



X. ¿Quiénes son los actores del tratamiento de DP?

Titular de datos personales

Persona natural a quien corresponde los datos personales.

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.

Responsable de tratamiento de datos personales

Persona natural o jurídica que decide sobre el tratamiento de datos personales, aun cuando no se encuentre en un BDP.

Encargado del 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 BDP. Por ejemplo, las empresas que brindan el servicio de asesoría jurídica, cobranza, hosting, entre otras, a diversas entidades públicas.

XI. ¿Cómo es el tratamiento de datos personales de menores de edad?

Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones:

1. Para el tratamiento de datos personales de menores de edad es necesario la obtención del consentimiento de los titulares de la patria potestad o tutores.
2. Excepcionalmente, en el caso de las entidades públicas, pueden tratar los datos personales de mayores de 14 años y menores de 18 con el consentimiento de estos siempre que la información se proporcione en un lenguaje comprensible, salvo que la ley exija la asistencia de los titulares de patria potestad (art. 28 del RLPDP).

Es importante saber que:
• No pueden entregar obsequios ni otorgar beneficios a los menores de edad con el fin de obtener su consentimiento.
•Constituye una prohibición expresa recopilar datos del grupo familiar de un menor de edad, excepto los datos de identidad y dirección de los padres o tutores a fin de obtener su consentimiento en el caso que se requiera realizar tratamiento de datos de menores de edad, entre otros supuestos habilitados legalmente.

XII. ¿En qué consiste el tratamiento de datos personales mediante los sistemas de video vigilancia?

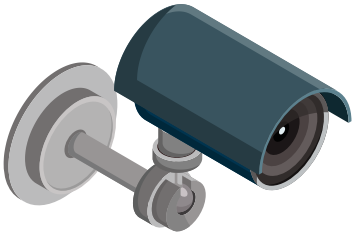
1. La imagen y la voz de una persona son considerados datos personales y, por ende, se encuentran bajo el ámbito de protección de la LPDP y su reglamento.

2. En caso las entidades públicas capten, graben, transmitan, conserven o almacenen imágenes y voces de personas mediante sistemas de video vigilancia, se encuentran sujeta al cumplimiento de las disposiciones establecidas en la LPDP y su Reglamento, así como cualquier otra normativa que regule tal actividad.

3. Para orientar y facilitar lo señalado, la ANPD ha elaborado la "Directiva sobre el tratamiento de datos personales mediante sistemas de videovigilancia", la cual se encuentra disponible en el siguiente enlace: https://bit.ly/3oGF7iB

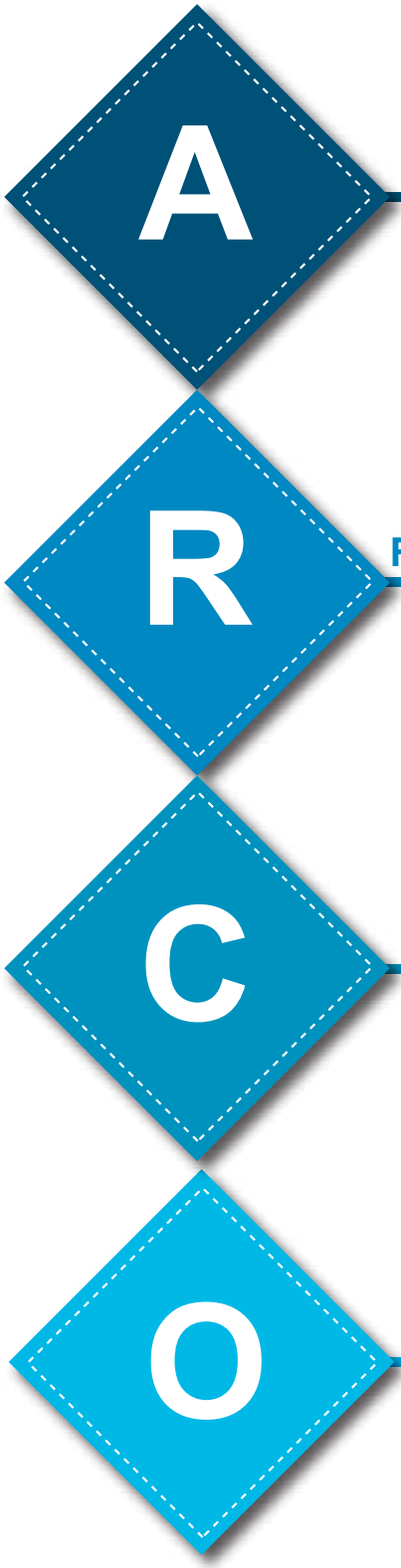
4. Como principales obligaciones se pueden señalar las siguientes:

- Se debe solicitar la inscripción del banco de datos personales ante la DGTAIPD.
- El acceso a la zona videovigilada debe tener un cartel o anuncio suficientemente visible con fondo amarillo u otro que contraste con el color de la pared, que debe indicar, entre otros, la identidad y domicilio del titular del banco de datos personales, cómo se pueden ejercitar los derechos ARCO, etc.
- El plazo de conservación o almacenamiento de la información grabada es de 30 a 60 días como máximo y debe eliminarse en el plazo máximo de 2 días hábiles.
- Se debe respetar los principios de proporcionalidad, seguridad y calidad.
- Se debe cumplir con las medidas de seguridad, para lo cual se pueden contar con procedimientos de identificación y autentificación de usuarios que den cuenta del control y monitoreo del sistema de videovigilancia, entre otros, según el RLPDP.



XIII. ¿Qué derechos tienen los titulares de datos personales?

Los titulares de datos personales tienen derecho a obtener, modificar y/o suprimir sus datos personales, así como a oponerse a su tratamiento por parte de entidades públicas o privadas. Estos derechos se denominan derechos ARCO:



Es el derecho a saber qué datos tiene una entidad sobre una persona natural, y preguntar cómo los obtuvieron, para qué los utilizaron, con quién los han compartido y todos los detalles de su uso.

Es el derecho a modificar y actualizar datos personales de una persona natural cuando estos sean erróneos, falsos, inexactos o incompletos.

Es el derecho a cancelar los datos entregados por una persona natural porque la finalidad ha concluido, venció el plazo establecido para su tratamiento, o se revocó el consentimiento para su uso.

Es el derecho a oponerse al uso de datos cuando existan motivos fundados y legítimos referidos a una situación personal concreta. Se ejerce sobre todo en ámbitos digitales.

XIV. ¿Cuáles son las obligaciones que tiene el titular del banco de datos y/o responsable del tratamiento?

1. Inscribir sus BDP ante el RNPD.

- En las entidades públicas, los bancos de datos se establecen en función de lo que dispone el Reglamento de Organización y Funciones (en adelante ROF) de cada entidad, es decir de acuerdo con las funciones o competencias asignadas a determinada entidad.

- Ello significa que la determinación de los bancos de datos bajo la administración de cada entidad dependerá de las funciones y competencias que le han sido asignadas mediante sus respectivas normas. Por ejemplo, las Oficinas de Recursos Humanos de las entidades públicas administran bancos de datos personales de los funcionarios y servidores de la entidad.

2. Comunicar ante la ANPD la realización de flujo transfronterizo de datos personales.

- El flujo transfronterizo es la transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, independientemente del soporte en que se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciben.

  Ejemplo: El servicio de hosting que podrían utilizar alguna entidad púbica, en atención a sus competencias, para el tratamiento de DP en un lugar fuera del territorio nacional.

3. Atender los pedidos de tutela de los ciudadanos.

- El TBD o responsable del tratamiento se encuentra obligado a brindar respuesta a las solicitudes realizadas por el titular de datos personales en ejercicio de sus derechos regulados en la LPDP y su Reglamento. De no haber respuesta oportuna y/o en caso de que esta no sea satisfactoria, el solicitante tendrá por denegada su solicitud y, con base en ello, podrá iniciar un procedimiento trilateral de tutela[1] ante la DPDP.

4. Efectuar el tratamiento de datos personales de acuerdo con los principios rectores.

5. Implementar las medidas de seguridad necesarias a fin de garantizar la protección adecuada de los datos personales que administra.

- Al respecto, la ANPD ha elaborado la "Directiva de seguridad de la información administrada por los bancos de datos personales" como un documento facilitador que contiene recomendaciones a ser implementadas en lo referente a la adopción de las medidas de seguridad. Dicho documento está disponible en el siguiente enlace: https://bit.ly/3AJ067b

  En caso se realice tratamiento de datos mediante soporte automatizado, como medios informáticos, se deberá tomar medidas como, por ejemplo, controlar la asignación y el uso de contraseñas de los usuarios de los sistemas de información, solicitándoles que mantengan el secreto de dichas contraseñas. Asimismo, dichas contraseñas deberán ser cambiadas cuando sea necesario y deberán contener al menos 8 dígitos alfanuméricos.

  Por otro lado, se deberá revisar periódicamente que los privilegios de acceso a los datos personales correspondan al personal autorizado, lo cual debe realizarse por lo menos semestralmente. Dicho control debe estar establecido claramente mediante un procedimiento documentado.

  En caso se realice tratamiento de datos mediante soporte no automatizado, (soporte físico), se deberá tomar en cuenta medidas como, por ejemplo, asegurar que los datos personales contenidos en fólderes o carpetas sean solo de acceso al personal autorizado y para ello se puede utilizar armarios o algún otro espacio con candado y llave.

  Asimismo, se debe asegurar que la generación o reproducción y eliminación de copias de documentos sean realizados por personal autorizado, para lo cual se puede implementar la configuración de contraseñas en las máquinas impresoras, supervisar el proceso de impresión verificando que se retire todos los documentos originales y copias del equipo inmediatamente después de finalizada la copia o reproducción.

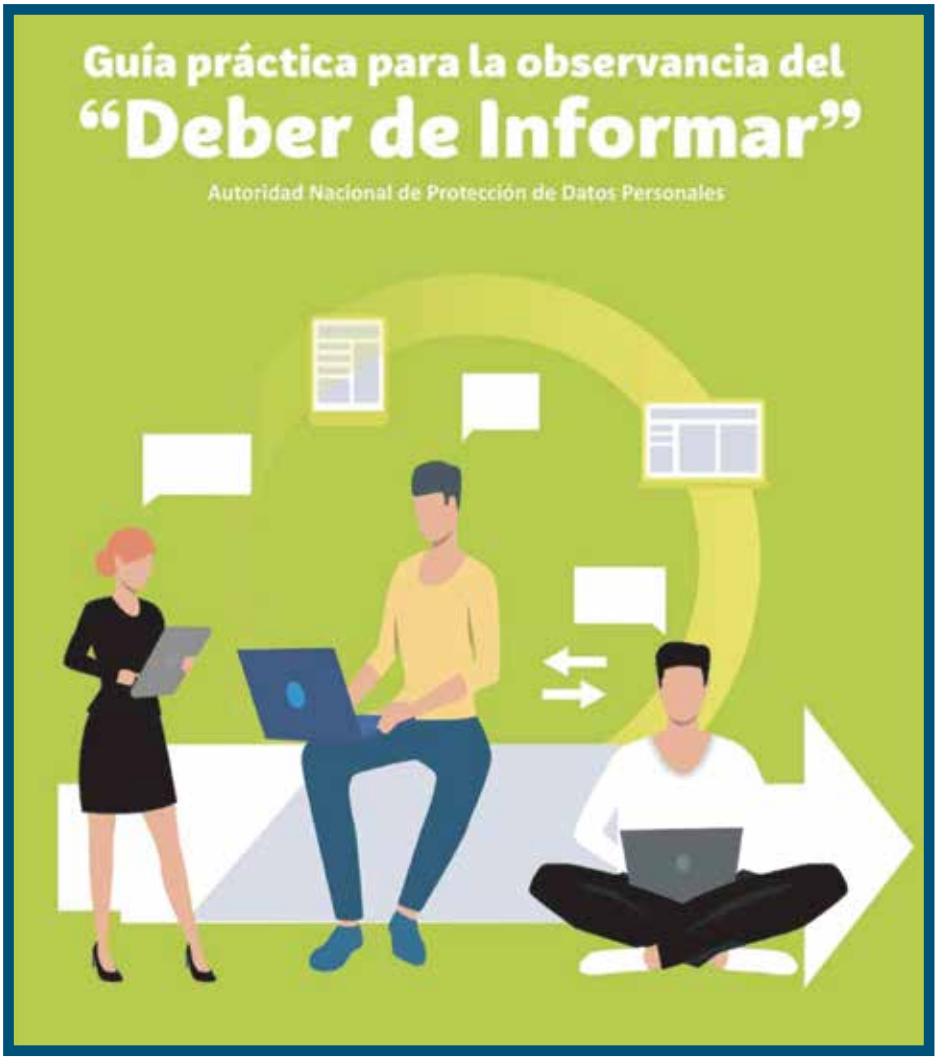
1. Véase pregunta xv

6. Cumplir con el deber de confidencialidad

- La confidencialidad es el deber/obligación correspondiente a quienes realizan tratamiento de datos (el TBD, el responsable del tratamiento u otros que intervengan) a fin de que mantengan en reserva y no se divulgue todos aquellos datos personales y sus antecedentes que se encuentran bajo su administración.

7. Cumplir con el derecho-deber de informar

- El artículo 18 de la LPDP establece que el titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación.



Ten en cuenta que:

La ANPD ha elaborado una "Guía práctica para la observancia del deber de informar" cuyo propósito es orientar de forma práctica y sencilla sobre cómo dar cumplimiento al derecho-deber de informar establecido en el artículo 18 de la LPDP. Esta guía se encuentra disponible en el siguiente enlace: https://bit.ly/3L3E4ka

XV. ¿Qué es el RNPD? ¿Cuál es el procedimiento de inscripción de los BDP?

El RNPD contiene principalmente la información sobre BDP, ya sea que provengan de entidades públicas o privadas. La finalidad es la publicidad de la inscripción de los bancos de datos a fin de facilitar el ejercicio de los derechos ARCO y demás derechos establecidos en la LPDP y su Reglamento.

Debes saber que:

El BDP es el 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. Por ejemplo, BDP de asegurados del Seguro Social de Salud (ESSALUD), entre otros.

El trámite de inscripción se realiza a través del siguiente enlace:

https://www.gob.pe/8060-inscribir-banco-de-datos-en-el-registro-nacional-de-proteccion-de-datos-personales

8.1 Son objeto de registro:

1 BDP de la administración pública

2 BDP de la administración privada

3 Códigos de conducta[2] (opcional)

4 Comunicaciones referidas al flujo transfronterizo, de ser el caso

5 Las sanciones, medidas cautelares o correctivas impuestas por la ANPD.

- Asimismo, en caso de que se cree un nuevo banco de datos o se modifique o cancele uno ya existente, esta situación también debe ser objeto de inscripción ante el RNPD.

2. Los códigos de conducta son un mecanismo de responsabilidad proactiva que permite demostrar el cumplimiento de las obligaciones establecidas en la Ley y el presente Reglamento para el tratamiento de datos personales. Los Códigos de conducta tienen carácter voluntario.

8.2 ¿Cómo desarrollamos el procedimiento de inscripción de un BDP?

El RNPD contiene principalmente la información sobre BDP, ya sea que provengan de entidades públicas o privadas. La finalidad es la publicidad de la inscripción de los bancos de datos a fin de facilitar el ejercicio de los derechos ARCO y demás derechos establecidos en la LPDP y su Reglamento.

PRESENTACIÓN DE LA SOLICITUD

Para la creación, modificación o cancelación de un banco de datos se debe pagar una tasa administrativa: i) S/. 75.80 para derecho de inscripción de BDP; ii) S/. 61.60 para derecho de modificación de BDP y iii) S/.69.80 para derecho de cancelación de BDP (según TUPA del MINJUSDH aprobado por D.S N.° 019-2021-JUS).

RESOLUCIÓN DE INSCRIPCIÓN(*)

(En caso de que no se emita la resolución dentro del plazo, se entenderá que el banco de datos ha quedado inscrito, modificado o cancelado, según corresponda).

A cargo de la DPDP
Se emite dentro del plazo de 30 días hábiles luego de presentada la solicitud.

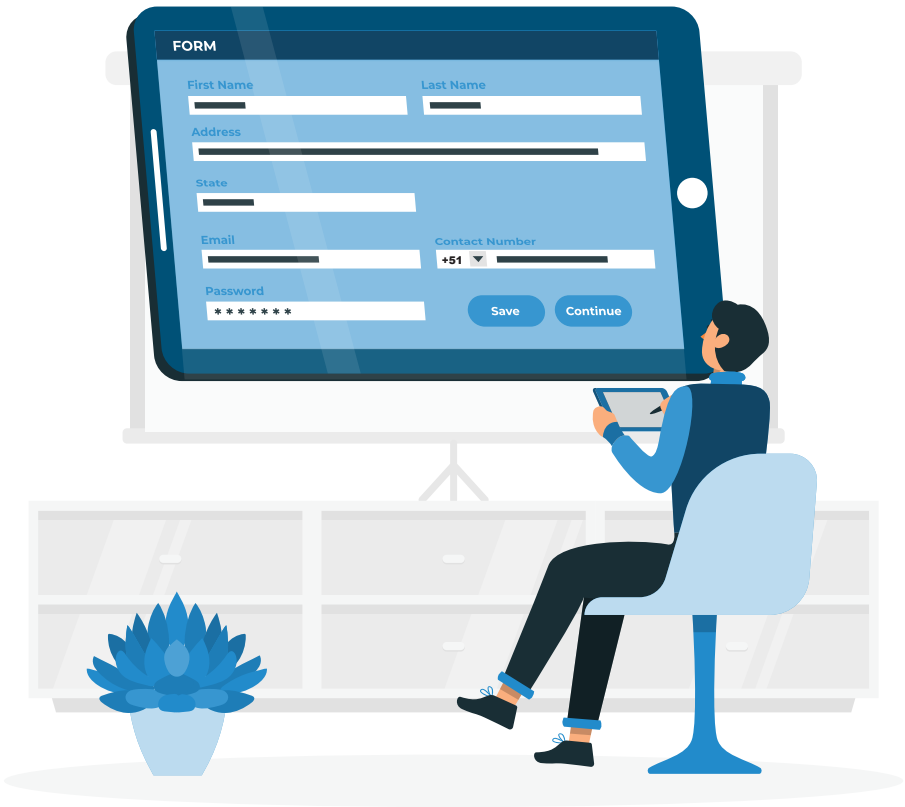
RECURSO DE RECONSIDERACIÓN

(En caso de que se deniegue la solicitud de inscripción o esta sea improcedente).

Es opcional y se encuentra a cargo de la DPDP

A cargo de la DGTAIPD

RECURSO DE APELACIÓN



XVI. ¿Qué es el procedimiento trilateral de tutela?

En el marco del ejercicio de los derechos ARCO de los titulares de datos, estos pueden formular su solicitud ante el titular del banco de datos o el encargado de su tratamiento.

En el supuesto de que su solicitud para el ejercicio de los derechos ARCO sea denegada, la respuesta no sea satisfactoria para sus intereses y/o esta no sea atendida dentro de los plazos legales, el titular de los datos podrá acudir ante la ANPD y formular una “solicitud de tutela de derechos”. El formato de la solicitud se encuentra disponible en https://bit.ly/3RmSBJz

El procedimiento trilateral de tutela se desarrolla de la siguiente manera:

Solicitud de ejercicio de derechos ARCO

- Se formula ante el TBD o responsable del tratamiento. El plazo de respuesta es de 8 días en el caso del derecho de información, 20 en caso del derecho de acceso y 10 en el caso de rectificación, cancelación u oposición.

Solicitud de tutela de derechos

- Se formula ante la DPDP.
- Plazo para resolver: 30 días hábiles luego de la absolución del reclamado, ampliable por 30 días hábiles adicionales.

Recurso de apelación

- La DGTAIPD se encarga de resolver. El plazo máximo de atención es de 30 días hábiles.
- La resolución agota la vía administrativa.

XVII. ¿Qué es el procedimiento administrativo sancionador?

La ANPD puede iniciar de oficio procedimientos administrativos sancionadores contra cualquier titular del banco de datos, responsable o encargado de su tratamiento que incumpla las disposiciones de la LPDP y su Reglamento. En caso de que se determine la responsabilidad por haber incurrido en una infracción, la autoridad podrá imponer una multa cuyo monto dependerá de la gravedad de dicha infracción (leve, grave o muy grave).

Cabe precisar que, de forma previa al inicio del PAS, se lleva a cabo del procedimiento de fiscalización. Este se encuentra a cargo de la DFI y se instaura por: (i) iniciativa propia; o, (ii) denuncia informativa de cualquier persona natural y/o entidad jurídica o privada. Los requisitos para que cualquier ciudadano o entidad presente una denuncia por el mal tratamiento de datos personales pueden ser consultados en el siguiente enlace: https://bit.ly/3QB5qis.

A través del procedimiento de fiscalización se busca determinar la concurrencia o existencia de hechos que justifican el inicio de un PAS contra cualquier TBD, responsable y/o encargado del tratamiento de datos que ha incumplido las obligaciones establecidas en la normativa de protección de datos.

El PAS se desarrolla de la siguiente manera:

- A cargo de la DFI.
- Plazo: 50 días hábiles.

- A cargo de la DPDP.
- Plazo: 20 días hábiles luego de recibido el informe y resolución de cierre de etapa instructiva de la DFI.

- Es opcional.
- Plazo para su interposición: 15 días hábiles.
- Se formula ante la DPDP, quien debe resolver dentro de 30 días hábiles.

- Plazo para su interposición: 15 días hábiles.

  La DGTAIPD se encarga de resolver.
- La resolución agota la vía administrativa.

Apéndice

Casos relevantes para la aplicación de la LPDP y su Reglamento por parte de los ODP

a) Sobre tratamiento de datos relacionados a la salud

Opinión Consultiva N.º 11-2022-JUS/DGTAIPD (22/04/2022)

La presente opinión versa sobre la procedencia de transferir datos relacionados con la salud por parte del Centro Nacional de Epidemiología, Prevención y Control de Enfermedades del MINSA al Observatorio Nacional de Seguridad Vial – ONSV, según el artículo 8 del Decreto Legislativo N.° 1216.

Se concluye que, existe una habilitación legal establecida en el artículo 8 del Decreto Legislativo N.° 1216 para que el Centro Nacional de Epidemiología, Prevención y Control de Enfermedades remita al ONSV información relacionada a diagnósticos médicos vinculados al documento de identidad, únicamente respecto de aquellos casos que estén vinculados a accidentes de tránsito, respetando los principios de finalidad y de proporcionalidad. Ello a efectos de poder articular información remitida por diversas entidades públicas.

https://bit.ly/41dYb5M

Opinión Consultiva N.º 26-2022-JUS/DGTAIPD (05/08/2022)

Esta opinión trató acerca de si procede atender los requerimientos de información realizados por el Ministerio Público, vinculados a datos personales sensibles.

En ese sentido se señala que el Ministerio Público no se encuentra legitimado expresamente para acceder a datos personales sensibles relacionados a la salud (por ejemplo, aquellos vinculados al COVID-19) que obren en poder de entidades públicas, en tanto no existe habilitación legal que le permita acceder a información confidencial sin autorización judicial previa.

Sin embargo, existe una habilitación legal establecida en el artículo 5° de la Ley N°26626, respecto a los datos personales sensibles (pruebas diagnosticadas con VIH/SIDA y la información sobre la causa cierta o probable de contagio), que permiten su entrega por parte del Ministerio de Salud al Ministerio Público para fines de investigación del delito, lo que constituye una excepción a la obligación de solicitar el consentimiento al titular del dato personal, conforme numerales 1 y 13 del artículo 14 de la LPDP.

https://bit.ly/40YHOu8

b) Sobre la información contenida en cámaras de video vigilancia

Opinión Consultiva N.º 33-2022-JUS/DGTAIPD (02/09/2022)

La presente opinión absolvió la consulta referida a la posibilidad de acceso a la información contenida en las grabaciones de las cámaras de videovigilancia de las entidades públicas, y si estas pueden contener información de carácter secreto, reservado o confidencial.

Se precisó que, en virtud del inciso 6 del artículo 17 del TUO de la LTAIP referida a la información confidencial, es posible determinar que la restricción al acceso a las grabaciones de cámaras de videovigilancia en bienes de dominio público se regula por el Decreto Legislativo 1218, como un supuesto de excepción el acceso a la información (imágenes, videos y/o audios), por configurar información confidencial.

En esa línea, las entidades públicas pueden estimar la denegación del acceso a la información contenida en las grabaciones de cámaras de videovigilancia por considerarla de carácter restringido, no obstante, deberán entregarla cuando sea solicitada a través del juez, quien sí está habilitado por la LTAIP a acceder (o disponer el acceso) a dicha información.

https://bit.ly/3mYifdE

c) Acerca de la interoperabilidad

Opinión Consultiva N.º 09-2022-JUS/DGTAIPD (31/01/2022)

En esta opinión se determinó que era procedente que la UGEL N.° 07 requiera a la directora de la institución educativa el registro de datos de los padres de familia (nombres, apellidos, DNI, teléfonos y correos electrónicos) en el módulo de Estudiantes del Sistema de Información de Apoyo a la Gestión de la Institución Educativa - SIAGIE, ya que se encontraba habilitada en virtud de la Resolución Ministerial N.° 432-2020-MINEDU del 28 de octubre de 2020 y por tanto, estaba dentro de sus competencias, siendo acorde al principio de proporcionalidad.

Así, las instituciones educativas pueden realizar tratamiento de los datos personales de sus estudiantes o de los padres de familia que deban encontrarse registrados en el repositorio central de registros del SIAGIE, sin solicitar el consentimiento, según el artículo 14 de la LPDP, sin perjuicio de cumplir los demás principios. Sin embargo, cuando se requiera transferir a terceros los datos de los estudiantes o padres de familia para fines distintos a los relacionados al registro del SIAGIE, se requerirá del consentimiento libre, previo e informado del titular de dichos datos, o, en el caso de menores de edad, de los padres de familia, quienes ejercen la patria potestad.

https://bit.ly/3KcsRgl

Opinión Consultiva N.º 10-2022-JUS/DGTAIPD (23/03/2022)

La presente opinión versa sobre el acceso a la base de datos del Registro Nacional de Sanciones contra Servidores Civiles - RNSSC por parte de la Contraloría General de la República- CGR.

Al respecto, la CGR, como entidad pública, no requiere el consentimiento de los titulares de los datos personales para acceder a la información del RNSSC, en el marco de sus competencias otorgadas por ley, en esa línea, se encuentra legitimada para acceder a la información y documentación sobre las operaciones de las entidades sujetas al ámbito de control gubernamental, aunque sea secreta.

Sin embargo, ello no debe entenderse de modo irrestricto, dado que se debe respetar el principio de proporcionalidad, en ese sentido, no es acorde a dicho principio que la CGR acceda a información sobre el régimen histórico de sanciones no vigentes impuestas a funcionarios públicos, en el marco de la fiscalización del cumplimiento de la obligación de declaración jurada de intereses, dado que dicha información no resulta necesaria para efectos de la fiscalización.

https://bit.ly/3KJWUxR

d) De los límites al tratamiento de datos

Opinión Consultiva N.º 17-2022-JUS/DGTAIPD (17/06/2022)

En la presente opinión, se trató acerca de la publicación de la relación de administrados que hubieren presentado declaraciones, información o documentos falsos o fraudulentos por la Central de Riesgo Administrativo-CRA.

Se precisó que, en la medida que existe interés público en conocer la relación de administrados infractores que publica la CRA (por derivar del ejercicio de la función pública de fiscalización posterior), los datos personales de las personas naturales contemplados por el artículo 34, numeral 34.4 del TUO de la LPAG (identidad y DNI) no estarían protegidos por el artículo 17, inicio 5 del TUO de la LTAIP.

La excepción del artículo 17, inicio 5 del TUO de la LTAIP cautela los datos de las personas naturales, cuya difusión no revista interés público y, por el contrario, suponga una intromisión en la intimidad.

https://bit.ly/3MnpTbX

Informe Jurídico N.º 12-2022-JUS/DGTAIPD (11/07/2022)

El presente informe jurídico trata, entre otros, sobre la procedencia del acceso a la información referida a nombres y apellidos de las víctimas y agresores contenidas en la base de datos del Registro Único de Víctimas y Agresores (RUVA) y del Registro Nacional de Condenas a cargo del Ministerio Público, concluyéndose que es desproporcional y contrario al inciso 13.8. del artículo 13 de la LPDP la publicación de dicha información.
Ello considerando que no resultaba necesario que dicha información sea de conocimiento público, teniendo en cuenta que estas bases de datos fueron creadas para ayudar a los operadores de justicia e instituciones intervinientes en la toma de decisiones destinadas al cumplimiento de sus funciones, sin embargo, lo contrario podría ocasionar la estigmatización de víctimas y de supuestos agresores.

https://bit.ly/3H5xMzl

Informe Jurídico N.º 21-2022-JUS/DGTAIPD (03/10/2022)

En el presente informe jurídico se hizo mención acerca del tratamiento de datos en el marco de la persecución del delito.

Al respecto, Osiptel administra un registro denominado RENTESEG, mediante el cual recopila y registra información acerca de equipos terminales móviles y de sus abonados. Dicho registro coadyuva a las funciones ejercidas por la Policía Nacional del Perú-PNP y el Ministerio Público-MP, instituciones que se vinculan con la seguridad pública y la persecución e investigación de delitos.

En ese marco, Osiptel solo debe acceder a la información para el cumplimiento de sus funciones, es decir, a la estrictamente necesaria para la administración del RENTESEG. No siendo proporcional que acceda a datos personales adicionales que figuran en las denuncias, tales como los nombres de los denunciados.

https://bit.ly/43WgbDM

e) En relación a la confidencialidad

Resolución Directoral N.° 69-2021-JUS/DGTAIPD (28/10/2021)

En el presente caso se trató sobre la responsabilidad del Hospital de Emergencias José Casimiro Ulloa por vulnerar el deber de confidencialidad en el tratamiento de los datos personales que administra, conforme a lo establecido en el artículo 17 de la LPDP.

Se precisó que si bien fue uno de los trabajadores de dicho hospital quien divulgó los datos personales (fotografías) de un paciente que se encontraba en la sala de trauma shock sin su consentimiento, dicha institución debía garantizar que el personal a su cargo cumpla con la obligación de confidencialidad respecto de los datos personales que manejan.

https://bit.ly/3NaAN5d

Resolución Directoral N.° 05 2023-JUS/DGTAIPD (14/02/2023)

En el presente caso se trató sobre la responsabilidad de la PNP por vulnerar el deber de confidencialidad de los datos personales establecido en el artículo 17 de la LPDP, debido a que se había acreditado que ciertos efectivos policiales estaban utilizado sus credenciales de acceso al Sistema Informático de Registro de Antecedentes Policiales (SIDPOL) y al Sistema de Información Policial (ESINPOL) para poner a disposición de empresas terceras, información contenida en los antecedentes policiales, para fines particulares, vulnerando con ello el principio de confidencialidad.

En ese sentido, se precisó que la PNP se encuentra obligada a asegurar el cumplimiento del deber de confidencialidad al ser la persona jurídica de derecho público que tiene a cargo el SIDPOL y ESINPOL, lo cual implica también instruir a sus dependientes o empleados/terceros autorizados al cumplimiento de las garantías de protección de los datos, de modo tal que estos últimos no realicen un tratamiento indebido de los datos.

https://bit.ly/3qnjJQ3

PERÚ | Ministerio de Justicia y Derechos Humanos

Autoridad Nacional de Protección de Datos Personales

CONSULTAS TELEFÓNICAS
(01) 204 8020 – anexo 2410
De lunes a viernes de 8:00 a.m. a 4:30 p.m.

CORREO ELECTRÓNICO:
protegetusdatos@minjus.gob.pe

MESA DE PARTES:

Presencial: Calle Scipión Llona N° 350, Miraflores - Lima

Virtual: https://sgd.minjus.gob.pe/sgd-virtual/public/ciudadano/ciudadanoMain.xhtml

www.gob.pe/anpd

Con Punche Perú