consejo para la Transparencia

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICAS

Sobre la base de lo dispuesto en la **Ley N°19.628**, sobre Protección de la Vida Privada y en las Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado, de diciembre de 2020.

RESUMEN EJECUTIVO

1- Este Consejo ha elaborado la presente guía, con la finalidad de contribuir a elevar los estándares de protección de los datos personales en poder de los órganos públicos a fin de asegurar los derechos que la Constitución Política y las leyes reconocen a los titulares de los mismos.

Lo anterior, en línea con la protección constitucional y legal de los datos personales y con las acciones que este Consejo ha adoptado al respecto, en particular, la actualización de las Recomendaciones sobre Protección de Datos Personales por parte de los órganos públicos (las "Recomendaciones").

2- Así, sobre la base de dichas Recomendaciones y con el ánimo de apoyar a los funcionarios y funcionarias de los órganos de la Administración del Estado y las municipalidades en las operaciones de tratamiento de datos personales que deban ejecutar en el cumplimiento de sus funciones, es que se expone sobre **(i)** definiciones fundamentales en materia de protección de datos personales; **(ii)** sus principios informadores; **(iii)** obligaciones de los órganos de la Administración del Estado en materia de tratamiento de datos personales; **(iv)** reglas específicas para el tratamiento de datos sensibles; **(v)** directrices sobre comunicación o transmisión de los datos personales; y **(vi)** la obligación de adoptar medidas de seguridad de las bases de datos y obligaciones asociadas al tratamiento de datos para encuestas, estudios de mercado y sondeos de opinión.

3- Finalmente, se formulan una serie de recomendaciones en materia de tratamiento y protección de los datos personales, atendiendo el cumplimiento de la función pública, además de considerar el derecho fundamental a la protección de datos personales.

ÍNDICE DE CONTENIDOS

Esta guía tiene por objeto orientar el resguardo del **derecho fundamental a la protección de datos personales**, además de entregar criterios prácticos a funcionarios y funcionarias de los órganos de la Administración del Estado y municipalidades, para el tratamiento de datos personales que realicen, a fin de dar cumplimiento a las obligaciones legales que éstos tienen como responsables del tratamiento.

Introducción

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICA

Introducción

A partir del año 2018, la Constitución Política asegura expresamente a **todas las personas el derecho a la protección de los datos personales** y establece que el tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley. Este derecho fundamental opera como límite al ejercicio de la soberanía y, por tanto, delimita la acción de los órganos estatales en materia de procesamiento de datos personales.

La reforma constitucional estableció, además, una reserva legal especial, en virtud de la cual el tratamiento y la protección de datos personales se realizará en la forma y condiciones que determine la ley.

Esta reserva es especialmente relevante para los órganos del Estado, atendido el principio de legalidad o juridicidad en la actuación del Estado.

La protección de datos personales se encuentra regulada en la Ley N°19.628, sobre Protección de la Vida Privada, *que establece las reglas sobre tratamiento de datos personales que realicen tanto los órganos públicos como particulares, determina un conjunto de derechos de los titulares y las obligaciones de los responsables del tratamiento.*

Los mecanismos de recolección, procesamiento y transferencia de datos personales se han intensificado en la última década y el proceso de digitalización de la Administración del Estado ha significado que estas operaciones se incrementen de manera constante.

Considerando tanto que la **Ley N°19.628** es una ley de larga data, no actualizada a los estándares modernos tanto técnicos como jurídicos sobre protección de datos personales, como también que el entendimiento íntegro de esta normativa puede ser complejo para los funcionarios y funcionarias que deben aplicar esta Ley, es que se elabora la siguiente guía, la que busca dos objetivos fundamentales:

1- Dar claridad en la comprensión y aplicación de las reglas de protección de datos personales para todos los funcionarios y funcionarias quienes tengan que cumplir aquellas, en el marco del ejercicio de sus funciones.

2- El Consejo para la Transparencia estima necesario contribuir a elevar los estándares de protección de los datos personales en poder de los órganos públicos a fin de asegurar los derechos que la Constitución y las leyes reconocen a sus titulares. Por tal razón, en diciembre de 2020 aprobó las Recomendaciones sobre Protección de Datos Personales por parte de los órganos públicos[1] y ahora, sobre la base de dichas recomendaciones, presenta la siguiente Guía Protección Datos Personales para Instituciones Públicas

Conforme lo indicado, esta guía se ha elaborado en atención a lo dispuesto en la Ley N°19.628 y las Recomendaciones, las cuales han tenido presente las legislaciones y modelos de protección de datos personales comparados.

[1] *Resolución Exenta N°304, de 30 de noviembre de 2020, publicada el Diario Oficial.*

Definiciones esenciales

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICA

Definiciones esenciales

Para una mejor comprensión de la Guía y de la ley, resulta esencial definir y explicar los conceptos más importantes que utilizaremos y que se sustentan en las definiciones que establece la **Ley N°19.628**.

1-

Datos personales:

Son los relativos a cualquier información concerniente a personas naturales, identificadas o identificables. Puede ser su nombre, RUT, una fotografía de su rostro, sus huellas dactilares o el historial de su navegación en internet, por mencionar algunos. No importa que los datos estén en un soporte papel o electrónico.

Basándonos en la definición legal, para determinar si un dato corresponde a un dato de carácter personal es importante verificar que se cumplan dos condiciones:

i) Debe tratarse de información sobre una persona natural (por lo que no aplica a personas jurídicas como empresas o sociedades).

ii) Debe tratarse de información que permita identificar al titular. Una persona es identificable cuando su identidad pueda determinarse, directa o indirectamente, mediante identificadores, siempre y cuando el esfuerzo de determinación no resulte excesivo o desproporcionado. Identificadores pueden ser una huella dactilar, el RUT, o antecedentes económicos, sociales o culturales de una persona (como la pertenencia a un grupo, club o asociación).

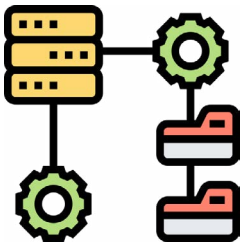
Los datos personales pueden ser privados (como un dato de salud) o públicos (como el nombre) lo que no incide en su calificación legal como dato personal. La ley aplica tanto para los datos personales públicos como los privados.

2-

Datos sensibles:

Son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

3-



Registro o bases de datos:

Es el conjunto organizado de datos de carácter personal, sea automatizado o no, y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos. Una base de datos puede ser un archivador con fichas de personal, un software que gestione datos o incluso una planilla electrónica.

4-

Responsable del registro o banco de datos:

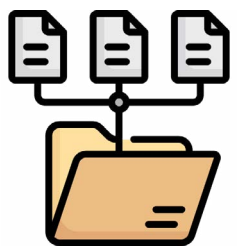
Es, en el contexto de esta Guía dirigida a funcionarios públicos, el organismo público que realiza el tratamiento de datos personales dentro del ámbito de sus competencias y para el cumplimiento de sus funciones legales, ya sea que lo realice directamente por sí mismo, o a través de un tercero encargado. También se le denomina, habitualmente, como "responsable del tratamiento de datos" o "responsable de datos".

5-

Encargado o mandatario del tratamiento de datos:

Es aquella persona, natural o jurídica, que realiza un tratamiento de datos por cuenta del responsable del registro o banco de datos. En la administración del Estado usualmente se externalizan diversos tratamientos de datos personales, los que son realizados por empresas que tienen la calidad de encargados del tratamiento.

6-



Tratamiento de datos:

Es cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

7-

Fuentes accesibles al público:

Son los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

8-

Dato caduco:

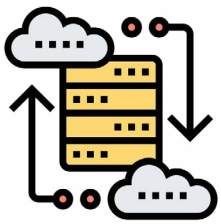
Es el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

9-

Dato estadístico:

Es aquel dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

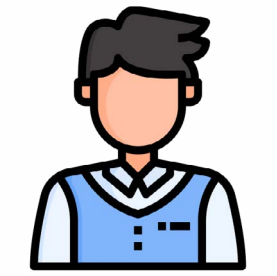
10-



Procedimiento de disociación de datos:

Es todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

¿Quiénes intervienen en el tratamiento de datos personales?



Titular de datos personales

Responsable del tratamiento

Encargado del tratamiento

Principios orientadores de la protección de datos personales

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICA

Principios orientadores de la protección de datos personales

Los principios ayudan a orientar la forma de aplicar las reglas sobre protección de datos por parte de los órganos públicos y son útiles cuando no existen reglas o normas específicas para un caso particular.

1-

Los principios que se consagran en la Ley N°19.628 son los de:

Licitud; calidad; finalidad; seguridad; confidencialidad; especial protección de datos personales sensibles; e información. Estos principios, si bien no se encuentran en un catálogo expreso, se pueden extraer de sus mismas disposiciones.

i.

Principio de licitud (artículos 4 y 20 de la Ley N°19.628).
El tratamiento de datos personales debe realizarse con sujeción a la ley y las bases de licitud que establece. Respecto de los órganos públicos, se consagra una habilitación legal genérica en el artículo 20 de la Ley N°19.628, que permite a éstos realizar tratamiento de datos personales solo respecto de las materias de su competencia y con sujeción a los artículos 1 al 19 de la misma ley.

En otras palabras, los órganos públicos sólo pueden realizar tratamiento de datos personales cuando exista autorización legal, o cuenten con el consentimiento previo, expreso y por escrito del titular

ii. **Principio de calidad de los datos (artículo 9 de la Ley N°19.628).**
Los datos contenidos en una base de datos deben ser exactos, actualizados y responder con veracidad a la situación real de su titular.

iii. **Principio de finalidad (artículo 9 de la Ley N°19.628).**
Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados. En el caso de los organismos públicos, la finalidad estará determinada por las materias propias de su competencia y por la función legal específica que está ejecutando y que justifica el procesamiento de datos personales.

iv. **Principio de seguridad (artículo 11 de la Ley N°19.628).**
Los organismos públicos deben adoptar medidas de seguridad técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información.

v. **Principio de confidencialidad o secreto (artículo 7 de la Ley N°19.628).**
Los funcionarios que trabajan en el tratamiento de datos personales o tengan acceso a éstos, están obligados a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, incluso después de terminada su relación laboral.

vi. **Deber de protección especial de los datos personales sensibles (artículo 10 de la Ley N°19.628).**
Existe una prohibición general de tratamiento de datos personales sensibles, salvo cuando una disposición legal lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

vii. **Deber de información (artículos 4 y 20 de la Ley N°19.628).**
Los organismos públicos están obligados a informar al titular acerca de la identidad del órgano responsable de la base de datos, la finalidad perseguida con el tratamiento de la información y de su posible comunicación a terceros.

2-

Otros principios que informan el tratamiento de datos personales son los de:

Proporcionalidad y responsabilidad. Estos principios son aplicados frecuentemente en otras ramas del derecho, y han sido reconocidos en la legislación comparada sobre datos personales.

i.

Principio de proporcionalidad.
Sólo pueden recabarse aquellos datos que sean necesarios para conseguir los fines que justifican su recolección. En aplicación de este principio, se recomienda a los órganos de la Administración del Estado optar, de entre los diversos tratamientos que le permitan conseguir los fines pretendidos dentro del ámbito de sus competencias, por aquel que menor incidencia tenga en el derecho a la protección de datos personales y por la utilización de los medios menos invasivos.

ii.

Principio de responsabilidad.
Quienes realicen tratamiento de datos personales serán responsable del cumplimiento de los principios, obligaciones y deberes de conformidad a la ley.

Derechos de los titulares de datos personales

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICA

Derechos de los titulares de datos personales

Conforme el artículo 12 y siguientes de la Ley N°19.628, los titulares de datos personales pueden ejercer, ante los organismos públicos que tengan la calidad de responsables, los siguientes derechos:

a. **Derecho a acceder a sus propios datos.**
Toda persona tiene derecho a exigir información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

b. **Derecho de rectificación o modificación.**
Toda persona tiene derecho a exigir que los datos que sean erróneos, inexactos, equívocos o incompletos, se modifiquen, siempre que se acredite debidamente cualquiera de dichas circunstancias y se indique con claridad la corrección solicitada.

c. **Derecho de cancelación o eliminación.**
Toda persona tiene derecho a exigir que se eliminen aquellos datos cuyo almacenamiento carece de fundamento legal; se encuentren caducos –según la definición legal entregada previamente; los haya proporcionado voluntariamente; o ellos se utilicen para comunicaciones de carácter comercial y el titular no desee seguir figurando en el registro de datos.

d. **Derecho al bloqueo de datos.**
Toda persona tiene derecho a exigir la suspensión temporal de cualquier operación de tratamiento de los datos almacenados, cuando el titular ha proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones informativas y no desee continuar figurando en el registro respectivo de modo temporal o definitivo. También procede cuando la exactitud de los datos personales no pueda ser establecida o cuya vigencia sea dudosa y respecto a los cuales no corresponda la cancelación.

El ejercicio de estos derechos no es absoluto, por lo que los organismos deben, antes de determinar su procedencia, verificar la concurrencia de alguna de las causales de denegación que establece la Ley N°19.628, *como, por ejemplo, cuando el ejercicio de los derechos impida o entorpezca el cumplimiento de funciones fiscalizadoras del organismo; cuando afecte la reserva o secreto establecido en disposiciones legales o reglamentarias, o la seguridad de la nación o el interés nacional; o cuando el ejercicio de los derechos se efectúe respecto de datos personales que están siendo almacenados por mandato legal.*

Obligaciones específicas de los órganos públicos

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICA

Obligaciones específicas de los órganos públicos

Condiciones de licitud en el tratamiento de los datos. Como ya dijimos, la habilitación legal genérica de tratamiento de datos personales de los órganos públicos está contenida en el **artículo 20 de la Ley N°19.628**, que permite a dichos órganos públicos realizar tratamiento de datos personales solo respecto de las materias de su competencia y con sujeción a las reglas de los artículos 1 al 19 de la misma ley.

Eventualmente, un órgano de la Administración del Estado podría realizar tratamiento de datos personales obteniendo el consentimiento del titular dando cumplimiento a las reglas del **artículo 4 de la Ley N°19.628**. En este caso, el órgano deberá requerir el consentimiento por escrito, el que podrá ser revocado por el titular o su representante legal.

Obligaciones para el tratamiento de datos. Los órganos que actúen como responsables deben sujetarse a las siguientes reglas:

a. **Informar al titular de los datos el propósito del almacenamiento de sus datos personales**, es decir, la finalidad perseguida con el tratamiento de la información, la posible comunicación a terceros, y la denominación del órgano o servicio responsable del tratamiento (artículos 4 y 20 de la Ley N°19.628).

b. **Efectuar el tratamiento de los datos personales cumpliendo con el principio de finalidad** (artículo 9 de la Ley N°19.628).

c. **De oficio y sin necesidad de requerimiento del titular de los datos:** eliminar los datos caducos conforme establece su definición legal en la letra d), del artículo 2, de la Ley N°19.628, y aquéllos que se encuentren fuera de su competencia por carecer de fundamento legal; bloquear los datos cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación; y modificar los datos inexactos, equívocos o incompletos (artículo 6 de la Ley N°19.628).

d. **Cuidar de los datos personales que traten con la debida diligencia**, haciéndose responsable de los daños (artículo 11 de la Ley N°19.628).

e. **Cumplir con la obligación de secreto o confidencialidad** en relación con los datos que provengan o hayan sido recolectados de fuentes no accesibles al público (artículo 7 de la Ley N°19.628).

Además de estas obligaciones legales, se recomienda a los organismos adoptar medidas tendientes a formar, capacitar y entrenar a sus funcionarios en el cumplimiento de las disposiciones de la Ley N°19.628 y respecto del derecho fundamental a la protección de datos personales.

Reglas especiales para el tratamiento de datos personales sensibles

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICA

Reglas especiales para el tratamiento de datos personales sensibles

La **Ley N°19.628** identifica una categoría especial de datos personales denominados datos sensibles, que son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Como señalan las Recomendaciones, al tratarse de una definición legal de carácter abierto, el concepto de dato personal sensible puede abarcar aspectos disímiles entre sí. Por ello, los órganos públicos deben tener presente, al menos, las siguientes categorías de datos personales sensibles que se extraen de la definición legal:

a. **Datos que se refieren a características físicas de una persona**, tales como datos biométricos, datos biológicos, datos de salud ya sea física, psíquica, entre otros.

b. **Datos que se refieren a características morales de una persona**, tales como información sobre orientación o preferencia sexual, creencias o convicciones religiosas, éticas o políticas, entre otros.

c. **Datos que se refieren a hechos o circunstancias de su vida privada o intimidad**, tales como los hábitos personales, la información sobre desplazamiento geográfico, la geolocalización, los datos asociados a la navegación en internet, entre otros.

Según establece el artículo 10 de la Ley N°19.628, existe una prohibición general de tratamiento de datos personales sensibles, salvo cuando **(i)** una disposición legal lo autorice, **(ii)** exista consentimiento del titular o **(iii)** sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares. **De esta manera, únicamente los órganos públicos que cumplan con alguna de esas condiciones expresas podrán realizar tratamiento de datos personales sensibles.**

Comunicación o transmisión de datos personales

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICA

Comunicación o transmisión de datos personales

La comunicación o transmisión de datos personales no está regulada expresamente en la **Ley N°19.628**. Sin embargo, las Recomendaciones disponen las siguientes orientaciones para que los órganos puedan efectuar esta clase de tratamiento:

a. **Los organismos públicos** podrán establecer procedimientos de comunicación, transmisión o cesión de datos de carácter personal para fines que digan directa relación con sus competencias legales y las de los organismos participantes, respecto del ejercicio de funciones específicas contenidas en sus respectivas leyes orgánicas o en otras disposiciones legales que expresamente los faculten para tales efectos, aplicando además los principios que informan el tratamiento.

b. **El receptor sólo podrá utilizar los datos personales para los fines que motivaron la transmisión**. Dicho procedimiento podrá contemplar las siguientes etapas: requerimiento expreso, admisibilidad de este y firma de un convenio de transmisión.

Las Recomendaciones del CPLT profundizan en estos lineamientos para la comunicación o transmisión de datos personales, los cuales se sugiere que sean tenidos a la vista por los organismos públicos en sus actividades de tratamiento.

Tratamiento de datos a través de un encargado

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICA

Tratamiento de datos a través de un encargado

Los órganos pueden encargar el tratamiento de los datos a un tercero, que tendrá la calidad de encargado o mandatario. Esta clase de tratamiento está regulada en el artículo 8 de la **Ley N°19.628**, que requiere que el mandato sea otorgado por escrito, dejando especial constancia de las condiciones de utilización de los datos por el tercero encargado. Para abordar este requisito, sugerimos tener presente las menciones que se señalan en las Recomendaciones del CPLT respecto del tratamiento de datos a través de un encargado.

Por su parte, se sugiere incorporar las mismas menciones en las contrataciones de bienes y servicios que se realicen en un proceso de contratación regido por la **Ley N°19.886**, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios y que involucren un tratamiento de datos personales a través de un encargado. En este caso, se recomienda que el órgano de la administración del Estado licitante incorpore, desde el diseño de las bases administrativas y técnicas, las menciones señaladas.

Se hace presente que, aún cuando opere la figura del tratamiento de datos a través de un encargado, la responsabilidad ulterior del tratamiento frente al titular de datos será del responsable del banco de datos que, en el contexto de esta Guía, corresponde al organismo público. Esto, ya sea que el encargado del tratamiento efectúe sus operaciones en Chile o en el extranjero.

Obligación de adoptar medidas de seguridad de los bancos o registros de datos

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICA

Obligación de adoptar medidas de seguridad de los bancos o registros de datos

Conforme lo dispuesto en el **artículo 11 de la Ley N°19.628**, los órganos públicos deben cuidar de los datos personales que traten con la debida diligencia, haciéndose responsable de los daños.

En las Recomendaciones, esta obligación se ha precisado en cuanto al deber de adoptar todas las medidas de seguridad (incluyendo de seguridad informática y ciberseguridad), tanto organizativas, técnicas y de formación de capital humano, para resguardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros. Esto, con la finalidad de evitar la alteración, filtración, pérdida, transmisión y acceso no autorizado de los mismos.

Obligaciones en caso de tratamiento de datos para encuestas, estudios de mercado y sondeos de opinión

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICA

Obligaciones en caso de tratamiento de datos para encuestas, estudios de mercado y sondeos de opinión

De acuerdo con el **artículo 3 de la Ley N°19.628**, cuando un organismo público recolecte datos personales a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que la ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información.

La comunicación de sus resultados debe omitir la información que pueda permitir la identificación de las personas consultadas, debiendo sólo comunicarse los datos que tengan la calidad de estadísticos, es decir, los que, en su origen o como consecuencia de un tratamiento, no pueden ser asociados a un titular identificado o identificable.

Recomendaciones sobre protección de datos personales por diseño

GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICA

Recomendaciones sobre protección de datos personales por diseño

El CPLT recomienda a los órganos públicos desarrollar e implementar sus sistemas de procesamiento bajo los siguientes principios que inspiran la protección de datos personales por diseño:

1. **Principio de proactividad y prevención.**
Es recomendable que los órganos públicos diseñen, implementen y operen sus sistemas de procesamiento de datos personales identificando previamente los riesgos al derecho a la protección de datos personales de los titulares, propendiendo a una gestión adecuada, mediante su neutralización o mitigación.

2. **Principio de protección predeterminada.**
Es recomendable que los órganos públicos proporcionen a los titulares de datos personales el más alto nivel de protección de sus datos por defecto y de manera automática en los sistemas de procesamiento de datos que desarrollen, implementen u operen.

3. **Principio de protección desde el diseño.**
Es recomendable que los órganos públicos incorporen la protección de datos personales como un componente esencial e indispensable de los sistemas de procesamiento de datos personales que desarrollen, implementen u operen, desde su diseño.

4. **Principio de funcionalidad total.**

Es recomendable que los órganos públicos comprendan sus sistemas de procesamiento de datos personales como sistemas funcionales eficaces y eficientes tanto respecto de su propósito principal (el cumplimiento de su mandato legal) como respecto del derecho constitucional a la protección de datos personales. Se recomienda la existencia de reglas y mecanismos que permitan una coexistencia balanceada entre el resguardo y protección del derecho, y los objetivos de los mecanismos de procesamiento de datos.

5. **Principio de seguridad punta a punta.**

Es recomendable que los órganos públicos protejan el ciclo completo del procesamiento de datos personales, desde su diseño, implementación y operación, adoptando las medidas necesarias para garantizar la seguridad de la información (integridad, confidencialidad y disponibilidad) como el uso de cifrado en todo momento, la anonimización temprana, la definición de roles de acceso a datos, la destrucción segura de datos y el establecimiento de mecanismos para el ejercicio de los derechos de los titulares.

6.

Principio de visibilidad y transparencia.

Es recomendable que los órganos públicos adopten las medidas de transparencia necesarias respecto a sus sistemas de procesamiento de datos personales, informando a los titulares sobre la recolección, procesamiento, eventual comunicación y purga de datos, a través de políticas legibles de protección de datos personales y mecanismos de notificación a titulares.

7.

Principio de enfoque centrado en el usuario.

Es recomendable que los órganos públicos pongan en funcionamiento, en el nivel operacional, el mandato constitucional de tutela del derecho a la protección de los datos personales al momento de diseñar, implementar y operar un sistema de procesamiento de datos personales manteniendo un enfoque centrado en las personas. Esto significa que se deben adoptar sistémicamente las medidas necesarias para garantizar un efectivo control por parte del titular de los tratamientos de datos que se realicen y que le conciernan.

consejo para la
Transparencia

www.consejotransparencia.cl