Dirección ChileCompra

DIRECCIÓN DE COMPRAS Y CONTRATACIÓN PÚBLICA

APRUEBA DIRECTIVA DE CONTRATACIÓN PÚBLICA N° 45 SOBRE RECOMENDACIONES PARA ORGANISMOS PÚBLICOS SOBRE EL TRATAMIENTO DE DATOS PERSONALES EN SUS PROCEDIMIENTOS DE COMPRAS PÚBLICAS

SANTIAGO, 06 de febrero de 2025

VISTOS:

Lo dispuesto en la Ley N° 18.575 Orgánica Constitucional de Bases General de la Administración del Estado, cuyo texto Refundido, Coordinado y Sistematizado fue fijado por el D.F.L. N°1/19.653, de 2001, del Ministerio Secretaría General de la Presidencia; en la Ley N° 19.880, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; en la ley N° 19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios y el Decreto N°661 de 2024 del Ministerio de Hacienda, que Aprueba el Reglamento de esta; en la Ley N° 21.634 que moderniza la Ley N° 19.886 y otras leyes, para mejorar la calidad del gasto público, aumentar los estándares de probidad y transparencia e introducir principios de economía circular en las compras del Estado; en la Ley N°20.285 sobre Acceso a la Información Pública, en la Ley N°19.628 sobre Protección a la Vida Privada; en la Ley 21.719 que regula la protección y el tratamiento de los datos personales y crea la Agencia de protección de datos personales; en el Decreto Supremo N°792 de 2023 que nombra a la Directora de la Dirección de Compras y Contratación Pública; en la Resolución Exenta N° 537-B de 2024, de esta Dirección, que deja sin efecto la Resolución Exenta N° 035-B/2024 y aprueba Nuevo Estatuto Interno para la Dirección de Compras y Contratación Pública, y en la Resoluciones Nºs 7, de 2019, y 14, de 2022, de la Contraloría General de la República, que establece normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1. Que, la Dirección de Compras y Contratación Pública, en adelante e indistintamente la “Dirección”, “ChileCompra” o la “DCCP”, es un servicio público descentralizado, sometido a la supervigilancia del Presidente de la República, a través del Ministerio de Hacienda, que tiene como misión crear valor en el mercado de las compras públicas, desarrollando políticas e iniciativas con la finalidad de generar confianza y eficiencia, con altos estándares de Probidad y Transparencia tanto para organismos compradores como proveedores del Estado.

2. Que, lo anterior, se funda en las funciones que el ordenamiento jurídico le encomienda a esta Dirección. Que, es así como el artículo 30 de la Ley de Compras, prescribe en su literal a) el deber de “asesorar a los organismos públicos en la planificación y gestión de sus procesos de compras y contrataciones” y en su literal g), la misión de “promover la máxima competencia posible en los actos de contratación de la Administración, desarrollando iniciativas para incorporar la mayor cantidad de oferentes. Además, deberá *ejercer una labor de difusión* hacia los

proveedores actuales y potenciales de la Administración, de las normativas, procedimientos y tecnologías utilizadas por ésta.”.

3. Que, en el mismo sentido, se contempla en el artículo 10 del Reglamento de Compras Públicas sancionado por el Decreto N° 661 del Ministerio de Hacienda, que esta Dirección en conformidad al literal a) señalado en el considerando precedente, podrá dictar directivas en el ejercicio de sus atribuciones, las cuales, tendrán como objetivo servir de referencia y guía para las Entidades en la planificación y gestión de sus procesos de compras y contrataciones, respetando el marco normativo aplicable.

4. Que, a través del Oficio Ordinario N°848 de fecha 2 de diciembre de 2021, esta Dirección adquirió el compromiso en materia de derechos humanos, con la Subsecretaría de Derechos Humanos, el emitir recomendaciones tendientes a que las entidades públicas compradoras contemplen medidas que resguarden los datos personales en el marco de los procedimientos de compras públicas que realicen a través del sistema de información www.mercadopublico.cl.

5. Que, en virtud de la existencia de las “Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado”, aprobados por la Resolución Exenta N°304 de 2020 del Consejo para la Transparencia, esta Directiva toma como fuente sustantiva dichas recomendaciones y tiene por objeto ejemplificar su aplicación en el ámbito de los procedimientos de compras públicas que se realicen a través del sistema de información www.mercadopublico.cl.

6. Que, para efectos de aprobar la señalada directiva, debe dictarse el correspondiente acto administrativo.

RESUELVO:

1. **APRUÉBASE,** la Directiva de Contratación Pública N° 45 sobre “Recomendaciones para organismos públicos sobre el tratamiento de datos personales en sus procedimientos de compras públicas”, cuyo texto se transcribe a continuación:

“DIRECTIVA DE CONTRATACIÓN PÚBLICA N° 45 SOBRE RECOMENDACIONES PARA ORGANISMOS PÚBLICOS Y PROVEEDORES DEL ESTADO SOBRE EL TRATAMIENTO DE DATOS PERSONALES EN SUS PROCEDIMIENTOS DE COMPRAS PÚBLICAS

1. OBJETIVO DE LA DIRECTIVA

La Dirección de Compras y Contratación Pública, en adelante ChileCompra, ha considerado necesario elaborar la presente directiva, que contiene diferentes recomendaciones tendientes a aclarar y orientar a los distintos organismos del Estado, a fin de que estos contemplen medidas oportunas que resguarden los datos personales de los usuarios compradores y proveedores en el marco de los procedimientos de compras públicas que

se realicen a través del Sistema de Información www.mercadopublico.cl.

En este sentido, se hace presente que esta Directiva, tomó como fuente sustantiva las "Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado", aprobados por la Resolución Exenta N°304 de 2020 del Consejo para la Transparencia, por lo que el objeto del presente instrumento es ejemplificar en materia de Compras Públicas, su correcta aplicación.

2. ALCANCE DE LA DIRECTIVA

Cabe recordar que las Directivas de Contratación que emite ChileCompra emanan de la función asesora de este organismo y constituyen orientaciones y lineamientos no vinculantes u obligatorios para los organismos del Estado, de acuerdo con los artículos 30, letra a), de la Ley N° 19.886 de Bases sobre los Contratos Administrativos de Suministro y Contratación de Servicios, en adelante Ley Compras Públicas y al artículo 10 del reglamento de dicha ley.

La presente directiva se encuentra, por un lado, dirigida a los funcionarios, funcionarias y autoridades de las entidades públicas sujetas a la Ley de Compras Públicas, en conformidad con su artículo 1°. Asimismo, este instrumento resulta aplicable a los contratos que celebren las mencionadas entidades, a título oneroso, para el suministro de bienes muebles, y de los servicios que se requieran para el desarrollo de sus funciones. Y, por otro lado, se encuentra dirigida a los oferentes y proveedores del Estado, a fin de que conozcan los derechos que poseen sobre la protección de sus datos personales, cuando actúan como proveedores del Estado o como terceros beneficiarios de una compra pública.

3. DEFINICIONES PREVIAS.

La Ley N°19.628 de Protección de la Vida Privada, establece en su artículo 2° una serie de definiciones a considerar para efectos de su aplicación, siendo relevante, en el marco de los procesos de compra y contratación, tener presente las siguientes:

- **Dato caduco**, 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.

- **Dato estadístico**, el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable

- **Datos personales**, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables, ya sea que se trate de información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, no importando el soporte en el que conste.

- **Datos sensibles,** 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.

- **Disociación de datos**, el procedimiento que se realiza para desvincular un conjunto de datos personales, de manera irreversible, de una persona determinada o determinable.

- **Encargado de tratamiento**, aquella persona natural o jurídica que realiza un tratamiento de datos por encargo o mandato del responsable de la base de datos, al que le serán aplicables las reglas generales en la materia. También se le denomina mandatario. El mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos, y el mandatario estará obligado a respetar esas estipulaciones en el cumplimiento de su encargo.

- **Fuentes accesibles al público**, los registros de datos personales, públicos o privados, que están permanentemente a disposición del público y cuya consulta pueden ser realizada por cualquier persona.

- **Organismos públicos,** las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

- **Registro o banco de datos**, 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.

- **Responsable del registro o banco de datos**, para estos efectos, se entenderá que es 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 por sí mismo, o a través de un encargado. No obstante, el responsable también puede ser una persona natural o jurídica privada, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.

- **Titular de los datos,** la persona natural a la que se refieren los datos de carácter personal.

- **Tratamiento de datos**, cualquier operación o conjunto 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. Estas operaciones pueden ser realizadas directamente por el responsable del registro o, también, por el encargado del tratamiento.

4. PRINCIPIOS ORIENTADORES DE LA PROTECCIÓN DE DATOS Y RECOMENDACIONES PARA SU CUMPLIMIENTO EN CONTRATACIONES SOMETIDAS A LA LEY DE COMPRAS PÚBLICAS.

1. Principio de Legalidad.

A través de Ley N° 21.096 de 2018, se consagró constitucionalmente el Derecho a la Protección de Datos Personales, mediante su incorporación expresa al numeral cuarto del artículo 19 de la Carta Fundamental. En esta norma, se establece una reserva legal especial en virtud de la cual el tratamiento y la protección de datos personales se deberá realizar en la forma y condiciones que establezca la ley. En este sentido, el artículo 4 de la Ley N°19.628, sobre Protección de la Vida Privada, señala que sólo será posible tratar datos de carácter personal cuando exista autorización legal, ya sea en la propia recién indicada u otras normas de igual rango, o el titular consienta expresamente en ello.

En el caso de los organismos del Estado, la habilitación legal genérica para el tratamiento de datos personales se encuentra contenida en el artículo 20 de la Ley sobre Protección de la Vida Privada antes mencionada, que permite a los 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, entre las cuales se encuentran los principios de legalidad, calidad, seguridad y confidencialidad de los datos, junto con los deberes de información y especial protección de los datos personales sensibles, además de permitir el ejercicio de los derechos de los titulares.

Aplicación del principio de legalidad en el tratamiento de datos en contrataciones sometidas a la Ley de Compras Públicas:

En materia de contrataciones, la habilitación legal para tratar los datos personales se establece en la propia Ley de Compras Públicas, la cual crea dos Bancos de Datos que pueden contener datos personales, ambos administrados por la Dirección de Compras y Contratación Pública. El primero, denominado **Mercado Público o Sistema de Información**, el cual es regulado en los artículos 18 y siguientes, estableciendo que se trata de un sistema de acceso público y gratuito a través del cual los organismos públicos regidos por esta ley deben cotizar, licitar, contratar, adjudicar, solicitar el despacho y, en general, desarrollar todos sus procesos de adquisición y contratación de bienes, servicios y obras por dicho medio y además, publicar la información relativa a sus contrataciones en observancia al principio de Transparencia y Publicidad.

El segundo, es el **Registro de Proveedores**, regulado en el artículo 16 y 17 de la Ley de Compras Públicas, este es un registro electrónico de acceso público donde se inscriben todas las personas naturales y jurídicas, chilenas y extranjeras que no tengan causal de inhabilidad para contratar con los organismos del Estado.

2. Principio de calidad de los datos.

Este principio consiste en que los datos personales tratados deben ser exactos, adecuados, pertinentes y no excesivos, y deberá ser observado durante la recolección y su posterior tratamiento, incluyendo la eliminación o cancelación de datos. Concurren, por tanto, tres

principios rectores:

a. **Principio de veracidad.**

El principio de veracidad se traduce en que los organismos del Estado deben velar que los datos personales sean exactos, actualizados y responder con veracidad a la situación real de su titular, de conformidad con el inciso segundo del artículo 9° de la Ley de Protección de la Vida Privada. Por consiguiente y en virtud del artículo 6 de la misma Ley, el organismo público responsable de la base de datos deberá, sin necesidad de requerimiento del titular, deberá eliminar los datos caducos y aquellos que estén fuera de su competencia; bloquear los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuáles no corresponda su cancelación; y modificar los datos inexactos, equívocos o incompletos.

Aplicación del principio de veracidad en el tratamiento de datos en contrataciones sometidas a la Ley de Compras Públicas:

A fin de dar cumplimiento a este principio, los organismos compradores previo a publicar los actos administrativos relativos a un determinado procedimiento de compra en www.mercadopublico.cl, deben revisar la veracidad de los datos que este contiene.

Un ejemplo de posible incumplimiento de este principio, es la inclusión del nombre de un tercero como representante de un proveedor en un contrato determinado, siendo que dicha información no era parte de los Anexos presentados por el mismo proveedor.

Es dable hacer presente que en virtud de las características y funciones que la propia normativa le otorga a www.mercadopublico.cl relativa a la transparencia de los procedimientos de compras y contrataciones públicas, no es dable la aplicación de este principio respecto de los datos caducos. Así, por ejemplo, un contrato ya finalizado, no corresponde que sea eliminado en virtud de dicho principio.

En el caso del Registro de Proveedores, esta Dirección, responsable del Banco de Datos, obtiene información de distintos Bancos de Datos de la Administración del Estado de manera permanente, de los propios titulares de la Información al momento de la solicitud de inscripción en el Registro y de los Organismos Compradores respecto del comportamiento contractual de los primeros.

Un ejemplo de un posible incumplimiento de este principio es la inclusión como incumplimiento contractual de un proveedor respecto de un contrato celebrado por otro proveedor.

Sin perjuicio de lo indicado, según la propia normativa de compras públicas es el proveedor quien es responsable de mantener la información que le corresponde aportar al Registro de Proveedores actualizada.

Se hace presente que, en virtud de las características y funciones que la propia normativa le otorga al Registro de proveedores en lo relativo a la transparencia de los procedimientos de compras y contrataciones públicas, no es dable la aplicación

de este principio respecto de los datos caducos.

Así, por ejemplo, un incumplimiento informado como comportamiento contractual del proveedor, no corresponde que sea eliminado de Registro, por el hecho de que fuese pagada la multa asociada al incumplimiento por el proveedor, dado que la finalidad de dicho Banco de Datos es disponibilizar las medidas que se tomaron a un proveedor especifico.

En caso de existir una falta al principio de veracidad, los organismos compradores que detecten el incumplimiento o el titular de los datos pueden dirigirse con los antecedentes pertinentes y por los canales de atención disponibles al responsable del Banco de Datos, sea esta Dirección u otros organismos públicos, a fin de solicitar su actualización, eliminación o bloqueo, quienes resolverán aplicando las normativas que les sean aplicables sobre protección de la vida privada.

b. Principio de finalidad.

Según lo dispone el inciso primero del artículo 9° de la Ley N°19.628, los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados. La referida finalidad, en el caso de organismos del Estado, estará determinada en función de las materias propias de su competencia, por la función legal específica que está ejecutando y que justifica el procesamiento de datos personales.

Aplicación del principio de finalidad en el tratamiento de datos en contrataciones sometidas a la Ley de Compras Públicas:

En el caso de los datos recolectados por los organismos públicos en el marco de un procedimiento de contratación pública, estos en general tienen por finalidad dar cumplimiento a los requisitos de transparencia que la propia normativa define, la verificación de que el proveedor se encuentra habilitado para contratar con la Administración del Estado y la verificación del cumplimiento del proveedor de requisitos administrativos y técnicos establecidos en las respectivas bases de licitación o contrato, debiendo utilizarse solo para cumplir estos fines determinados.

Un ejemplo de un posible incumplimiento de este principio es la creación por parte de un organismo comprador y con los datos que recolecte, de un ranking de “buenos” o “malos” proveedores, que mantenga público en su sitio institucional o la entrega de datos a terceros con fines distintos para los cuales fueron proporcionados por el titular de los datos al organismo. De ambas situaciones se observa que el objetivo de estas, no se condice con las funciones que el ordenamiento jurídico le encomienda, por lo que vulneraria el principio tratado en este punto.

c. Principio de proporcionalidad.

Este principio es la manifestación de los principios de eficiencia, eficacia e idónea administración de los medios que deben observar los organismos del Estado. Este implica que sólo pueden recabarse aquellos datos que sean necesarios para conseguir los fines que justifican su recolección. Por tanto, se entenderá que se cumple con el principio de proporcionalidad cuando: el o los datos que se recolecten, así como su posterior tratamiento, sean adecuados o apropiados a la

finalidad que lo motiva; sean pertinentes o conducentes para conseguir la referida finalidad y no excesivos en relación con dicha finalidad para la cual se han obtenido, en el sentido que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia. En aplicación de este principio, los órganos o servicios públicos deberán 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.

Aplicación del principio de proporcionalidad en el tratamiento de datos en contrataciones sometidas a la Ley de Compras Públicas:

Como ya se indicó, en el caso de los datos recolectados por los organismos públicos en el marco de un procedimiento de contratación pública, en general tienen por finalidad dar cumplimiento a los requisitos de transparencia que la propia normativa define, la verificación de que el proveedor se encuentra habilitado para contratar con la Administración del Estado y la verificación del cumplimiento del proveedor de requisitos administrativos y técnicos establecidos en las respectivas bases de licitación o contrato.

Así, para dar cumplimiento a este principio, los Organismos Compradores al momento de requerir datos a los proveedores, o al establecer la necesidad de entrega de datos por estos en las bases de licitación, deben siempre tener en cuenta la finalidad para la cual se está requiriendo ese dato y si ese dato en particular es el que menor incidencia tiene en el derecho a la protección de datos personales de los proveedores.

Un ejemplo de un posible incumplimiento de este principio es la solicitud en las bases de licitación de la presentación de una copia de la cédula de identidad de los proveedores o de sus representantes legales al momento de presentar su oferta y no solo al proveedor que resulte adjudicado, pudiendo llegar a esta conclusión haciendo el siguiente análisis:

En este caso, la finalidad con la que un organismo puede requerir una copia de la cédula de identidad es para verificar de forma certera la identidad de una persona, pero su requerimiento tiene una gran incidencia en el derecho que poseen los titulares a la protección de sus datos personales, en cuanto esta indica su nombre, su fecha de nacimiento, el número de documento de identidad, su firma y una fotografía de su cara. Por lo que la recomendación es efectuar dichas solicitudes sólo en la etapa que sea pertinente, debiendo regularse en las Bases de licitación.

Luego, determinada la finalidad, el organismo debe ponderar el nivel de certeza que necesita respecto de la identidad del oferente al momento de presentar la oferta y al momento de suscribir el contrato, evidenciándose una diferencia, en cuanto el proveedor solo luego de la firma del contrato adquiere los derechos y obligaciones que nacen de este.

De esta forma es dable evaluar la existencia de medios menos invasivos de corroborar la identidad de los oferentes o sus representantes legales para la etapa

de presentación y evaluación de las ofertas, existiendo en este caso la posibilidad de solicitar anexos donde el oferente entregue dichos datos, o utilizar los datos que el propio Sistema de Información posea respecto de estos.

Finalmente, cabe hacer presente que el artículo 58 del Reglamento N° 661 de 2024, establece la posibilidad de readjudicar la licitación cuando el proveedor adjudicado se desistiere de firmar el contrato, o aceptar la orden de compra, o no cumpliese con las demás condiciones y requisitos establecidos en las Bases para la suscripción o aceptación de los referidos documentos, por lo cual, el establecer esta diferencia en los niveles de certeza respecto de la identidad del oferente y del adjudicado, no debiese generar grandes costos administrativos en caso de que el oferente adjudicado se niegue o no pueda verificar su identidad previo a contratar a través de la entrega de la copia de su cedula de identidad, cuya aplicación debiese quedar establecido en la respectiva Base de licitación.

3. **Deber de información.**

De acuerdo con lo dispuesto en los artículos 3°, 4° y 20 de la Ley de Protección de la Vida Privada, los organismos públicos están obligados a informar a su titular acerca de la identidad del órgano responsable de la base de datos, de la finalidad perseguida con el tratamiento de la información, de la posible comunicación a terceros y de los derechos que pueden ser ejercidos por ellos.

Aplicación del principio de información en el tratamiento de datos en contrataciones sometidas a la Ley de Compras Públicas:

En el caso del Sistema de Información o Mercado Público, esto se encuentra descrito en las Políticas y Condiciones de Uso de Mercado Público, las cuales están disponibles el sitio www.chilecompra.cl/terminos-y-condiciones-de-uso, las cuales son dictadas conforme el mandato efectuado por el literal h) del artículo 30 de la Ley de Compras.

4. **Principio de seguridad.**

Conforme a lo establecido en el artículo 11 de la Ley de Protección de la Vida Privada, el responsable de los registros o bases donde se almacenen datos personales, con posterioridad a su recolección, deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños. Por tanto, los organismos del Estado, a fin de dar cumplimiento a lo anterior, deben aplicar medidas de seguridad, técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información. Por lo que se recomienda la definición de flujos en los respectivos manuales de compra respecto al tratamiento de datos personales en el ámbito de las contrataciones públicas.

Asimismo, respecto de la seguridad y confidencialidad de los documentos electrónicos, deben aplicar estrictamente las disposiciones del Decreto Supremo N°83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad de los documentos electrónicos.

Los organismos públicos, además, deben implementar las medidas pertinentes de la Política Nacional de Ciberseguridad, la Norma Técnica de Seguridad de la Información y

Ciberseguridad conforme a la Ley N°21.180 y los Instructivos Presidenciales que imponen medidas específicas sobre ciberseguridad que deben observar los órganos de la administración del Estado.

Aplicación del principio de seguridad en el tratamiento de datos en contrataciones sometidas a la Ley de Compras Públicas:

Sobre este punto, en el ámbito de las compras públicas es especialmente relevante regular el cumplimiento de este principio por los proveedores y los trabajadores de estos que requieran tener acceso al tratamiento de datos para el cumplimiento de la prestación de los servicios contratados por los organismos compradores.

Esto debe ser regulado para el caso de las licitaciones públicas en las bases de licitación y en el caso de los tratos o contrataciones directas en el contrato.

Un ejemplo de cláusulas que regulan la materia son las siguientes:

“Acceso a sistemas

En caso de que el personal del proveedor requiera acceso a los sistemas del organismo para llevar a cabo las prestaciones contratadas, deberá previamente informar a través de su coordinador del contrato a la contraparte del órgano comprador, el nombre y RUT de las personas que accederán, el objeto de actividad, la fecha y lugar, y el tipo de sistemas, información o equipos que requerirá.

Sólo podrán tener acceso a los sistemas aquellas personas autorizadas por la contraparte del órgano contratante, en los términos que ésta determine y se entenderá que existe prohibición de acceso a todo otro sistema, información y equipos que no estén comprendidos en la autorización.

Si el personal del proveedor que recibe la autorización de acceso utiliza equipos propios, deberán singularizarse previamente”.

“Seguridad de la información

El contrato que se celebre en el marco de esta licitación entregará al proveedor acceso a información del organismo comprador o sus sistemas, en consecuencia, es obligación de éste resguardar debidamente esta información y cumplir las demás consideraciones que se establecen en esta cláusula.

El proveedor reconoce que es el único responsable por la confidencialidad y seguridad de la Información del organismo comprador a la que accede, custodia o controla, por lo cual será responsable de tomar las medidas apropiadas de seguridad administrativas, técnicas y físicas, asegurará la confidencialidad, disponibilidad, integridad y seguridad de la Información del organismo.

El proveedor deberá implementar y mantener un programa de seguridad que cumpla con los requisitos de seguridad y privacidad y que incorpore las mejores prácticas de la industria. El programa de seguridad del proveedor deberá incluir las medidas apropiadas de seguridad administrativas, técnicas y físicas, asegurará la confidencialidad, disponibilidad, integridad y seguridad de la Información del organismo comprador y sus sistemas e incluirá

por lo menos las siguientes medidas de seguridad:

- Controles adecuados para la autentificación de usuarios, incluyendo métodos seguros para asignar, seleccionar y almacenar el acceso de credenciales, limitar el acceso sólo a los usuarios activos y bloquear el acceso después de un número intentos de accesos fallidos acorde a las buenas prácticas de seguridad definidos de la industria detallados en los requisitos de seguridad y privacidad.
- Controles de acceso seguro, incluyendo aquellos que limiten el acceso a la Información del organismo para los individuos que tengan una razón fidedigna y demostrable de negocios para acceder a dicha información, respaldados mediante políticas, protocolos y controles apropiados que faciliten la autorización, establecimiento, modificación y eliminación de los accesos.
- Ajustes apropiados y oportunos para el Programa de Seguridad del Proveedor que se basen en: el riesgo periódico de valoraciones; evaluaciones exhaustivas y frecuentes (tales como las valoraciones efectuadas a terceros) de dicho programa; monitoreo y pruebas frecuentes de la efectividad de medidas de seguridad; y revisión de dichas medidas de seguridad con una frecuencia mínima de un año, o cada vez que se presente un cambio sustancial en el ambiente técnico del Proveedor o en las prácticas del negocio que pudieran comprometer la confidencialidad, disponibilidad, integridad o seguridad de los sistemas informáticos del Proveedor.
- Programas de sensibilización y capacitación continua y apropiada de los trabajadores y demás personal que actúe en nombre y representación del adjudicatario para asegurar que se apeguen a las políticas, procedimientos y protocolos del Programa de Seguridad.
- Monitoreo de los sistemas diseñados para garantizar la integridad de la información y prevenir la pérdida o acceso no autorizado a, o la adquisición, utilización y divulgación de la Información del organismo comprador.
- Medidas técnicas de seguridad, incluyendo la protección de firewalls y antivirus, administración de parches de seguridad, registro de accesos a, utilización o divulgación de la Información del organismo comprador, detección de intrusiones y cifrado de los datos estáticos y en tránsito.
- Medidas de seguridad en unidades físicas, incluyendo controles de accesos diseñados para restringir acceso a la Información del organismo comprador para los individuos que se describen en el segundo punto de la presente cláusula.
- Segmentación lógica de la Información del organismo comprador de los datos que pertenezcan a otros clientes.
- Las tareas de mantenimiento de software solicitadas al proveedor deben cumplir con prácticas de desarrollo seguro y arquitectura recomendadas por OWASP o similares.

El proveedor deberá ejercer la supervisión necesaria y apropiada sobre sus empleados y sobre cualquier otro personal que actúe en su representación para mantener la confidencialidad, integridad, disponibilidad y seguridad de la Información del organismo comprador.

El Proveedor deberá cumplir con todos los Requisitos de Seguridad de la Información y Privacidad aplicables.

El Proveedor deberá mantener un nivel de certificaciones o evaluaciones de seguridad que sea consistente con las mejores prácticas, y que se lleve a cabo mediante terceros que a

juicio del organismo comprador estén calificados. Frente a una solicitud fundada del organismo comprador, dichas certificaciones deberán ser entregadas".

"Portabilidad y transferencia de datos

La información del organismo comprador que se clasifique como reservada o confidencial no deberá almacenarse o transportarse en laptops ni en cualquier otro tipo de dispositivo móvil, ni en medios de almacenamiento extraíbles, incluyendo: USB, memorias portátiles, DVD o CD, a menos que dichos dispositivos se cifren utilizando una metodología de cifrado que se apruebe por escrito por el Departamento de Seguridad de la Información o correspondiente del organismo comprador.

Todas las transferencias de datos electrónicos de la información del organismo comprador que se clasifiquen como reservada o confidencial se deberán realizar a través de FTP seguro u otro protocolo o metodología de cifrado que se apruebe por escrito por el Departamento de Seguridad de la Información o correspondiente del organismo comprador.

Cualquier acuerdo de servicio con empresas que subcontraten de Hosting o Cloud que el proveedor use o en el futuro utilice para proveer servicios al organismo comprador, es un servicio de tercero que está sujeto a los lineamientos de las cláusulas de seguridad de la información y la presente cláusula.

Cualquier acuerdo de servicio con empresas que subcontraten, de Hosting o Cloud que sea confiada su ejecución a un proveedor previo a la ejecución del acuerdo, está sujeto a la presente cláusula. Cualquier acuerdo de servicio con empresas que subcontraten de Hosting o Cloud que el proveedor proponga incluir en la siguiente ejecución del contrato está sujeto a la presente cláusula.

De acuerdo con lo previsto en la presente cláusula, no se podrá transferir, almacenar, o procesar la información del organismo comprador fuera del país en donde el Proveedor la recibe sin antes obtener una aprobación por escrito, comprendiéndose las transferencias a agentes o subcontratados".

"Evaluación y revisión seguridad de la información

El Departamento de Seguridad de la Información del organismo comprador deberá llevar a cabo una revisión de seguridad cuando lo considere razonablemente necesario.

A solicitud del organismo comprador, el Proveedor deberá proporcionar las copias de sus políticas de seguridad y privacidad, así como los procedimientos aplicables a la información de éste. Asimismo, el adjudicatario, a solicitud del organismo comprador, también podrá emitir respuestas por escrito a las preguntas relacionadas con las prácticas de seguridad de la información y privacidad que le sean aplicables a la información de este. El proveedor deberá emitir respuestas escritas dentro de los primeros 10 días hábiles siguientes a la fecha de recepción de la solicitud.

El Proveedor deberá proporcionar al Departamento de Seguridad de la Información o al que corresponda del organismo comprador la oportunidad de llevar a cabo una evaluación de seguridad y privacidad del Programa de Seguridad de la información, de los sistemas y los procedimientos de este. El personal del organismo comprador, o los terceros que este contrate, deberán llevar a cabo dicha valoración in-situ, o bien, se deberá realizar mediante

encuestas y entrevistas a discreción del organismo. Dicha evaluación se llevará a cabo sólo una vez por cada año, a no ser que exista algún Incidente de Datos, en cuyo caso la frecuencia será mayor.

Cuando vaya a realizarse una evaluación in-situ, el organismo deberá dar aviso al Proveedor con al menos de 15 días hábiles previos a dicha evaluación, con excepción que exista un Incidente de Datos, o en el caso que el organismo tuviera alguna base razonable para pensar que el Proveedor pudiese no cumplir con los puntos del presente apartado, en cuyo caso dicho aviso no será mayor a 48 horas.

El proveedor deberá notificar oportunamente por escrito al organismo comprador de cualquier incidente de datos, hallazgo, evaluación o revisión de seguridad que puedan impactar adversamente su información o sistemas, realizadas por el proveedor o por un tercero; incluyendo, auditorías, evaluaciones de vulnerabilidad, revisión de códigos y análisis de penetración. El proveedor mantendrá informado oportunamente al organismo comprador de sus esfuerzos de remediación.

Asimismo, debe notificar inmediatamente al coordinador de contrato y a los correos electrónicos que se dispongan sobre cualquier Incidente de Datos. Si bien la notificación inicial podrá darse a manera de resumen, se deberá entregar una notificación extendida por escrito. La notificación deberá comprender con detalle razonable la naturaleza y alcance del Incidente de Datos (Incluyendo una descripción de toda la Información que se ha afectado) y las acciones correctivas que el Proveedor ha tomado. Se deberá suplementar oportunamente dicha notificación con el nivel de detalle razonable que solicite el organismo, incluyendo los reportes de investigaciones o forenses relevantes.

El Proveedor deberá tomar oportunamente todas las acciones correctivas necesarias y sugeridas, y deberá cooperar completamente con el organismo comprador y el personal designado en todos los esfuerzos razonables para investigar el Incidente de Datos, mitigar los efectos adversos, y prevenir la recurrencia. Dicha cooperación deberá incluir la pronta respuesta a las averiguaciones del organismo sobre el incidente de Datos.

Las partes deberán colaborar en caso de que sea necesario o recomendable proporcionar aviso del Incidente de Datos a cualquier persona, entidad gubernamental, los medios de comunicación o cualquier otra parte. Las Partes deberán colaborar con el contenido del aviso. El organismo comprador deberá realizar las determinaciones finales sobre a quién, y si es que se proporcionaran notificaciones, el contenido de la notificación, y a qué parte deberá ser la firmante de dicha notificación".

"Entrega segura o eliminación y terminación de accesos

Una vez que concluya el contrato, el Proveedor deberá regresar la información del organismo comprador que posea, custodie o controle.

No obstante, lo anterior, el Proveedor no podrá eliminar la información del organismo comprador, salvo que esta acción sea acordada con este y en concordancia a la normativa aplicable. Cualquier eliminación de la información del organismo deberá garantizar que dicha información quede permanentemente ilegible e irrecuperable, siempre y cuando el organismo la disponga dentro de sus herramientas internas.

En la medida que el Proveedor tenga acceso o contacto con los sistemas del organismo

comprador, deberá garantizar que dicho acceso cesará en la fecha de terminación del Contrato.

Mediante aviso razonable y a solicitud del organismo comprador, el proveedor deberá proporcionar a éste, las certificaciones de un órgano externo que dé fe del cumplimiento del Proveedor de las cláusulas de Seguridad de la Información y entrega segura o eliminación y terminación de accesos.

5. **Principio de confidencialidad o secreto.**

Según lo prescribe el artículo 7° de la Ley N°19.628 de Protección de la Vida Privada , las personas que trabajan en el tratamiento de datos personales o tengan acceso a éstos de otra forma (como aquellos funcionarios públicos autorizados para el acceso a bancos de datos de los organismos respectivos), están obligadas 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, obligación que no cesa por haber terminado sus actividades en ese campo.

Aplicación del principio de confidencialidad en el tratamiento de datos en contrataciones sometidas a la Ley de Compras Públicas:

Sobre este punto en el ámbito de las compras públicas es especialmente relevante regular el cumplimiento de este principio por los proveedores y los trabajadores de estos que requieran tener acceso al tratamiento de datos para el cumplimiento de la prestación de los servicios contratados por los organismos compradores.

Esto debe ser regulado para el caso de las licitaciones públicas en las bases de licitación y en el caso de los tratos o contrataciones directas en el contrato.

Un ejemplo de cláusulas que regulan la materia son las siguientes:

“Confidencialidad
El Adjudicatario no podrá utilizar para ninguna finalidad ajena a la ejecución de los servicios licitados, los antecedentes y, en general, cualquier información, que haya conocido o a la que haya accedido, en virtud de la ejecución del contrato, o de cualquier actividad relacionada con éste.

El Adjudicatario, así como sus consultores y personal dependiente, que de una u otra manera se hayan vinculado a la ejecución de los servicios licitados, en cualquiera de sus etapas, deben guardar confidencialidad sobre los antecedentes vinculados con el desarrollo de dichos servicios. Para ello se le solicitará suscribir declaraciones con compromisos de confidencialidad.

La responsabilidad del respectivo Adjudicatario en este ámbito será solidaria respecto de la de sus administradores, representantes, personeros, empleados, o consultores.

El Adjudicatario debe dar garantías respecto al resguardo de la confidencialidad de la información, reservándose el organismo comprador el derecho de ejercer las acciones legales que correspondan, de acuerdo con las normas legales vigentes.

La divulgación, por cualquier medio, de la totalidad o parte de la información referida en los párrafos anteriores, por parte del Adjudicatario, durante la vigencia del contrato o una vez finalizado éste, dará pie a que el organismo comprador entable en su contra las acciones judiciales que correspondan, sin perjuicio de la responsabilidad solidaria por los actos en infracción de esta obligación que hayan ejecutado sus empleados.

Se deja constancia que, en el contrato a suscribir, el equipo consultor del adjudicatario deberá firmar un acuerdo de confidencialidad con la finalidad de resguardar lo anteriormente señalado".

"Tratamiento de datos personales por mandato

En caso de que se encomiende al adjudicatario el tratamiento de datos personales por cuenta del organismo comprador, ésta deberá suscribir un contrato de mandato escrito con el proveedor, en donde se especifiquen las condiciones bajo las cuales se podrán utilizar esos datos, según el artículo 8 de la Ley N°19.628, sobre Protección de la Vida Privada. En dicho contrato de mandato se indicará, a lo menos, la finalidad del tratamiento, el tipo de datos que se entrega al adjudicatario (en calidad de mandatario), la duración del encargo y un procedimiento para la devolución de los datos y su eliminación efectiva por parte del proveedor, al terminar ese contrato. Además, deberá prohibir expresamente el uso de dichos datos personales para fines distintos a los que persigue el organismo comprador (en calidad de órgano público mandante) y señalar expresamente que no se permite su comunicación a terceros".

6. **Deber de protección especial de los datos personales sensibles.**

Conforme prescribe el artículo 10 de la Ley N° 19.628 de Protección de la Vida Privada, 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.

De esta manera, únicamente los organismos de la Administración del Estado que cumplan con alguna de esas condiciones expresas podrán realizar tratamiento de datos personales sensibles, sobre los cuales deberán adoptar medidas de seguridad adecuadas al nivel de sensibilidad y riesgo de los datos tratados.

Aplicación del deber de protección especial de los datos personales sensibles en el tratamiento de datos en contrataciones sometidas a la Ley de Compras Públicas:

En este sentido, es deber del organismo comprador resguardar los datos sensibles que posea y revisar previamente a la publicación de algún documento en el Sistema de Información que este no los contenga.

Sin perjuicio de los derechos que asisten al titular de los datos, el organismo comprador que por error publique documentos sensibles en el Sistema de Información debe oficiar a la

Dirección ChileCompra solicitando la eliminación de estos con el sustento normativo correspondiente.

7. **Actualización legal en materia de tratamiento de datos personales**

Por último, cabe señalar que, al momento de aprobación de la presente directiva, se debe considerar la publicación en el Diario Oficial de la Ley N° 21.719 que regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales.

Respecto al objeto de la Ley, por un lado, regula la forma y condiciones en las que se realiza el tratamiento de datos personales y mejora la protección de los derechos de sus titulares, elevando el estándar de protección a los derechos de las personas. Con esto, el estándar chileno se homologa al establecido por el Reglamento General de Protección de Datos de la Unión Europea, erigido como la referencia internacional para la protección de los derechos de las personas y sus datos personales. Y, por otro lado, crea la Agencia de Protección de Datos Personales, la cual se trata de una corporación autónoma de derecho público, de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio, que se relacionará con el Presidente de la República a través del Ministerio de Economía, Fomento y Turismo, cuyo objetivo será velar por la efectiva protección de los derechos establecidos en las disposiciones legales y aplicar las sanciones correspondientes.

Con todo, es importante destacar, que dicha normativa entrará en vigencia en los 24 meses posterior a su publicación en el Diario Oficial, es decir, a contar del 1 de diciembre de 2026, por lo que los organismos del Estado, durante dicho periodo, deberán adaptarse a las nuevas disposiciones, las que contemplan importantes modificaciones a las leyes N° 19.628, sobre protección de la vida privada; N° 20.285, sobre acceso a la información pública, y N° 19.496, que establece normas sobre protección de los derechos de los consumidores.

2. **PUBLÍQUESE** la presente resolución en el Sistema de Información www.mercadopublico.cl

Anótese, Regístrese y Comuníquese,

VERÓNICA VALLE SARAH
DIRECTORA
DIRECCIÓN DE COMPRAS Y CONTRATACIÓN PÚBLICA

REQ-03927
VPC/BMC/CPC/VMH/PMS/JMC/DRM/PJR/CCV/LHP
Distribución:
- Dirección
- Fiscalía
- División de Gestión de Usuarios
- Departamento de Gestión y Participación de Proveedores
- Departamento de Gestión y Asesoría de Organismos Compradores
- División de Compras Públicas
- Departamento de Observatorio
- Departamento de Seguridad de la Información y Ciberseguridad
- Departamento de Comunicaciones y Participación Ciudadana

Firmado electrónicamente por:
Verónica Valle
DIRECTORA DCCP
Fecha: 6-2-2025 - 19:17:8