

**Resolución Exenta N° E484 / 21-10-2026**

El folio ha sido generado electrónicamente.

APRUEBA REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES DEL CONSEJO PARA LA TRANSPARENCIA Y DEROGA LAS RESOLUCIONES EXENTAS QUE INDICA.**VISTOS:**

Lo dispuesto en la Constitución Política de la República; en la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la Ley N°20.285, sobre acceso a la información pública, en adelante, Ley de Transparencia; en el Decreto Supremo N°20, de 2009, del Ministerio Secretaría General de la Presidencia, que aprueba los Estatutos de Funcionamiento del Consejo para la Transparencia, especialmente, su artículo 22; en la Ley N°19.628, sobre protección de la vida privada; en 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, en adelante Ley N°21.719; en el Decreto con Fuerza de Ley N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; 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°21.180, de Transformación Digital del Estado; en el Decreto con Fuerza de Ley N°1, de 2020, del Ministerio Secretaría General de la Presidencia, que establece normas de aplicación del artículo 1° de la Ley N°21.180; en la Ley N°21.663, Ley Marco de Ciberseguridad; en la Ley N°21.459, que establece normas sobre delitos informáticos; en la Ley N°19.886, de bases sobre contratos administrativos de suministro y prestación de servicios; en la Ley N°20.609, que establece medidas contra la discriminación; en el Decreto N°13, de 2009, del Ministerio Secretaría General de la Presidencia que establece el reglamento de la Ley de Transparencia; en la Resolución Exenta N°151, de 10 de julio de 2020, del Consejo, que aprueba el reglamento sobre grabación y procedimiento de acceso, resguardo y conservación de la grabación de las sesiones del Consejo Directivo; en la Resolución Exenta N°304, de 30 de noviembre de 2020, del Consejo, que aprueba el texto actualizado y refundido de las recomendaciones del Consejo para la Transparencia sobre protección de datos

personales por parte de los órganos de la Administración del Estado; en el acuerdo del Consejo Directivo adoptado en Sesión Ordinaria N°1.375, de 25 de julio de 2023; y, en la Resolución Exenta N°139, de 17 de junio de 2021, del Consejo, que Aprueba Anexo de contrato de trabajo suscrito con don David Ibaceta Medina, nombrándolo Director General de esta Corporación.

CONSIDERANDO:

I. MARCO CONSTITUCIONAL Y LEGAL DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

1º) Que, el numeral 4 del artículo 19 de la Constitución Política de la República asegura a todas las personas el respeto y protección a la vida privada y a sus datos personales, y establece que el tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.

2º) Que, conforme al inciso segundo del artículo 5º de la Constitución Política de la República, el Consejo tiene el deber de respetar y promover los derechos esenciales que emanan de la naturaleza humana, garantizados en la Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes.

3º) Que, con fecha 13 de diciembre de 2024, se publicó en el Diario Oficial 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, la cual modifica de manera sustantiva la Ley N°19.628, elevando el estándar de protección de datos personales en Chile, y estableciendo reglas generales para su tratamiento por parte de los órganos públicos y privados. Entre dichas modificaciones se sustituyó el nombre de la Ley N°19.628 por el de “sobre protección de los datos personales” y se reemplazaron o modificaron sus títulos.

4º) Que, la Ley N°21.719, y las modificaciones que ella introduce a la Ley N°19.628, entrarán en vigencia conforme los términos de su artículo primero transitorio.

II. EL CONSEJO PARA LA TRANSPARENCIA EN SU CALIDAD DE RESPONSABLE DE DATOS PERSONALES

5º) Que, el Consejo para la Transparencia, en adelante Consejo, ha sido creado por la Ley de Transparencia como una corporación autónoma de derecho público con personalidad jurídica y patrimonio propio, que tiene por objeto promover la

transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del Estado, y garantizar el derecho de acceso a la información.

6º) Que, en ejercicio de sus competencias y en cumplimiento de sus obligaciones legales, el Consejo actúa como responsable de datos personales cuyos titulares son múltiples, incluyendo, entre otros, a las personas trabajadoras del CPLT, a los enlaces de transparencia de las diversas reparticiones públicas, y a aquellos ciudadanos que se han relacionado con el Consejo, ya sea formulando consultas, participando en seminarios o capacitaciones, ejerciendo su derecho de acceso a la información pública, solicitando amparo a su derecho de acceso a la información pública, o interponiendo reclamos respecto de incumplimientos a deberes de transparencia activa; tratamientos que se fundan principalmente en el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias.

7º) Que, conforme al artículo 20 de la LPDP, es lícito el tratamiento de datos personales que efectúan los órganos públicos cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y con arreglo a las disposiciones de su Título IV, actuando en tal caso como responsables de datos y sin requerir el consentimiento del titular, de modo que ésta constituye la base de licitud general de los tratamientos del Consejo, sin perjuicio de las bases específicas que la ley contemple para casos determinados.

8º) Que, el artículo 21 de la LPDP determina las normas que resultan aplicables al tratamiento de datos que efectúan los órganos públicos, entre ellas los deberes de los artículos 14 y siguientes, las normas sobre transferencia internacional del Título V y el régimen de infracciones y sanciones del Título VII, así como los artículos 4º a 8º, en conformidad a lo dispuesto en el artículo 23.

9º) Que, por su parte, el artículo segundo de la Ley N°21.719 suprimió el literal m) del artículo 33 de la Ley de Transparencia, de manera que, a contar de la entrada en vigencia de dicha ley, las atribuciones que el Consejo ejercía en materia de protección de datos personales respecto de los órganos de la Administración del Estado corresponderán a la Agencia de Protección de Datos Personales, quedando el Consejo sujeto a la fiscalización de aquélla en su calidad de responsable de datos; circunstancia que, además, priva de sustento a las recomendaciones dirigidas a otros órganos aprobadas por la Resolución Exenta N°304, de 30 de noviembre de 2020, cuya derogación se dispone.

III. PRINCIPIOS Y DEBERES QUE RIGEN AL CONSEJO COMO RESPONSABLE

10º) Que, la Ley N°21.719 dispone para los responsables de datos que sean organismos públicos la observancia de los principios de licitud y lealtad; de

finalidad; de proporcionalidad; de calidad; de responsabilidad; de seguridad; de confidencialidad; de transparencia e información; y los principios generales que rigen la Administración del Estado, especialmente los de coordinación, probidad y eficiencia.

11º) Que, en particular, respecto del principio de transparencia e información, se requiere a los responsables la entrega al titular de toda la información que sea necesaria para el ejercicio de los derechos que establece la ley, incluyendo las políticas y prácticas sobre el tratamiento de los datos personales, las que además deberán encontrarse permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita, debiendo el responsable adoptar las medidas adecuadas y oportunas para facilitar al titular el acceso a toda la información que se señala en la ley, así como cualquier otra comunicación relativa al tratamiento que realiza.

12º) Que, los responsables, además, deben dar cumplimiento a una serie de obligaciones en pos de la protección de datos personales, tales como el deber de secreto o confidencialidad del artículo 14 bis; el de información y transparencia del artículo 14 ter, que exige facilitar y mantener permanentemente a disposición del público, en su sitio web o en cualquier otro medio equivalente, la política de tratamiento adoptada, con su fecha y versión, y el medio a través del cual se le notifican las solicitudes de los titulares; el de protección desde el diseño y por defecto del artículo 14 quáter; el de adoptar medidas de seguridad del artículo 14 quinquies; el de reportar las vulneraciones a las medidas de seguridad del artículo 14 sexies; y el relativo al tratamiento de datos a través de un tercero mandatario o encargado del artículo 15 bis.

13º) Que, el tratamiento de datos personales sensibles exige resguardos reforzados, atendido que su divulgación o uso indebido puede dar lugar a actos de discriminación arbitraria de aquellos que sanciona la Ley N°20.609; resguardo reforzado que también debe observarse respecto de los datos de niños, niñas y adolescentes, y de los datos relativos a infracciones penales, civiles, administrativas y disciplinarias.

IV. PREVENCIÓN DE INFRACCIONES Y RÉGIMEN DE RESPONSABILIDAD

14º) Que, los responsables de datos sean personas naturales o jurídicas, públicas o privadas, tienen la obligación de adoptar acciones destinadas a prevenir la comisión de las infracciones establecidas en los artículos 34 bis, 34 ter y 34 quáter del nuevo texto de la Ley N°19.628, conforme lo dispone su artículo 48.

15º) Que, por su parte, la LPDP consagra en su artículo 49 un modelo de prevención de infracciones que los responsables de datos podrán voluntariamente adoptar y que consiste en un programa de cumplimiento que deberá contener, entre otros, los

siguientes elementos: la designación de un delegado de protección de datos personales y la definición de sus medios y facultades; el establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades o procesos de la entidad en cuyo contexto se genere o incremente el riesgo de infracción, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de dichas infracciones; mecanismos de reporte interno y de reporte a la autoridad de protección de datos para el caso de vulneraciones a medidas de seguridad; y la existencia de sanciones administrativas internas, así como de procedimientos de denuncia o castigo de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.

16º) Que, conforme indica la Ley N°21.719, “la regulación interna a que dé lugar la implementación del programa, en su caso, deberá ser incorporada expresamente como una obligación en los contratos de trabajo o de prestación de servicios de todos los trabajadores, empleados y prestadores de servicios de las entidades que actúen como responsables de datos o los terceros que efectúen el tratamiento, incluidos los máximos ejecutivos de ellas, o bien, como una obligación del reglamento interno del que tratan los artículos 153 y siguientes del Código del Trabajo. En este último caso, se deben realizar las medidas de publicidad establecidas en el artículo 156 del mismo Código”.

17º) Que, tratándose de órganos públicos, las infracciones a los principios, derechos y obligaciones de la LPDP son determinadas por la Agencia y sancionadas, conforme al artículo 44 de dicha ley, con multa de veinte a cincuenta por ciento de la remuneración mensual del jefe superior del servicio infractor, sin perjuicio de la responsabilidad del funcionario infractor que establece su artículo 45; lo que refuerza la necesidad de contar con reglas internas claras, verificables y conocidas por todos los obligados.

V. SOPORTE DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

18º) Que, por su parte, la Ley N°19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado, reformada por la Ley N°21.180, dispone, entre los principios del procedimiento, aquellos aplicables a la tramitación de procedimientos administrativos por medios electrónicos, incluyendo los de neutralidad tecnológica, de actualización, de equivalencia funcional, de fidelidad, de interoperabilidad y de cooperación.

19º) Que, asimismo, el resguardo de los datos personales que trata el Consejo debe articularse con las obligaciones que le impone la Ley N°21.663, Ley Marco de Ciberseguridad, y con la normativa interna sobre seguridad de la información y gestión de incidentes, sin perjuicio de las responsabilidades que puedan derivar de la Ley N°21.459, que establece normas sobre delitos informáticos.

VI. NECESIDAD DEL REGLAMENTO Y SU RELACIÓN CON EL PROCEDIMIENTO DE EJERCICIO DE DERECHOS

20º) Que, por lo anteriormente expuesto, y sin perjuicio de que el Consejo ya ha regulado desde su inicio distintos aspectos internos sobre el adecuado tratamiento de datos en el marco de su quehacer institucional, ha estimado necesario contar con un Reglamento de Protección de Datos Personales con el objeto de fijar las reglas, principios, roles y responsabilidades, reportes, mecanismos sancionatorios, y, en general, pautas comunes y obligatorias en virtud de las cuales se realizará el tratamiento de datos personales a su interior, de forma de habilitar el cumplimiento de sus funciones legales y dar cumplimiento a la normativa sobre protección de datos aplicable, resguardando así este derecho fundamental respecto de todas las personas con que se relacione.

21º) Que, en forma coetánea, el Consejo ha aprobado el Procedimiento de tramitación de solicitudes de ejercicio de derechos de los titulares de datos personales ante el Consejo para la Transparencia, de modo que ambos instrumentos conforman un cuerpo normativo interno único y coherente: el Reglamento fija el marco general de gobernanza, principios, roles, seguridad, cesiones, conservación y responsabilidad, mientras que el Procedimiento regula específicamente la recepción, tramitación y resolución de las solicitudes de los titulares, rigiendo preferentemente en ese ámbito y aplicándose el Reglamento en forma supletoria.

VII. POTESTAD DEL DIRECTOR GENERAL PARA APROBAR EL REGLAMENTO

22º) Que, conforme al artículo 42 de la Ley de Transparencia y al artículo 22 de los Estatutos de Funcionamiento del Consejo, el Director General es el representante legal de la Corporación y le corresponde, entre otras funciones, planificar, organizar, dirigir y coordinar su funcionamiento, así como poner en ejecución los acuerdos adoptados por el Consejo Directivo, cumplirlos y hacerlos cumplir, en su calidad de autoridad ejecutiva.

23º) Que, en ejercicio de dichas atribuciones, el Consejo Directivo, en Sesión Ordinaria N°1.375, de 25 de julio de 2023, acordó que las decisiones referidas a la planificación, organización, administración, dirección y coordinación de esta Corporación, que permitan su funcionamiento, tanto en el ámbito administrativo, de gestión, de personas y de procesos internos, son de competencia exclusiva del Director General en conformidad a lo establecido en el artículo 42 de la Ley de Transparencia, por lo que, no deberán ser sometidas a decisión del Consejo Directivo y sólo serán reportadas a este, de forma periódica, para su conocimiento.

24º) Que, el Reglamento que por este acto se aprueba constituye un instrumento de gestión interna destinado a ordenar la organización y los procesos internos de la

Corporación en materia de protección de datos personales, distribuyendo tareas entre sus direcciones y unidades, por lo que se encuentra comprendido en el ámbito de competencia exclusiva a que se refiere el considerando anterior, sin perjuicio de su reporte al Consejo Directivo para su conocimiento.

VIII. VIGENCIA Y DEROGACIONES

25º) Que, finalmente, a fin de que el Consejo cuente con un marco interno ajustado a la nueva legislación desde el momento mismo en que ésta comience a regir, y de evitar vacíos normativos durante el período intermedio, resulta pertinente fijar la entrada en vigencia del Reglamento y la derogación de los instrumentos que reemplaza, estableciendo las reglas transitorias que correspondan.

RESUELVO:

ARTÍCULO PRIMERO: APRUÉBESE Y FÍJESE, el Reglamento de Protección de Datos Personales del Consejo para la Transparencia, cuyo texto es el siguiente:

“REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES DEL CONSEJO PARA LA TRANSPARENCIA

ÍNDICE

TÍTULO I. DISPOSICIONES GENERALES (Artículos 1º a 5º)

Párrafo 1º. Visión, objetivo y ámbito del Reglamento. (Artículos 1º a 3º)

Párrafo 2º. Siglas y marco normativo. (Artículos 4º y 5º)

TÍTULO II. PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES EN EL CPLT (Artículos 6º a 15)

TÍTULO III. ROLES, RESPONSABILIDADES Y MEDIDAS DE CUMPLIMIENTO (Artículos 16 a 29)

Párrafo 1º. Gobernanza y Grupo de Protección de Datos Personales del CPLT. (Artículos 16 y 17)

Párrafo 2º. Delegado de Protección de Datos Personales del CPLT. (Artículos 18 a 21)

Párrafo 3°. Roles y responsabilidades. (Artículo 22)

Párrafo 4°. Recolección e identificación de datos personales en el CPLT. (Artículos 23 y 24)

Párrafo 5°. Registro de actividades de tratamiento de datos del CPLT. (Artículos 25 y 26)

Párrafo 6°. Protección desde el diseño y gestión de riesgos. (Artículos 27 a 29)

TÍTULO IV. TRANSPARENCIA E INFORMACIÓN (Artículos 30 a 35)

TÍTULO V. DERECHOS DEL TITULAR DE DATOS PERSONALES ANTE EL CPLT (Artículos 36 a 42)

TÍTULO VI. MEDIDAS DE SEGURIDAD Y CONFIDENCIALIDAD DE LOS DATOS PERSONALES (Artículos 43 a 60)

Párrafo 1°. Aspectos generales. (Artículos 43 a 49)

Párrafo 2°. Detección y manejo de incidentes. (Artículos 50 a 54)

Párrafo 3°. Uso de herramientas tecnológicas. (Artículos 55 a 57)

Párrafo 4°. Confidencialidad de los datos personales. (Artículos 58 a 60)

TÍTULO VII. CESIONES Y COMUNICACIONES DE DATOS PERSONALES (Artículos 61 a 83)

Párrafo 1°. Mandatarios del tratamiento de datos personales. (Artículos 61 a 67)

Párrafo 2°. Comunicación o cesión de datos personales por parte del CPLT. (Artículos 68 a 72)

Párrafo 3°. Datos personales en el contexto de instituciones de la Ley de Transparencia. (Artículos 73 a 75)

Párrafo 4°. Datos relativos a infracciones penales, civiles, administrativas y disciplinarias. (Artículos 76 y 77)

Párrafo 5°. Transferencias internacionales de datos personales. (Artículos 78 a 80)

Párrafo 6°. Transferencia o cesión de datos personales hacia el CPLT. (Artículos 81 a 83)

TÍTULO VIII. CONSERVACIÓN O RETENCIÓN DE DATOS PERSONALES (Artículos 84 a 86)

TÍTULO IX. CAPACITACIÓN Y CONCIENTIZACIÓN (Artículos 87 a 89)

TÍTULO X. SUPERVISIÓN DEL REGLAMENTO, REPORTES E INFRACCIONES (Artículos 90 a 101)

TÍTULO XI. DISPOSICIONES FINALES (Artículos 101 a 107)



DISPOSICIONES TRANSITORIAS (Artículos primero a tercero transitorios)

ANEXO I GLOSARIO DE SIGLAS Y DEFINICIONES

ANEXO II MARCO NORMATIVO

ANEXO III CATÁLOGO DE CONTROLES

ANEXO IV GUÍA DE USO DE FOTOGRAFÍAS Y VIDEOS EN ACTIVIDADES DEL
CPLT

TÍTULO I. DISPOSICIONES GENERALES

Párrafo 1°. Visión, objetivo y ámbito del Reglamento

Artículo 1°. Visión. El Consejo para la Transparencia, en adelante e indistintamente CPLT, reconoce la necesidad de tratar, como responsable, datos personales de diversos titulares para ejercer sus funciones legales, así como la relevancia del adecuado tratamiento de dichos datos bajo una óptica de respeto y promoción de los derechos fundamentales, comprometiéndose, por tanto, en el tratamiento de datos de acuerdo con prácticas y estándares apegados a la ley.

Artículo 2°. Objetivo del Reglamento. Este Reglamento fija las reglas y principios en virtud de los cuales se realizará el tratamiento de datos personales al interior del CPLT, de forma de habilitar el cumplimiento de sus funciones legales y de la normativa sobre protección de datos personales que le es aplicable, y de propender a la actuación coordinada con otros instrumentos internos relacionados, como los de ciberseguridad y seguridad de la información.

Artículo 3°. Ámbito de aplicación. Este Reglamento es obligatorio para todas las personas trabajadoras del CPLT, directivos, jefaturas, Consejeros del Consejo Directivo, honorarios, pasantes, practicantes, mandatarios y submandatarios del tratamiento, y cualquiera que realice funciones en nombre del CPLT, y que se vincule con el tratamiento de datos personales que el CPLT trata como responsable.

También es obligatorio para entidades externas con las que exista comunicación o cesión de datos personales, interoperabilidad o convenios de colaboración, en lo que resulte aplicable conforme las disposiciones que defina el CPLT.

Comprende los datos personales en formato físico o electrónico, en infraestructura local o de terceros, y tratados en las oficinas del CPLT o fuera de ellas.

Párrafo 2°. Siglas y marco normativo

Artículo 4°. Siglas y definiciones. Para los efectos de este Reglamento, las expresiones y siglas utilizadas tendrán el significado señalado en el Anexo N°1 “Glosario de siglas y definiciones”. Dichas definiciones se aplicarán también al Procedimiento de tramitación de solicitudes de ejercicio de derechos de los titulares de datos personales ante el Consejo para la Transparencia, en todo aquello que éste no defina de modo específico.

Artículo 5°. Marco normativo. El marco normativo relevante en el contexto del tratamiento de datos personales del CPLT está detallado en el Anexo N°2 “Marco normativo”, el cual se indica de modo referencial y que se entenderá actualizado de pleno derecho según se vaya modificando el panorama normativo en la materia.

TÍTULO II.

PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES EN EL CPLT

Artículo 6°. Principios que regulan el tratamiento de datos en el CPLT. El tratamiento de datos personales en el CPLT se sujetará a los principios de licitud y lealtad, finalidad, proporcionalidad, calidad, responsabilidad, seguridad, transparencia e información, confidencialidad y los principios generales que rigen a la Administración del Estado.

Estos se aplicarán en todo tratamiento, incluyendo procesos internos y sus procedimientos, la prestación de servicios, los contratos y obligaciones que formalice, y el desarrollo e implementación de plataformas.

Artículo 7°. Principio de licitud y lealtad: El CPLT tratará los datos personales de manera lícita y leal. Su base de licitud general es el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias, conforme al artículo 20 de la LPDP, caso en el cual no se requiere el consentimiento del titular. Excepcionalmente, y sólo en los casos en que la ley lo prevea, el tratamiento podrá ampararse en alguna de las siguientes bases, que estarán expresadas en el RAT:

- a) El cumplimiento de una obligación legal que resulte aplicable al CPLT, como en el caso de las obligaciones laborales, previsionales o tributarias.
- b) La celebración o ejecución de un contrato en que el titular sea parte, o la ejecución de medidas precontractuales adoptadas a solicitud de éste.
- c) Fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, y otras hipótesis en los términos del artículo 16 bis, literal e), de la LPDP.
- d) El consentimiento del titular, en los casos en que la LPDP lo exija o lo admita, como ocurre en las hipótesis del inciso cuarto del artículo 22 de la LPDP. El consentimiento será obtenido bajo los requisitos que señala la LPDP, y de manera escrita, sea en papel o de forma electrónica, debiendo mantenerse registro del otorgamiento.
- e) El tratamiento con fines históricos, estadísticos, científicos o de estudios o investigaciones que atiendan fines de interés público, en los términos del artículo 16 quinquies de la LPDP.

Está prohibido el tratamiento de datos que exceda el ámbito de competencia asignado al CPLT o el conferido por las normas habilitantes. Si no se ha identificado previamente una base habilitante entonces no se debe proceder a la recolección y tratamiento de los datos personales.

El tratamiento no debe realizarse mediante medios engañosos, que induzcan a error al titular o que no sea consistente con sus expectativas razonables.

El tratamiento de datos de NNA se realizará atendiendo a su interés superior y al respeto de su autonomía progresiva.

Artículo 8°. Principio de finalidad: El CPLT recolectará datos personales con fines específicos, explícitos y lícitos relacionados con el cumplimiento de sus funciones legales dentro de sus competencias, o con el cumplimiento de la ley, y el tratamiento se enmarcará únicamente en el cumplimiento de dichos fines. Las finalidades estarán indicadas en el RAT. El CPLT no tratará los datos para fines distintos a los informados en la recolección, salvo cuando:

- a) El tratamiento sea para fines compatibles con los autorizados originalmente;
- b) Exista una relación contractual o precontractual entre el titular y el CPLT que justifique el tratamiento con una finalidad distinta, siempre que se enmarque en los fines del contrato o sea coherente con las tratativas o negociaciones previas a la celebración del mismo;
- c) El titular otorgue nuevamente su consentimiento; o
- d) Lo disponga la Ley de Transparencia u otra norma legal.

Artículo 9°. Principio de proporcionalidad: Si el objetivo se puede obtener sin el tratamiento de datos personales o con una cantidad menor de ellos, no deberá efectuarse dicho tratamiento en el CPLT o deberá ajustarse en consecuencia.

El CPLT sólo recolectará y tratará aquellos datos personales que sean necesarios, adecuados y pertinentes para el cumplimiento de sus funciones legales, dentro del ámbito de su competencia, o de una obligación legal, lo cual aplicará, por ejemplo, en formularios, registros, solicitudes de datos, etc.

El CPLT conservará los datos personales sólo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento, luego de lo cual serán suprimidos o anonimizados, sin perjuicio de las excepciones que establezca la ley. La implementación de esta regla se detalla en el Título VIII de este Reglamento.

Artículo 10. Principio de calidad: El CPLT tomará medidas para que los datos personales tratados y comunicados sean exactos, suficientes, completos, actuales y pertinentes en relación con su proveniencia y los fines del tratamiento. Ello implica adoptar medidas para suprimir o rectificar los datos inexactos o desactualizados, y permitir el ejercicio de los derechos de rectificación y supresión, cuando sea procedente.

Artículo 11. Principio de responsabilidad: El CPLT será responsable del cumplimiento de los principios indicados que regulan el tratamiento y de las obligaciones que señala la LPDP.

Las unidades orgánicas del CPLT serán responsables de las actividades de tratamiento de datos que realicen en el ejercicio de sus funciones y de las bases de datos personales que utilizan en dicho contexto, cualquiera sea la plataforma en que estén alojadas; esto, con independencia de las responsabilidades técnicas que la DDD pudiese tener.

Cada obligado por este Reglamento es responsable de la protección de datos personales en el CPLT conforme sus disposiciones.

La implementación de este principio se detalla en los Títulos III y X de este Reglamento.

Artículo 12. Principio de seguridad: El CPLT garantizará estándares adecuados de seguridad, protegiendo los datos personales contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad, que deberán ser observadas por los obligados por este Reglamento, serán acordes con el tratamiento y con la naturaleza de los datos.

La implementación de este principio se detalla en el Título VI de este Reglamento.

Artículo 13. Principio de transparencia e información: El CPLT proporcionará información clara, precisa, gratuita e inequívoca a los titulares sobre el tratamiento de sus datos personales según señala la LPDP, la que estará permanentemente accesible y a disposición de los titulares y que incluirá toda la información necesaria para que puedan ejercer sus derechos, y sobre sus políticas y prácticas.

El CPLT adoptará medidas adecuadas y oportunas para facilitar al titular el acceso a esta información.

La implementación de este principio se detalla en el Título IV de este Reglamento.

Artículo 14. Principio de confidencialidad: El CPLT y todos los obligados por este Reglamento deben guardar secreto o confidencialidad acerca de los datos personales que se traten. Se establecerán controles y medidas adecuadas para ello que serán de carácter obligatorio.

Artículo 15. Principios generales que rigen la Administración del Estado: El tratamiento de datos del CPLT también se sujetará a los principios generales que rigen la Administración del Estado, tales como los de coordinación; probidad; eficiencia; eficacia; responsabilidad; impulsión de oficio del procedimiento; de impugnabilidad de los actos; de control; transparencia y publicidad administrativas; y participación ciudadana.

TÍTULO III.

ROLES, RESPONSABILIDADES Y MEDIDAS DE CUMPLIMIENTO

Párrafo 1°. Gobernanza y Grupo de Protección de Datos Personales del CPLT

Artículo 16. Gobernanza de la Protección de Datos Personales. La gobernanza de la protección de datos personales en el CPLT se estructura en tres niveles:

- a) Un nivel estratégico compuesto por el Director General y el Grupo de PDP.
- b) Un nivel de supervisión y control, compuesto por el DPD, el Auditor Interno y la UECG. A este nivel también contribuyen las jefaturas del CPLT respecto de sus unidades orgánicas.
- c) Un nivel operativo, compuesto por las unidades orgánicas del CPLT que ejecutan las actividades de tratamiento de datos personales en el marco de sus funciones.

Artículo 17. Grupo de Protección de Datos Personales. Habrá en el CPLT un grupo compuesto por los directores del CPLT, los jefes de la UECG y del ADGP, y el DPD. Esto, sin perjuicio que puedan ser convocados por el Director General otras personas trabajadoras del CPLT. Este grupo tiene por objeto:

- a) Adoptar definiciones de alto nivel respecto de la protección de datos personales, velando por la coherencia con las funciones legales del CPLT.
- b) Promover el cumplimiento de este Reglamento y los demás instrumentos internos de protección de datos en el CPLT, e impulsar una cultura de protección de datos personales.
- c) Revisar y coordinar aspectos estratégicos asociados a la LPDP en el CPLT, y los planes, programas de cumplimiento, políticas y procedimientos que se definan o según sea propuesto por el DPD.
- d) Revisar y validar los análisis de riesgos vinculados con el cumplimiento de la LPDP, y acordar las acciones para la gestión y seguimiento.
- e) Facilitar la coordinación entre las unidades orgánicas del CPLT en materia de protección de datos personales.

En caso de que el Grupo de PDP tome decisiones respecto de medios y fines del tratamiento, el DPD se abstendrá de votar en dicha decisión.

Párrafo 2°. Delegado de Protección de Datos Personales del CPLT

Artículo 18. Aspectos orgánicos. El CPLT incluirá en su estructura orgánica un DPD, que corresponderá a una persona de la dotación vigente nombrada por el Director General y que dependerá directamente de él. Este reunirá los requisitos de idoneidad, capacidad y conocimientos específicos.

En caso de ausencia, subrogará temporalmente al DPD quien sea definido por el Director General.

Artículo 19. Autonomía e independencia del DPD. En el desempeño de sus funciones, el DPD actuará con autonomía e independencia. Dicha independencia se garantizará:

- a) Permitiéndole efectuar tareas de supervisión, teniendo acceso a los datos personales tratados y las operaciones de tratamiento, y pudiendo requerir información y colaboración de las unidades del Consejo;
- b) No dándole instrucciones sobre la forma de ejercer sus funciones, ni tampoco siendo sancionado por dicho ejercicio;
- c) No encomendándole funciones que impliquen un conflicto de interés con las funciones propias del cargo de DPD, como aquellas relacionadas con la definición de fines y medios del tratamiento;
- d) Otorgándole acceso y capacidad de reporte directo al Director General y al Consejo Directivo; y
- e) No representando al CPLT ante las autoridades administrativas o los tribunales de justicia para efectos de su defensa administrativa o judicial, lo cual deja a salvo su función colaboradora en los términos del literal h), del artículo 50, de la LPDP.

Artículo 20. Funciones y reporte del DPD. El DPD tendrá las funciones que señala el artículo 50 de la LPDP, el párrafo sobre Roles y responsabilidades de este Título y el Reglamento orgánico del CPLT. El DPD podrá realizar otras funciones en el Consejo, debiendo evitar cualquier conflicto de interés.

El DPD reportará al Director General y al Consejo Directivo del Consejo de manera periódica.

Artículo 21. Medios del DPD. El CPLT dispondrá de recursos y medios suficientes al DPD para el ejercicio de sus funciones y garantizar su independencia, entre las que se considerará, según capacidad presupuestaria, recursos humanos, tecnología, como sistemas informáticos para apoyar el cumplimiento de la LPDP, y acceso a especialización continua.

Párrafo 3°. Roles y responsabilidades

Artículo 22. Roles y responsabilidades. Se establecerán los siguientes roles y responsabilidades en el CPLT:

1. Directores del Consejo para la Transparencia:

- a) Asegurar y supervisar que, en su respectiva dirección, el tratamiento de datos personales se realice en cumplimiento de la LPDP y de este Reglamento, adoptando medidas correctivas cuando corresponda.
- b) Fomentar la capacitación y concientización de la protección de datos personales en el CPLT, transmitiendo a sus equipos las orientaciones e instrucciones necesarias para ello.

- c) Colaborar con las acciones requeridas frente a una vulneración a medidas de seguridad conforme el procedimiento dictado al efecto.
- d) Colaborar con el DPD para el cumplimiento de la LPDP y de este Reglamento, facilitándole la información que les sea solicitada para ello.

2. Dirección General:

- a) Aprobar los recursos necesarios para la implementación y cumplimiento de este Reglamento, conforme su disponibilidad.
- b) Nombrar al DPD y asegurar su involucramiento oportuno en asuntos de protección de datos.
- c) Liderar el Grupo de PDP.
- d) Resolver las investigaciones vinculadas con la eventual infracción de este Reglamento y aplicar las sanciones que correspondan.
- e) Designar al investigador en el contexto de procedimientos por infracción al Reglamento.

3. Dirección Jurídica:

- a) Monitorear los desarrollos normativos de orden legal e infralegal relativos a la LPDP.
- b) Dirigir, a través de la UAJI, la tramitación y respuesta de las solicitudes de ejercicio de los derechos de los titulares de datos, en coordinación con el DPD y conforme al Procedimiento, visando los proyectos de resolución u oficio que las resuelvan.
- c) Gestionar la publicación mensual de convenios suscritos por el CPLT para la cesión o transferencia de datos personales.
- d) Supervisar la legalidad de los acuerdos, contratos o convenios que tengan por objeto el intercambio de datos personales entre el CPLT y otros responsables.
- e) Supervisar la legalidad de las resoluciones y otros actos administrativos del CPLT que puedan incidir en el tratamiento de datos personales en el CPLT.
- f) Encargarse de establecer los resguardos y cláusulas necesarias para la protección de datos personales en aquellos actos jurídicos que suscriba el CPLT.
- g) Revisar y validar las bases de licitud y demás habilitantes legales necesarias para los tratamientos de datos del CPLT, pudiendo requerir para ello la colaboración de las jefaturas y del DPD.

- h) Colaborar en el proceso de compras en lo que concierne al cumplimiento de las obligaciones asociadas al tratamiento de datos por mandatario, y de transferencias internacionales de datos.
- i) Remitir al DPD los proyectos de políticas, procedimientos o instrumentos internos que puedan tener vinculación con los datos personales que trata el CPLT, para el ejercicio de sus funciones.
- j) Elaborar instrumentos jurídicos o minutas de análisis necesarias para cumplir la LPDP en el CPLT.
- k) Participar en el Grupo de PDP del CPLT.
- l) Aquellas otras funciones que señala este Reglamento.

4. Dirección de Desarrollo Digital:

- a) Implementar, diseñar y mantener medidas técnicas y organizativas de seguridad de la información y ciberseguridad para proteger los datos personales y dar cumplimiento a este Reglamento y la LPDP, colaborando y coordinándose con los jefes de unidades orgánicas en lo pertinente.
- b) Mantener registro actualizado de las medidas implementadas bajo el literal anterior.
- c) Mantener identificadas las transferencias internacionales de datos personales y las jurisdicciones donde estos son importados.
- d) Implementar el deber de protección de datos personales desde el diseño y por defecto, y la observancia a los principios de protección de datos en el desarrollo de sus funciones.
- e) Establecer mecanismos para detectar y gestionar vulneraciones a medidas de seguridad.
- f) Coordinar las acciones necesarias en caso de una vulneración a medidas de seguridad conforme el procedimiento dictado.
- g) Informar al DPD respecto de nuevas tecnologías, productos o servicios que conlleven un tratamiento de datos personales en el CPLT, para el ejercicio de sus funciones.
- h) Mantener registro de los datos personales que se tratan en las plataformas del CPLT, incluyendo la estructura de la base de datos, los flujos de datos, metadatos y el ciclo de vida de los datos, en conformidad con la gestión de activos de información y de los inventarios de datos del CPLT.
- i) Habilitar herramientas para la clasificación o etiqueta de datos personales reservados o confidenciales por parte de las personas trabajadoras del CPLT.

- j) Mantener registro y control de cuentas y perfiles de acceso respecto de los sistemas tecnológicos y plataformas del CPLT que almacenan o tratan datos personales.
- k) Efectuar, a requerimiento del DPD, las gestiones para mantener disponibles los avisos de tratamiento de datos en las plataformas del CPLT y el centro de protección de datos personales.
- l) Diseñar, implementar y mantener, a través de la USD, el Sistema de Gestión de Solicitudes de derechos de los titulares de datos que contemple un expediente electrónico conforme la LPDP y la Ley N°21.180, en los términos del Procedimiento.
- m) Diseñar, implementar y mantener un sistema tecnológico para gestionar el RAT.
- n) Diseñar, implementar y mantener, o coordinar su adquisición, conforme criterios presupuestarios, otros sistemas tecnológicos que sean necesarios para el cumplimiento de la LPDP en el CPLT.
- o) Colaborar en la respuesta ante el ejercicio de los derechos de los titulares de datos conforme al Procedimiento.
- p) Participar en el Grupo de PDP del CPLT.
- q) Contribuir, a través de la UEE, en el resguardo de datos personales que deban ser despachados o notificados por el CPLT.
- r) Aquellas otras funciones que señala este Reglamento.

5. Jefatura de la Unidad de Comunicaciones del CPLT:

- a) Contribuir en la difusión y comunicación del Reglamento y las informaciones que se deban remitir, incluyendo disponibilizar la información sobre protección de datos personales en el sitio web del CPLT según sea requerido por el DPD.
- b) Contribuir en la diagramación y accesibilidad de los instrumentos que se generen en el marco del Reglamento.
- c) Hacer los ajustes en el sitio web del CPLT respecto de información sobre protección de datos personales según sea requerido por el DPD.
- d) Consultar previamente al DPD respecto de publicaciones, de cualquier tipo, que se refieran a la LPDP y a la protección de datos personales, o que involucren datos personales.

6. Jefatura de la Unidad de Estrategia y Control de Gestión:

- a) En el marco de sus funciones, efectuar seguimiento y control de metas y objetivos institucionales que contribuyan al cumplimiento de la LPDP y de este Reglamento.

- b) Coordinar con el DPD y el Director General la incorporación de metas y objetivos institucionales vinculados con la protección de datos personales en el CPLT.
- c) Identificar y documentar, en coordinación con el DPD, los procesos institucionales que conlleven el tratamiento de datos personales.
- d) Informar al DPD de las modificaciones de procesos institucionales que tengan impacto en el tratamiento de datos personales por el CPLT.
- e) Efectuar la supervisión del Reglamento en el marco de sus funciones.
- f) Participar en el Grupo de PDP del CPLT.

7. Auditoría Interna:

- a) Coordinar con el DPD la identificación de los riesgos a la protección de datos personales y al cumplimiento de la LPDP en el marco de la gestión de riesgos del CPLT, para su gestión y mitigación.
- b) Hacer seguimiento y supervisar, en el marco de sus funciones, el cumplimiento o aplicación de los controles establecidos en los procesos del CPLT que se vinculan con el tratamiento de datos personales.
- c) Efectuar la supervisión del Reglamento en el marco de sus funciones.

8. Jefatura de la Unidad de Administración y Personas:

- a) Verificar y gestionar la incorporación de las cláusulas sobre protección de datos personales en aquellos contratos de compras que suscriba el CPLT, independiente de la modalidad de contratación y de la responsabilidad que tiene la jefatura que inicie y requiera la contratación respectiva.
- b) Desarrollar las gestiones necesarias para el cumplimiento de este Reglamento en el contexto de la contratación de productos y servicios del CPLT.
- c) Llevar registro de las contrataciones del CPLT, las cláusulas sobre protección de datos incorporadas y los mandatarios del tratamiento.

9. Delegado de Protección de Datos Personales del CPLT:

- a) Supervisar y orientar el cumplimiento de este Reglamento y de la LPDP por el CPLT.
- b) Informar y asesorar al Consejo, mandatarios y personas trabajadoras del CPLT sobre el derecho a la protección de datos personales y la regulación de su tratamiento.

- c) Denunciar aquellas infracciones a este Reglamento, a la LPDP o a cualquier otra norma aplicable al tratamiento de datos personales para efectos de lo dispuesto en el Título X.
- d) Contribuir en la consolidación del RAT conforme la información proporcionada por las distintas unidades orgánicas.
- e) Proponer los avisos de tratamiento de datos conforme la información proporcionada por las unidades orgánicas, y coordinar su disponibilidad con la DDD.
- f) Asistir en la identificación de riesgos y medidas para resguardar a los titulares.
- g) Ser punto de contacto de la Agencia.
- h) Participar en la elaboración, revisión y modificación del modelo de prevención de infracciones del CPLT a que se refiere el artículo 49 de la LPDP.
- i) Participar en la capacitación y concientización de las personas trabajadoras del CPLT respecto del derecho a la protección de datos personales, la LPDP y este Reglamento, y coordinar acciones con el ADGP.
- j) Participar en el Grupo de PDP del CPLT.
- k) Colaborar con la DJ y la UAJI en la tramitación y respuesta ante el ejercicio de los derechos de los titulares de datos, conforme al Procedimiento.
- l) Absolver consultas y solicitudes de los titulares de datos, conforme al artículo 92 de este Reglamento y a las reglas de consulta previa del Procedimiento.
- m) Desarrollar un plan de trabajo anual y rendir cuenta de sus resultados.
- n) Coordinarse, colaborar y requerir colaboración de las direcciones y unidades para el ejercicio de sus funciones.
- o) Reportar al Director General y al Consejo Directivo del Consejo de manera periódica.
- p) Aquellas otras funciones que señalan este Reglamento y el artículo 50 de la LPDP.

10. Jefatura del Área de Desarrollo y Gestión de Personas:

- a) Participar en el procedimiento de denuncias por infracción a este Reglamento, y efectuar el reporte que corresponda.

- b) Diseñar, junto con el DPD, planes de capacitaciones en protección de datos para las personas trabajadoras del CPLT.
- c) Colaborar en las gestiones necesarias para establecer resguardos de protección de datos en los contratos de las personas trabajadoras del CPLT, o en otros instrumentos que sea necesario.
- d) Resguardar los datos personales de las personas trabajadoras del CPLT y coordinar las medidas necesarias para tal fin; esto sin perjuicio de las medidas dispuestas por la DDD.
- e) Efectuar las comunicaciones requeridas para deshabilitar cuentas de usuario conforme a la política sobre identidad y acceso.
- f) Participar en el Grupo de PDP del CPLT.

11. Jefes de unidades orgánicas del CPLT:

- Cumplimiento y gobernanza

- a) Gestionar medidas para que, en su unidad orgánica, se cumpla este Reglamento y la LPDP en las actividades de tratamiento que se realizan, actualizando los procedimientos, manuales, guías o instrucciones internas según sea necesario.
- b) Supervisar la aplicación de los controles sobre protección de datos definidos en sus procesos y procedimientos institucionales, y reportar al DPD cualquier desviación relevante.
- c) Promover, en su unidad orgánica, buenas prácticas en protección de datos personales.
- d) Colaborar con las unidades del CPLT y con el DPD en el cumplimiento de la LPDP y este Reglamento.

- Identificación y registro

- a) Identificar y mantener actualizadas las actividades de tratamiento de datos que se realizan en su unidad orgánica, así como las bases de datos que se utilizan en dicho contexto y de las que son responsables, reportando al DPD los cambios para actualizar el RAT del CPLT.
- b) Confirmar anualmente al DPD la vigencia de la información del RAT de su unidad orgánica.
- c) Asegurarse de que las actividades de tratamiento estén reflejadas en un aviso de tratamiento disponible para los titulares, proporcionando la información necesaria para mantenerlos actualizados.
- d) Asegurarse de que los datos tratados se encuentren debidamente clasificados como reservados o confidenciales cuando estos sean sensibles, relativos a NNA o relativos a infracciones, penales, civiles,

administrativas y disciplinarias, coordinando con la DDD y el DPD en lo que corresponda.

- e) Verificar que cada formulario que recolecte datos personales en su unidad orgánica cumpla el principio de proporcionalidad, y esté vinculado a un aviso revisado por el DPD.
- f) En caso de que una actividad de tratamiento de datos sea amparada en el consentimiento del titular, recolectar dicha autorización y custodiar la documentación que acredite el otorgamiento.

- **Seguridad y mandatarios**

- a) Identificar las personas trabajadoras del CPLT con acceso a los datos personales tratados en la respectiva unidad orgánica, y limitar su acceso sólo a quienes necesiten conocerlos.
- b) De ser necesario, coordinar con la DDD aquellas medidas de seguridad adicionales o específicas que se deban implementar en el contexto de los tratamientos de datos que realiza en su unidad orgánica.
- c) Informar oportunamente cambios en la composición de sus equipos para efectos de deshabilitar cuentas de usuarios y/o modificar accesos a datos personales o sistemas.
- d) Reportar a la brevedad las vulneraciones a medidas de seguridad de las que tome conocimiento mediante el canal que se defina en el procedimiento respectivo.
- e) Informar al DPD iniciativas o contrataciones relacionadas con el tratamiento de datos personales, especialmente en el caso de datos sensibles, de NNA, de un volumen importante de datos, o cuando detecten un riesgo para los derechos de los titulares o de potencial infracción a la LPDP.
- f) Identificar aquellas situaciones donde se prevea un tratamiento de datos por un mandatario, de forma que se tomen las prevenciones para dar cumplimiento oportuno a la LPDP.
- g) Aquellas otras funciones que señala este Reglamento.

12. Personas trabajadoras del Consejo para la Transparencia:

- **Cumplimiento y conocimiento normativo**

- a) Dar cumplimiento a este Reglamento y a la demás normativa sobre protección de datos del CPLT, efectuando el tratamiento de datos personales de acuerdo con sus disposiciones.

- b) Mantenerse interiorizados respecto de este Reglamento y la LPDP, de las políticas de ciberseguridad y seguridad de la información, así como de los materiales disponibles en el Repositorio de PDP.
- c) Participar en las capacitaciones y especializaciones en protección de datos personales que se realicen.
- d) Acceder, requerir acceso y tratar únicamente los datos personales necesarios para sus funciones, evitando la recopilación, acceso o conservación de datos innecesarios o desactualizados.
- e) Abstenerse de usar los datos personales que tomen conocimiento en el ejercicio de sus cargos para una finalidad distinta de la autorizada, o utilizarlos en beneficio propio o de terceros.
- f) Comunicar o transferir datos conforme este Reglamento.

- **Confidencialidad y seguridad**

- a) Guardar secreto o confidencialidad respecto de los datos personales que tomen conocimiento en el ejercicio de sus cargos, obligación que subsiste incluso después del término de sus funciones.
- b) Seguir y aplicar las directrices institucionales definidas en este Reglamento y por el CPLT en lo que concierne a medidas de seguridad para los datos personales.
- c) Utilizar exclusivamente herramientas tecnológicas, cuentas y plataformas institucionales para el tratamiento de datos personales.
- d) Tarjar o anonimizar aquellos datos personales que consten en documentos o archivos que deban ser remitidos a terceros y que no corresponda comunicar o ceder.
- e) Activar oportunamente la herramienta de reserva u otras de clasificación disponibles cuando en sus funciones detecten un caso que contenga datos personales sensibles, de NNA o relativo a infracciones penales, civiles, administrativas o disciplinarias.

- **Reportes y cooperación**

- a) Reportar a la brevedad las vulneraciones a medidas de seguridad de las que tome conocimiento mediante el canal que se defina en el procedimiento respectivo.
- b) Consultar a su jefatura o al DPD ante cualquier duda relacionada con el tratamiento de datos personales en el contexto del CPLT como responsable de datos.
- c) Atender las tareas que se le requieran para la tramitación de solicitudes de ejercicio de derechos de la LPDP.

En el caso que alguna de las unidades orgánicas del CPLT modifique su denominación, los roles y responsabilidades indicadas serán asignadas y asumidas por aquellas direcciones, unidades, áreas u otras divisiones organizativas que les reemplacen o sustituyan en sus funciones. Asimismo, las unidades dependientes de una dirección ejercerán, en el ámbito de su competencia, las funciones que a ésta corresponden conforme a este Reglamento, al reglamento orgánico del CPLT y al Procedimiento.

Párrafo 4°. Recolección e identificación de datos personales en el CPLT.

Artículo 23. Recolección de datos personales. La recolección de datos en el CPLT se rige por los principios establecidos en este Reglamento.

La recolección de datos personales desde fuentes de acceso público, como parte de un proceso regular, requerirá visto bueno de la Dirección Jurídica y aviso previo al DPD.

Está prohibida la recolección de datos personales de fuentes ilícitas, de fuentes que no garanticen su legítima procedencia, de fuentes cuyos datos hayan sido recabados contraviniendo la ley, o a través de aplicaciones o sistemas no autorizados por el CPLT.

Artículo 24. Identificación y clasificación de datos tratados en el CPLT. El CPLT implementará mecanismos para identificar y clasificar o etiquetar los datos personales, cualquiera sea su formato o soporte, incluyendo los contenidos en documentos, bases de datos, plataformas o repositorios.

- a) Estos mecanismos podrán comprender inventarios de datos, registros, el Catastro de Bases de Datos Personales del Consejo, registros de datos tratados en plataformas tecnológicas, registros sobre el ciclo de vida del dato, etc. La información podrá ser almacenada en herramientas tecnológicas que permitan una visualización adecuada y actualizada.
- b) Serán clasificados o etiquetados como reservados o confidenciales:
 - los datos personales sensibles.
 - los datos relativos a NNA.
 - los datos relativos a infracciones penales, civiles, administrativas y disciplinarias.
- c) Esta identificación y clasificación formará parte de procesos o procedimientos institucionales vinculados a la gestión de activos de información del CPLT, y contribuirá en la aplicación de medidas de seguridad, y para la actualización del RAT. Para estos efectos, el Catastro de Bases de Datos Personales del Consejo se articulará con el RAT, de modo que las bases individualizadas en aquel se asocien a las respectivas actividades de tratamiento.

Párrafo 5°. Registro de actividades de tratamiento de datos del CPLT.

Artículo 25. RAT y su contenido. El CPLT llevará un RAT que será consolidado por el DPD, y cuyo contenido estará basado en el artículo 14 ter de la LPDP y en aquellos aspectos que se estimen pertinentes.

Artículo 26. Responsabilidad y actualización periódica del RAT. Las jefaturas del CPLT serán responsables de la información del RAT concerniente a las actividades de tratamiento de la respectiva unidad orgánica y de que ella se mantenga actualizada. Esta actualización deberá coordinarse con el deber de informar cambios para la actualización de avisos establecido en el Título IV de este Reglamento.

Nuevas actividades de tratamiento requieren aviso al DPD y su inclusión en el RAT.

Sin perjuicio del deber de actualización, cada jefatura deberá revisar, al menos una vez al año, la información del RAT correspondiente a su unidad orgánica y confirmar al DPD que dicha información se encuentra vigente o, en su caso, las actualizaciones que correspondan. Esta confirmación deberá efectuarse aun cuando no existan cambios que informar.

Párrafo 6°. Protección desde el diseño y gestión de riesgos.

Artículo 27. Protección desde el diseño y por defecto. El CPLT, en sus iniciativas que involucren el tratamiento de datos personales, tales como la creación o implementación de sistemas, programas informáticos, sitios electrónicos, productos, procesos y procedimientos, incluyendo procedimientos de compras públicas, aplicará desde el diseño, con anterioridad y durante el tratamiento, medidas técnicas y organizativas destinadas a cumplir los principios de este Reglamento y los derechos de los titulares de datos.

Por su parte, el CPLT aplicará medidas para garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales específicos y estrictamente necesarios para dicha actividad.

Artículo 28. Procesos relacionados al tratamiento de datos personales. Los procesos institucionales, y los procedimientos que los formalicen, deben incorporar los principios que informan el tratamiento de datos personales y las medidas de este Reglamento, para lo cual, incorporarán los elementos necesarios para alcanzar dicho objetivo, tales como referencias normativas a la protección de datos y controles específicos.

Artículo 29. Gestión de riesgos y evaluaciones de impacto a la protección de datos. La identificación, evaluación y mitigación de riesgos es un aspecto importante de la protección de los derechos y libertades de los titulares y del cumplimiento de la LPDP, para lo cual se adoptarán las medidas de este Reglamento y otras que resulten adecuadas a dicho fin. El Auditor Interno considerará los riesgos en el modelo de gestión de riesgos del CPLT, para lo cual se coordinará con el DPD. Esto es sin perjuicio de la realización de una EIPD cuando corresponda, y de la gestión de riesgos de ciberseguridad y seguridad de la información que deba efectuar la DDD.

Frente a tratamientos susceptibles de producir un alto riesgo para los derechos de los titulares, el CPLT realizará EIPD cuando así lo requiera la LPDP y según los criterios que defina la Agencia. Se considerará especialmente la realización de EIPD respecto de aquellos nuevos tratamientos de datos personales al interior del Consejo que se vinculen con:

- a) La evaluación sistemática y exhaustiva de aspectos personales de los titulares, basadas en tratamiento o decisiones automatizadas, como la elaboración de perfiles, y que produzcan en ellos efectos jurídicos significativos.
- b) El tratamiento masivo de datos personales o a gran escala, por ejemplo, por número de titulares, el número de ítems tratados, la extensión geográfica del tratamiento, o la duración del tratamiento.
- c) El tratamiento que implique observación o monitoreo sistemático de una zona de acceso público.
- d) El tratamiento de datos sensibles y de categorías especiales de datos.
- e) El tratamiento de datos de personas de grupos vulnerables.
- f) El tratamiento basado en la incorporación de nuevas tecnologías a la institución.

La EIPD se revisará cuando existan cambios relevantes del tratamiento o del riesgo. Durante el proceso de evaluación, la opinión del DPD debe ser recabada y documentada.

TÍTULO IV. TRANSPARENCIA E INFORMACIÓN

Artículo 30. Regla general y avisos de tratamiento de datos personales. El CPLT otorgará información suficiente, oportuna y en lenguaje claro a los titulares respecto del tratamiento de datos que realiza en atención a lo dispuesto en la LPDP y al principio de transparencia e información. Así, el CPLT mantendrá avisos de tratamiento de datos que den cumplimiento al artículo 14 ter de la LPDP.

Los jefes de las unidades orgánicas serán responsables de que las actividades de tratamiento que realicen estén reflejadas en un aviso de tratamiento disponible para consulta de los titulares.

Avisos o señalética específica deberá ser disponibilizada en el contexto del sistema de videovigilancia del CPLT.

Artículo 31. Contenido de los avisos de tratamiento de datos personales.

- a) La política de tratamiento adoptada por el CPLT, su fecha y versión.
- b) La individualización del CPLT, su representante legal y la identificación del DPD.
- c) El mecanismo para el ingreso de las solicitudes de los titulares de datos.
- d) Las categorías, clases o tipos de datos que trata el CPLT, la descripción genérica del universo de personas que comprenden sus bases de datos, los destinatarios a los que se prevé comunicar o ceder los datos, las finalidades de los tratamientos que realiza, y la base de legitimidad del tratamiento. En caso de tratamientos que se basen en la satisfacción de intereses legítimos, cuáles serían éstos.
- e) La política y las medidas de seguridad adoptadas para proteger las bases de datos personales, conforme lo dispuesto en el Título VI de este Reglamento.
- f) Los derechos que asisten a los titulares de datos ante el CPLT, conforme lo dispuesto en el Título V de este Reglamento.
- g) El derecho que asiste al titular de recurrir ante la Agencia, en caso de que el CPLT rechace o no responda oportunamente las solicitudes que le formule.
- h) La transferencia de datos personales a un tercer país u organización internacional y si estos ofrecen o no un nivel adecuado de protección, conforme lo dispuesto en el Título VII de este Reglamento.
- i) El periodo de conservación de los datos personales, conforme lo dispuesto en el Título VIII de este Reglamento.
- j) La fuente de la cual provienen los datos personales y, en su caso, si proceden de fuentes de acceso público.

- k) El derecho del titular a revocar su consentimiento, en caso de que este corresponda a la base de legalidad aplicable.
- l) La existencia de decisiones automatizadas, incluida la elaboración de perfiles, incluyendo información significativa sobre la lógica aplicada, y las consecuencias previstas de dicho tratamiento para el titular.

Información adicional se incorporará en el caso que se traten datos biométricos o de geolocalización conforme disponga la LPDP.

Artículo 32. Disponibilidad de los avisos. El acceso a los avisos por los titulares deberá habilitarse en:

- a) Los sitios electrónicos del CPLT.
- b) Las instancias de recolección de datos desde los titulares, tales como formularios de inscripción.
- c) Las instancias de comunicación directa con los titulares, como boletines, comunicados o similares.
- d) Las oficinas del CPLT, ya sea entregándoles indicaciones para el acceso en el sitio electrónico del CPLT o proveyéndoles de una copia física para consulta.

Artículo 33. Accesibilidad de los avisos de tratamiento. Los avisos deberán ser redactados en lenguaje claro y sencillo, de forma que sean fácilmente comprensibles para los titulares de datos, pudiendo emplearse avisos de tratamiento por capas.

Artículo 34. Elaboración y actualización de los avisos de tratamiento. El o los avisos de tratamiento serán propuestos por el DPD conforme la información entregada por los jefes de las unidades orgánicas. Estos deberán reflejar fielmente las actividades de tratamiento efectuadas por el CPLT.

Cuando existan modificaciones en el tratamiento que afecten el contenido de los avisos, las jefaturas serán responsables de comunicar dicha situación al DPD, a fin de efectuar las actualizaciones correspondientes.

Las modificaciones en los avisos deberán reflejarse correlativamente en el RAT.

Artículo 35. Centro de protección de datos personales. El CPLT mantendrá disponible al público en su sitio web, un centro de protección de datos personales o sección equivalente que permita acceder a este Reglamento, los avisos de tratamiento, el procedimiento de ejercicio de derechos de los titulares del Título V, el medio de contacto del CPLT y la Agencia, y a los otros antecedentes que se estimen pertinentes.

La DDD y la Unidad de Comunicaciones contribuirán en la disponibilidad técnica de esta sección en coordinación con el DPD.

TÍTULO V.

DERECHOS DEL TITULAR DE DATOS PERSONALES ANTE EL CPLT

Artículo 36. Derechos de los titulares de datos personales. El CPLT respeta el ejercicio de los derechos de los titulares de datos, los cuales son personales, intransferibles e irrenunciables y no pueden limitarse por ningún acto o convención.

Los derechos que consagra la LPDP se pueden ejercer ante el CPLT dirigidos al Director General, en su calidad de jefe superior del servicio conforme al inciso tercero del artículo 23 de la LPDP, todo ello sujeto a las condiciones y limitaciones que la LPDP y el Procedimiento establecen.

El ejercicio de los derechos será gratuito para el titular, sin que pueda exigírsele pago alguno por la presentación, tramitación o respuesta de su solicitud.

Artículo 37. Procedimiento de ejercicio de derechos. El CPLT cuenta con el Procedimiento de tramitación de solicitudes de ejercicio de derechos de los titulares de datos personales ante el Consejo para la Transparencia, aprobado por Resolución Exenta, el cual regula el ingreso de las solicitudes, la verificación de identidad del solicitante, su admisibilidad y subsanación, la distribución, y la respuesta y su notificación, así como los roles de las direcciones y unidades que intervienen.

Este procedimiento será actualizado según las definiciones que pueda tomar la Agencia, y prevalecerá sobre este Reglamento en todo aquello que regule de modo específico, aplicándose éste en forma supletoria.

Artículo 38. Plazo de respuesta. El CPLT responderá las solicitudes de ejercicio de derechos en el plazo máximo de treinta días corridos contados desde el ingreso; plazo que podrá ser prorrogado por el CPLT, por una sola vez, hasta por treinta días corridos adicionales.

Artículo 39. Ingreso de solicitud de ejercicio de derechos. El ingreso de solicitudes se realizará por escrito a través del sitio electrónico del CPLT o de forma presencial en su Oficina de Partes, sin perjuicio de la casilla institucional que se habilite para las presentaciones complementarias conforme al Procedimiento. El canal electrónico que se disponga estará actualizado, operativo y será de fácil acceso y uso para el ejercicio de estos derechos.

Lo anterior, es sin perjuicio de la asistencia, guía u orientación que pueda brindar la UPF al titular, en el marco de sus funciones.

Artículo 40. Gestión de solicitudes y herramientas tecnológicas. La tramitación de solicitudes será realizada por la DJ, a través de la UAJI, conforme defina el procedimiento dictado al efecto, y en donde también participarán el DPD, la DDD, y la unidad orgánica que corresponda en atención a los datos objeto del derecho ejercido.

El CPLT dispondrá de herramientas tecnológicas para responder al ejercicio de derechos de los titulares.

Artículo 41. Reclamación ante la Agencia. El titular podrá reclamar ante la Agencia cuando el CPLT deniegue una solicitud, en forma expresa o tácita, o no otorgue respuesta dentro del plazo legal.

Artículo 42. Habeas data impropio. En el caso de que una SAI presentada de acuerdo con la Ley de Transparencia conlleve la entrega de datos personales a quien dice ser su titular, se deberá efectuar, antes de la entrega, una verificación de la identidad del titular o su apoderado. Lo anterior es sin perjuicio de que las SAI se rigen por la Ley de Transparencia y no por el Procedimiento, conforme éste dispone.

TÍTULO VI. MEDIDAS DE SEGURIDAD Y CONFIDENCIALIDAD DE LOS DATOS PERSONALES

Párrafo 1°. Aspectos generales.

Artículo 43. Regla general y políticas de ciberseguridad y seguridad de la información. Los datos personales estarán sometidos a medidas destinadas a garantizar un nivel de seguridad adecuado al nivel de riesgo, en conformidad a la LPDP, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Estas medidas asegurarán la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales y de los sistemas de tratamiento de datos.

Las medidas considerarán controles físicos, administrativos y técnicos tales como los que se indican de forma ejemplificativa en el Anexo N°3 “Catálogo de controles”.

Sin perjuicio de los aspectos específicos que señale este Reglamento, las medidas de seguridad serán también reguladas por las políticas de seguridad de la información y de ciberseguridad del CPLT, y por aquellos procedimientos y normativa interna sobre seguridad de datos.

La detección y manejo de incidentes se regirá por el Párrafo 2° de este Título VI.

Artículo 44. Elementos para la determinación de medidas de seguridad. Para esta determinación, el CPLT tendrá en cuenta el estado de la técnica; los costos de aplicación; la naturaleza, alcance, contexto y fines del tratamiento; la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados.

Se dispondrán medidas de seguridad reforzadas respecto de los datos clasificados como reservados o confidenciales en el CPLT, incluyendo los datos personales sensibles, los datos personales de NNA y los relativos a infracciones penales, civiles, administrativas o disciplinarias. En este último caso, se estará a lo dispuesto en el artículo 25 de la LPDP.

Artículo 45. Medidas de seguridad en el Portal de Transparencia. Las medidas de seguridad que se implementen deberán considerar las características particulares del tratamiento de datos que involucra el Portal de Transparencia del Estado, y que comprende un tratamiento de datos de gran volumen, de diversos titulares, y donde concurren distintos organismos.

Artículo 46. Registro de medidas de seguridad. La DDD mantendrá documentación y registros necesarios para acreditar la existencia y funcionamiento de las medidas que haya adoptado conforme este Título.

Artículo 47. Acceso a datos personales por las personas trabajadoras del CPLT. Las personas trabajadoras del CPLT sólo tendrán acceso a los datos personales necesarios para sus funciones, lo que incluye sólo habilitar o requerir la activación de herramientas o funcionalidades cuando sean necesarias para las labores.

El CPLT mantendrá mecanismos de control de acceso a datos personales, de forma de garantizar que sólo las personas trabajadoras del CPLT autorizadas accedan a ellos. Cada jefatura deberá supervisar los accesos de su equipo, debiendo dar aviso en caso de tener que modificar un perfil o deshabilitar una cuenta de usuario.

Las medidas señaladas podrán formar parte de un procedimiento o política sobre identidad y acceso.

Artículo 48. Ambientes de explotación. La existencia de ambientes de explotación de datos en el CPLT que incluyan datos personales requerirá que la USD establezca medidas de seguridad robustas para la protección de esos datos y mantenga registro de los sistemas involucrados en cada ambiente, las categorías de datos personales almacenados, la identificación de los usuarios autorizados, y la trazabilidad de sus acciones.

Sólo aquellas personas trabajadoras del CPLT autorizadas tendrán acceso a dichos ambientes, debiendo, respecto de los datos personales:

- a) Utilizarlos sólo para la finalidad específica que hubiera sido indicada para otorgar el acceso, en el marco de las funciones legales del CPLT.
- b) No compartirlos con terceros u otras personas trabajadoras del CPLT no autorizadas, ni habilitar dicha obtención.
- c) No generar reportes o informes sin previa anonimización, salvo autorización expresa de la jefatura de la Unidad respectiva.
- d) Acceder únicamente a los datos necesarios para la finalidad que se vaya a desarrollar.

Artículo 49. Solicitudes de datos entre unidades orgánicas del CPLT. Los accesos temporales o para proyectos o estudios particulares a bases de datos personales de responsabilidad de otra unidad orgánica deberán solicitarse a través del procedimiento establecido al efecto. La solicitud será efectuada por escrito por el jefe de la unidad respectiva, indicando la finalidad del tratamiento, el plazo por el que requiere el acceso, y los analistas que accederán a los datos. La solicitud será revisada y aprobada por el jefe de la unidad responsable de la base de datos.

Estos datos podrán disponibilizarse en el ambiente de explotación específico señalado en el artículo anterior, en cuyo caso también se requerirá la aprobación del jefe de la USD.

El acceso se otorgará por el plazo mínimo necesario y se revocará automáticamente.

Párrafo 2°. Detección y manejo de incidentes.

Artículo 50. Procedimiento de gestión y manejo de incidentes. El CPLT contará con un procedimiento para la gestión de incidentes o vulneraciones a las medidas de seguridad que afecten datos personales, que considerará:

- a) La detección, contención y evaluación del impacto del incidente;

- b) Los mecanismos de notificación de vulneraciones reportables, según corresponda;
- c) El registro de notificaciones que señala la LPDP; y
- d) La determinación de roles y responsabilidades para las personas trabajadoras del CPLT, tales como la intervención del DPD.

Este procedimiento podrá formar parte del procedimiento general de gestión de incidentes de ciberseguridad y seguridad de la información del CPLT, sin perjuicio de los aspectos particulares que deban atenderse bajo la LPDP.

Artículo 51. Calificación de la vulneración a medidas de seguridad como reportable. La calificación de una vulneración a medidas de seguridad como reportable a la Agencia y/o a los titulares de datos requerirá consulta previa al DPD y a la DJ.

Artículo 52. Notificación a la Agencia y a los titulares de datos. El CPLT notificará a la Agencia las vulneraciones reportables por los medios más expeditos posibles, sin dilaciones indebidas y conforme las instrucciones que establezca dicho organismo.

El CPLT también notificará a los titulares de datos cuando las vulneraciones reportables se refieran a datos personales sensibles, datos relativos a niños y niñas menores de catorce años o datos relativos a obligaciones económicas, financieras, bancarias o comerciales. Esta deberá efectuarse en lenguaje claro y sencillo, singularizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas.

Esta notificación se realizará a cada titular afectado o, si ello no es posible, mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional.

Lo anterior es sin perjuicio de las notificaciones que deban efectuarse a la Agencia Nacional de Ciberseguridad, u otras que resulten aplicables.

Artículo 53. Registros de notificaciones. El CPLT mantendrá registro de las notificaciones de vulneraciones a las medidas de seguridad, que contendrán, al menos, la fecha de la notificación, la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos, el número de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

Artículo 54. Reporte interno de incidentes. El que detecte una vulneración a medidas de seguridad o tenga una sospecha de aquella, incluyendo posibles afectaciones a la confidencialidad, integridad o disponibilidad de datos personales, deberá dar aviso en el menor plazo posible mediante el canal que se defina en el procedimiento respectivo. Deberá entregar:

- a) Una descripción del incidente.
- b) La fecha en que fue detectado.

- c) Los datos o categorías de datos afectados, de ser posible.

Esto, sin perjuicio de las alertas que pueden ser generadas por los sistemas de monitoreo del CPLT.

El incumplimiento de este deber podría ser objeto de un procedimiento sancionatorio en los términos del Título X de este Reglamento.

Párrafo 3°. Uso de herramientas tecnológicas.

Artículo 55. Tratamiento de datos personales mediante herramientas tecnológicas y sistemas de inteligencia artificial. Sólo se permite el tratamiento, envío o transmisión de datos personales a través de herramientas tecnológicas institucionales y según las condiciones de seguridad establecidas. En ese contexto, se prohíbe:

- a) El almacenamiento o tratamiento de datos personales en dispositivos, medios o cuentas no institucionales, incluyendo dispositivos o cuentas personales no autorizadas.
- b) La utilización de redes públicas, Wi-Fi abiertas o canales no cifrados adecuadamente para acceder, enviar o compartir datos personales.
- c) El uso de aplicaciones, plataformas o servicios no autorizados que puedan comprometer la protección de datos personales.
- d) El ingreso de datos personales en sistemas o funcionalidades de inteligencia artificial no autorizados por el CPLT, incluidos servicios gratuitos o de acceso mediante cuentas personales.

Con todo, el uso de un sistema de inteligencia artificial autorizado en el CPLT en ningún caso sustituye la responsabilidad, el análisis ni la decisión que corresponde a la persona trabajadora del CPLT que lo utiliza, debiendo verificar personalmente cualquier resultado antes de emplearlo.

Artículo 56. Almacenamiento de datos en plataformas internas compartidas. Las personas trabajadoras del CPLT deben estar conscientes de los datos personales que traten en plataformas internas del CPLT cuando dicha acción implique un acceso a los datos por parte de otras unidades orgánicas. Siempre deberán utilizar plataformas que permitan el acceso controlado a los datos conforme las reglas de este Reglamento.

Artículo 57. Uso de herramientas para fines de ciberseguridad. Las acciones de ciberseguridad del CPLT serán proporcionales a los fines perseguidos sobre protección de la infraestructura tecnológica y la información, respetando el derecho a la vida privada y la protección de datos de los usuarios. A su turno, éstos estarán conscientes de que el CPLT monitorea el uso de recursos tecnológicos, y, por tanto, dicho uso debe circunscribirse sólo a las funciones institucionales.

Párrafo 4°. Confidencialidad de los datos personales.



Artículo 58. Deber de confidencialidad en el tratamiento de datos personales. El CPLT tomará las medidas necesarias para garantizar el principio de confidencialidad de los datos personales.

Las personas trabajadoras del CPLT y obligados por este Reglamento deben mantener confidencialidad de los datos personales que traten. Para ello, deberán seguir las medidas que se establezcan y usar las herramientas disponibles, no dejando expuestos los datos personales que traten.

Artículo 59. Deber de confidencialidad del DPD. El DPD estará obligado a mantener estricto secreto o confidencialidad de los datos personales que conociere en el ejercicio de su cargo en conformidad a lo que señala el artículo 50 de la LPDP.

Artículo 60. Duración del deber de confidencialidad. El deber de confidencialidad es de carácter indefinido y subsiste tanto después de concluida la relación con el titular, como después de concluida la relación entre el obligado por este Reglamento y el CPLT.

TÍTULO VII. CESIONES Y COMUNICACIONES DE DATOS PERSONALES

Párrafo 1°. Mandatarios del tratamiento de datos personales.

Artículo 61. Mandatarios del tratamiento de datos. Conforme el artículo 15 bis de la LPDP, se deberá suscribir un contrato de mandato para el tratamiento con todos aquellos que traten datos personales por cuenta o bajo instrucciones del CPLT.

La jefatura que inicie y requiera la contratación o compra pública en el CPLT, es responsable de que se suscriba este contrato de mandato, esto, sin perjuicio de las funciones de la DJ y de la UAP.

El mandatario tendrá prohibido el tratamiento de datos para un objeto distinto al convenido con el CPLT, así como su cesión en los casos en que el CPLT no lo haya autorizado de manera expresa y específicamente para cumplir con el objeto del encargo.

Artículo 62. Contenido del mandato para el tratamiento de datos personales. Estos contratos deberán incluir el objeto del encargo, la duración del mismo, la finalidad del tratamiento, el tipo de datos personales tratados, las categorías de titulares a quienes conciernen los datos, y los derechos y obligaciones de las partes. Se deberán incorporar obligaciones de confidencialidad, de adopción de medidas de seguridad y notificación de incidentes, relativas al régimen de subcontratación o submandatarios, de colaboración respecto de los derechos de los titulares de datos, de colaboración respecto de las obligaciones del CPLT como responsable, de información sobre el cumplimiento de las obligaciones del proveedor, de ubicación o localización del tratamiento, de responsabilidad del mandatario por el tratamiento indebido, y de destino de los datos al finalizar el encargo.

El CPLT podrá elaborar cláusulas tipo o modelo, que podrán ser adaptadas a las necesidades específicas del tratamiento y que se dispondrán en el Repositorio de PDP.

Artículo 63. Responsabilidad solidaria del CPLT por la actuación del mandatario. Conforme la LPDP, el CPLT será solidariamente responsable por los daños que ocasione el mandatario del tratamiento, cuestión por lo cual se deben tomar las precauciones para que los terceros que tengan esta calidad otorguen garantías suficientes de protección de datos personales.

Artículo 64. Inicio de flujo de contratación pública del CPLT. Quien inicie un requerimiento de contratación o compra pública en el CPLT tendrá la obligación de recabar e indicar aquella información que sea necesaria para la redacción e incorporación de las disposiciones contractuales señaladas en este párrafo, especialmente en lo que concierne a:

- a) Si la compra o contratación conllevará el tratamiento de datos personales por parte de un proveedor que actuará como mandatario del tratamiento.

- b) Los datos personales que en dicha circunstancia se van a entregar o comunicar al proveedor, las categorías de titulares y la finalidad del tratamiento.
- c) Aquella otra información que pueda requerir el flujo del CPLT o directamente la UAP, la DJ o el DPD.

Artículo 65. Gestión e incorporación del mandato. Con esta información, la UAP deberá gestionar, en conjunto con la DJ, la incorporación de las disposiciones necesarias para cumplir con este párrafo. Para ello podrá requerir colaboración del DPD, especialmente en contratos que involucren un volumen importante de datos personales o datos de carácter sensible.

El contrato de mandato deberá incorporarse preferentemente en las bases administrativas del proceso de licitación, sin perjuicio de poder utilizar otros mecanismos que sean obligatorios para el proveedor.

Artículo 66. Selección de mandatarios del tratamiento del CPLT. Teniendo presente la Ley N°19.886, el CPLT seleccionará proveedores que ofrezcan un adecuado nivel de protección de los datos personales que trata como responsable. Así, la selección y contratación de un tercero mandatario deberá considerar, según el alcance, naturaleza y riesgos del tratamiento a encomendar, como criterios de calidad, elementos tales como:

- a) Los controles de seguridad de la información y de los datos personales implementados, incluyendo su observancia de la normativa nacional sobre ciberseguridad,
- b) La capacitación de sus trabajadores en protección de datos personales,
- c) Sus mecanismos de gestión de incidentes,
- d) La existencia de certificaciones bajo estándares de la industria,
- e) La existencia de políticas y procedimientos relacionados con la protección de datos personales,
- f) La existencia de un Delegado de Protección de Datos Personales o de funciones similares,
- g) Su inclusión en el Registro Nacional de Sanciones y Cumplimiento, y/o
- h) Aspectos de localización y transferencia internacional de datos, etc.

El CPLT no utilizará mandatarios cuyos antecedentes den cuenta de un bajo o insuficiente nivel de protección de datos personales.

En el caso que el mandatario trate los datos personales fuera de Chile, como podría ocurrir en el caso de un proveedor de servicios de nube, se deberán considerar las reglas para las transferencias internacionales de datos que señala este Reglamento.

Artículo 67. Manual de compras y otras regulaciones. El proceso de compras en el CPLT estará regulado por el Manual de Procedimientos de adquisiciones y de gestión de contratos del CPLT, la Ley N°19.886 y su reglamento, y otras regulaciones que lo complementen o sustituyan, las cuales podrán complementar o especificar lo indicado en este Párrafo. En caso de contradicción sobre un aspecto de protección de datos personales, tendrá prevalencia lo indicado en este Reglamento.

Párrafo 2°. Comunicación o cesión de datos personales por parte del CPLT.

Artículo 68. Regla general. El CPLT no comunicará o cederá datos personales a terceros, salvo cuando la comunicación o cesión cuente con una habilitante legal conforme la LPDP y las disposiciones aplicables, así como se enmarque en este Reglamento. El CPLT tomará medidas para que los datos personales que ceda o comunique sean exactos, completos y actuales. En estas comunicaciones se considerarán aquellas publicaciones de datos personales en portales accesibles al público vía Internet.

En la remisión o envío de documentos que contengan datos personales que no deban ser comunicados, se aplicarán técnicas de tarjado o anonimización que impidan que terceros accedan a esos datos.

Las comunicaciones a mandatarios se registrarán por lo que se señala sobre mandatarios en el Párrafo 1° de este Título VII.

Artículo 69. Tarjado y versiones públicas. El tarjado o censura de documentos es una medida destinada a prevenir la divulgación no autorizada de datos personales y, cuando proceda, generar versiones públicas conforme el principio de divisibilidad o para publicar documentos que no revelen datos personales. El tarjado debe efectuarse siempre mediante herramientas que eliminen de forma irreversible el contenido respectivo, las que deberán disponibilizarse por el CPLT.

El tarjado en el CPLT se regulará por este Reglamento y por lo que establezca la LPDP y el reglamento que sea dictado conforme al artículo 26 de dicha ley.

Artículo 70. Notificaciones de actos administrativos. En la notificación de actos administrativos, como resoluciones u oficios, se deberán tomar resguardos cuando su contenido o contexto (por ejemplo, adjuntos), comprendan datos personales. Así, deberán, entre otras medidas, tarjar los datos que no puedan formar parte de la notificación, utilizar los mecanismos dispuestos para restringir el acceso, y, según estimen necesario, avisar a la UEE para el resguardo de los datos personales.

La UEE contribuirá con las demás unidades orgánicas para el resguardo de los datos personales en el marco de sus funciones.

Las medidas de restricción de acceso se ajustarán al Título VI de este Reglamento.

Artículo 71. Solicitudes de comunicación o cesión de datos personales por parte de organismos públicos al CPLT. Salvo un procedimiento especial, las solicitudes de comunicación o cesión de datos personales serán revisadas y gestionadas

conforme las reglas y habilitantes que dispone el artículo 22 de la LPDP, entre las que se encuentra aquella comunicación o cesión que resulte necesaria para el cumplimiento de las funciones legales, y que el CPLT y el receptor de los datos actúen dentro del ámbito de sus competencias. Estas comunicaciones o cesiones se regirán también por lo que indique el reglamento que sea dictado conforme al artículo 26 de dicha ley.

Artículo 72. Publicación de fotografías y videos con imágenes de rostros de personas en Internet. Esta materia estará regida por el Anexo N°4 “Guía de uso de fotografías y videos en actividades del CPLT”.

Párrafo 3°. Datos personales en el contexto de instituciones de la Ley de Transparencia.

Artículo 73. Datos personales en el contexto de publicaciones en transparencia activa. La publicación de datos personales en virtud de obligaciones de transparencia activa constituye un tratamiento de datos personales. En ese contexto, los intervinientes en la tramitación deben tomar todos los resguardos para que dicho tratamiento se efectúe en conformidad con la Ley de Transparencia, la Instrucción General sobre Transparencia Activa, este Reglamento, y la demás normativa aplicable.

Estas publicaciones sólo deberán contener aquellos datos personales que la normativa mandate específicamente publicar. El tarjado de datos personales será responsabilidad de aquella unidad orgánica responsable de la información a publicar, sea que la cargue directamente o a través de la UAJI.

Artículo 74. Datos personales en el contexto de SAI. La tramitación de SAI implica un tratamiento de datos personales, tanto de los datos que componen la solicitud, de los de terceros o de los que pudieran contenerse en la documentación requerida. En dicho contexto, los intervinientes en la tramitación deben tomar todos los resguardos para que dicho tratamiento se efectúe en conformidad con este Reglamento, el Manual de Gestión de Solicitudes de acceso a la información en el CPLT vigente, la Instrucción General que regula las SAI vigente, y las demás normas aplicables.

Respecto de SAI que involucren datos personales cuyo titular no sea el solicitante, se deberá tener especialmente en cuenta lo dispuesto en el inciso quinto del artículo 22 de la LPDP y en el artículo 20 de la Ley de Transparencia.

La notificación del artículo 20 de la Ley de Transparencia al tercero interesado sólo incluirá el nombre y apellidos del solicitante, reservando otros antecedentes.

El tarjado de datos personales que se requiera de la información que vaya a ser entregada en virtud de una SAI, será responsabilidad de aquella unidad orgánica responsable de la información solicitada.

Artículo 75. Datos personales en el contexto de procedimientos de amparo al derecho de acceso y de reclamo por obligaciones de transparencia activa. La tramitación de estos procedimientos implica un tratamiento de datos personales de

diversos titulares, incluyendo terceros interesados. En dicho contexto, quienes intervengan en los mismos deberán tomar todos los resguardos para que dicho tratamiento se efectúe en conformidad con este Reglamento y las demás normas aplicables, lo que incluye, al menos, resguardos y controles en lo que se refiere a:

- a) El buen uso de las plataformas del CPLT y sus herramientas, como la de reserva: Ya sea plataformas internas del CPLT, o aquellas que dispone en línea. En el caso de la herramienta de reserva, esta se deberá utilizar, al menos:
 - Cuando la solicitud o los antecedentes del caso incluyen datos sensibles o de NNA del reclamante;
 - Cuando la solicitud o los antecedentes del caso incluyen datos sensibles o de NNA de terceros;
 - Cuando los descargos o adjuntos incorporen datos sensibles o de NNA del reclamante o de terceros, o datos sobre denuncias, investigaciones o sanciones penales o administrativas.
- b) El buen uso de plataformas de terceros, como la Oficina Judicial Virtual OJV, y en la tramitación de recursos o acciones judiciales. En el caso de la OJV, se deberán tarjar o anonimizar los antecedentes que se acompañan cuando sea procedente, o, de ser necesario, requerir la reserva de la carpeta electrónica o de alguna pieza del expediente conforme las reglas que estén definidas para ello y los autos acordados del Poder Judicial.
- c) El desarrollo y seguridad de plataformas por la DDD para la tramitación de estos procedimientos conforme la protección de datos desde el diseño y por defecto, y los demás principios de la LPDP.
- d) La redacción y preparación de escritos y documentos en general: Incluyendo traslados a terceros, oficios, correos, decisiones, y el envío de adjuntos. En este caso se deben tomar medidas tales como el tarjado de datos, o el uso de fórmulas genéricas o siglas que eviten la divulgación indebida de datos personales. Particular atención se debe prestar en la información o antecedentes que consten en el documento y que, junto con un identificador como el nombre y apellido, pueda conllevar inferencias o revelar datos personales o sensibles que deberían ser resguardados.

Sin perjuicio de lo anterior, la notificación del artículo 25 de la Ley de Transparencia al tercero interesado sólo incluirá el nombre y apellidos del solicitante, reservándose otros datos personales.

Por regla general, no corresponderá la publicación o comunicación de datos personales de solicitantes de SAI y reclamantes de amparo y de transparencia activa.

Párrafo 4°. Datos relativos a infracciones penales, civiles, administrativas y disciplinarias.

Artículo 76. Tratamiento de datos relativos a infracciones penales, civiles, administrativas y disciplinarias. El CPLT sólo tratará datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y en los casos expresamente previstos en la ley. Esta información se mantendrá en el CPLT como información reservada, conforme lo dispuesto en el Título III.

Las unidades orgánicas que traten estos datos deberán tomar las medidas necesarias para su resguardo conforme los términos de este Reglamento.

Artículo 77. Comunicación o publicación de esta clase de datos. No se comunicarán o publicarán estos datos una vez prescrita la acción o cumplida o prescrita la pena o sanción, conforme al inciso tercero del artículo 25 de la LPDP, salvo respecto de los registros que los órganos públicos lleven por expresa disposición de la ley, y sin perjuicio de la excepción de su inciso sexto en favor de los tribunales de justicia y de otros organismos públicos que los requieran para el cumplimiento de sus funciones legales. En ese contexto, y conforme a la letra b) del inciso cuarto del mismo artículo, se publicarán las sanciones previstas en el Título VI de la Ley de Transparencia en conformidad con el artículo 48 de dicha ley, las que permanecerán accesibles al público por un periodo de cinco años.

El CPLT velará por que los datos relativos a infracciones que sean publicados o comunicados sean exactos, suficientes, actuales y completos, lo que comprenderá especialmente la comunicación de información sobre sancionados en procedimiento sumario bajo la Ley de Transparencia.

La US deberá velar por que la publicación de estos datos se realice conforme con este artículo, dando los avisos oportunos a las unidades involucradas en el procedimiento, de ser procedente.

Está prohibido incorporar, en las resoluciones y otros documentos cuya publicación sea requerida por ley, enlaces, hipervínculos o similares, que redirijan a repositorios de información en la nube concernientes a procedimientos sumarios o de investigaciones sumarias del CPLT.

Párrafo 5°. Transferencias internacionales de datos personales.

Artículo 78. Regla general y habilitaciones para las transferencias internacionales de datos. El CPLT tratará los datos personales en Chile, salvo que se encuentre en el marco de las habilitaciones legales establecidas en la LPDP y en la normativa interna que resulte aplicable. Así, conforme al artículo 27 de la LPDP, sólo transferirá datos personales cuando:

- a) La transferencia se realice a una persona, entidad u organización pública o privada, sujeta al ordenamiento jurídico de un país que proporcione niveles adecuados de protección de datos personales, y que haya sido determinado así por la Agencia.

- b) La transferencia quede amparada por cláusulas contractuales, u otros instrumentos jurídicos suscritos entre el CPLT y el responsable o tercero mandatario, y en ellas se establezcan garantías adecuadas, de conformidad a lo dispuesto en el artículo 28 de la LPDP.
- c) El CPLT y el responsable o tercero mandatario que la recibe, adopten un modelo de cumplimiento o mecanismo de certificación y en ellos se establezcan garantías adecuadas de conformidad con el artículo 28 de la LPDP.
- d) Excepcionalmente, y en ausencia de los mecanismos anteriores, conforme alguna de las hipótesis aplicables para transferencias no habituales, como cuando la transferencia resulte necesaria por aplicación de convenios de cooperación, intercambio de información o supervisión que hayan sido suscritos por el CPLT para el cumplimiento de sus funciones y en el ejercicio de sus competencias.

Artículo 79. Responsabilidad especial para los requirentes de compras o convenios. Será responsabilidad de cada jefatura o persona trabajadora del CPLT requirente de una compra o de un convenio en que se transfieran datos personales encargarse de que, en el contexto de dicha compra o convenio, se cumplan las reglas de transferencia internacional señaladas y exista una habilitante, exigiendo, de ser necesario y de forma previa, todos los antecedentes al proveedor o contraparte respectiva.

Artículo 80. Contratación de proveedores tecnológicos. En la contratación de proveedores tecnológicos que actúen como mandatarios o responsables del tratamiento de datos que sean comunicados por parte del CPLT, deberá prestarse especial atención a la ubicación de aquellos servidores e infraestructura tecnológica que vayan a tratar o almacenar los datos para efectos de dar debido cumplimiento a las normas que regulan la transferencia internacional de datos personales en la LPDP.

Párrafo 6°. Transferencia o cesión de datos personales hacia el CPLT.

Artículo 81. Regla general para cesiones o transferencias de datos personales hacia el CPLT. El CPLT podrá ser destinatario de datos personales desde otros responsables para que los trate en calidad de responsable. En dichas circunstancias, la cesión y el tratamiento deberán dar cumplimiento a este Reglamento y los principios que regulan el tratamiento de datos.

El CPLT sólo requerirá los datos necesarios para la finalidad señalada, y así se lo deberá informar al potencial cedente de ser factible.

Particular atención se deberá prestar cuando los datos sean sensibles o de NNA, como podría ocurrir, por ejemplo, cuando se coordinan acciones con establecimientos educacionales.

Artículo 82. Cesiones o comunicaciones en el marco de un contrato o convenio. En las cesiones que sean reguladas o estén enmarcadas en el cumplimiento de contratos o convenios, se deberán incorporar resguardos a la protección de datos que incluyan al menos, el objeto y finalidad de la cesión, los tipos de datos y categorías de titulares, los principios del tratamiento de datos, declaraciones y garantías asociadas, las obligaciones relevantes de cooperación e información entre las partes, seguridad y confidencialidad de los datos. Estos casos pueden acontecer, por ejemplo, cuando se requiere a un proveedor de servicios el envío de determinados antecedentes de sus trabajadores.

Artículo 83. Cesiones o comunicaciones en el marco del funcionamiento de portales del CPLT. Las cesiones o comunicaciones de datos personales, incluyendo disponibilizaciones al público, que se efectúen en la operación o funcionamiento de portales que el CPLT disponibiliza en el marco de sus funciones legales, tales como el Portal de Transparencia del Estado, InfoLobby o InfoProbidad, deberán ajustarse a lo dispuesto en este Reglamento y la normativa que sea aplicable. Estas deberán reflejarse en el RAT y en los avisos de tratamiento conforme el Título IV de este Reglamento.

Respecto de los portales y plataformas de su responsabilidad, la DDD establecerá medidas para que los datos comunicados al CPLT se limiten a los estrictamente necesarios, y se traten conforme los principios de la LPDP, como los de finalidad y seguridad.

El CPLT podrá establecer normativa particular o instrucciones específicas respecto del tratamiento de datos en el contexto de dichos portales.

TÍTULO VIII. CONSERVACIÓN O RETENCIÓN DE DATOS PERSONALES

Artículo 84. Retención de datos personales. El CPLT conservará los datos personales durante el periodo de tiempo en que sean necesarios para cumplir el propósito del tratamiento en el marco de sus funciones legales, o según indique la ley. Respecto de datos personales que sean recibidos desde otros órganos públicos aplicará lo dispuesto en el inciso tercero del artículo 22 de la LPDP.

La retención en el caso del tratamiento exclusivo con fines históricos, estadísticos, científicos, de estudio o investigación se regirá por el artículo 16 quinquies de la LPDP.

Luego del periodo de retención, los datos serán suprimidos o anonimizados de manera segura.

La potencial solicitud de datos personales que eventualmente se pueda realizar ante el CPLT a partir de una SAI no constituirá fundamento para la conservación de datos personales.

Artículo 85. Política o procedimiento sobre retención de datos personales. El CPLT tendrá un documento formal, política o procedimiento, aprobado por el Director General, en que se fijen parámetros para la retención o conservación de los datos personales, y que podrá formar parte de la regulación interna sobre gestión documental. Estos parámetros deberán considerar:

- a) El tipo de datos personales tratados por el CPLT.
- b) La normativa aplicable al CPLT sobre gestión documental y archivo, tal y como la dispuesta por la Ley N°21.180, la Ley de Transparencia o aquella sobre almacenamiento y remisión de documentos a otras entidades como el Archivo Nacional.
- c) Las funciones legales a las que está mandatado el CPLT dentro del ámbito de sus competencias.
- d) Las otras medidas sobre gestión documental dispuestas al interior del CPLT.

Los parámetros de retención definidos deberán reflejarse en el RAT y en los avisos de tratamiento, cuando corresponda.

Artículo 86. Responsabilidad de las jefaturas en la retención de datos personales. Será responsabilidad de cada jefatura de las unidades orgánicas:

- a) Proponer el periodo de retención conforme la actividad de tratamiento de datos que realice en virtud de sus funciones y los parámetros indicados, y su modificación de ser aplicable.

- b) Iniciar el procedimiento para la eliminación o anonimización de datos personales conforme la LPDP y la normativa aplicable, como en el caso de un procedimiento de expurgación documental.

TÍTULO IX. CAPACITACIÓN Y CONCIENTIZACIÓN

Artículo 87. El CPLT realizará capacitaciones y actividades de concientización periódicas para las personas trabajadoras del CPLT en materias de protección de datos personales y este Reglamento, de forma de reforzar los requerimientos que se han establecido. Según sea definido, la participación en las capacitaciones podrá resultar obligatoria y sujeta a evaluación.

Artículo 88. Ingresos al CPLT. Los nuevos ingresos al CPLT deberán participar en una o más inducciones relativas a este Reglamento y la LPDP.

A su turno, el ADGP estará encargada de difundir y entregar a todos los nuevos ingresos al CPLT una copia de este Reglamento y de los instrumentos relevantes en la materia, lo cual podrá coordinar con el DPD. Los nuevos ingresos deberán dar cuenta de que han tomado conocimiento de este Reglamento.

Artículo 89. Desarrollo y coordinación de actividades. Capacitaciones, inducciones y actividades de concientización serán efectuadas por el DPD en conjunto con el ADGP. Estas acciones también podrán ser efectuadas por otras unidades orgánicas del CPLT, las cuales deberán atenerse a los lineamientos que pueda otorgar el DPD para mantener la consistencia de criterios en los contenidos.

TÍTULO X.

SUPERVISIÓN DEL REGLAMENTO, REPORTES E INFRACCIONES

Artículo 90. Aspectos generales. La infracción a este Reglamento y la LPDP puede generar responsabilidad disciplinaria, sin perjuicio de otras responsabilidades. En particular, las infracciones a los principios, derechos y obligaciones de la LPDP en que incurra el CPLT se tipifican en los artículos 34 bis, 34 ter y 34 quáter de dicha ley, son determinadas por la Agencia y se sancionan, conforme a su artículo 44, con multa que recae sobre el jefe superior del servicio, sin perjuicio de la responsabilidad del funcionario infractor que establece su artículo 45.

La supervisión de este Reglamento tiene dos mecanismos. El mecanismo principal de supervisión que recaerá en el DPD, en la UECG y el Auditor Interno. Y el mecanismo secundario de supervisión, que recae en todas las jefaturas de las unidades orgánicas del CPLT.

Artículo 91. Supervisión del DPD. La supervisión de este Reglamento y de la LPDP recae de forma autónoma en el DPD a través de mecanismos tales como la solicitud de información, la realización de entrevistas o cuestionarios, la revisión de sistemas o plataformas, la revisión de políticas y procedimientos, u otros que determine procedentes.

Estas labores de supervisión podrán resultar, entre otras, en la realización de una denuncia por infracción al Reglamento o la LPDP, en un requerimiento directo para la atención de la conducta al o los involucrados, o en su inclusión en sus reportes.

Artículo 92. Canal de Consultas. El DPD dispondrá de un canal de consultas en torno a las materias de este Reglamento y del derecho a la protección de datos personales en el CPLT, disponible para todos los titulares de datos personales. Las consultas que los titulares formulen se canalizarán a través de la UPF, en los términos del Procedimiento.

Artículo 93. Supervisión de la UECG y del Auditor Interno. La supervisión del Reglamento también la efectuará la UECG y el Auditor Interno, en el marco de sus funciones y reportes. Los hallazgos relevantes podrán ser comunicados al DPD, al Director General o al Grupo de PDP, o gestionados a través de una denuncia por infracción al Reglamento.

Artículo 94. Supervisión de las jefaturas del CPLT. Las jefaturas del CPLT deberán mantener una vigilancia permanente respecto de la observancia de este Reglamento en las respectivas unidades orgánicas, adoptando las medidas adecuadas, procediendo a la corrección de aquellas conductas que no se ajusten a lo requerido o efectuando las consultas que sean pertinentes.

Artículo 95. Auditorías. El CPLT podrá realizar auditorías para revisar la aplicación de este Reglamento y el tratamiento de datos personales al interior de la institución, las cuales podrán ser realizadas internamente o a través de terceros. El CPLT podrá

establecer un procedimiento específico para la realización de estas auditorías, las cuales serán desarrolladas sin perjuicio de las disposiciones de este Título.

Artículo 96. Reportes internos y avisos. Para el cumplimiento de este Reglamento se establecerán reportes internos y avisos que consistirán, en general, en:

- a) Avisos de parte de las jefaturas y las personas trabajadoras del CPLT al DPD conforme lo dispuesto en el Párrafo 3° de Roles y Responsabilidades, del Título III de este Reglamento.
- b) Avisos en el contexto de vulneraciones a medidas de seguridad.
- c) Reporte interno de incidentes.
- d) Reportes del DPD al Director General y al Consejo Directivo.
- e) Reporte de la UECG o del Auditor Interno al DPD en el marco de sus funciones de supervisión.
- f) Reportes consistentes en denuncias por infracción al Reglamento.
- g) Reporte del ADGP al Director General en torno a denuncias que sean recibidas por infracción a este Reglamento.
- h) Reportes en el contexto del Grupo de PDP.

Artículo 97. Denuncia por infracción al Reglamento y Canal de Denuncias. La denuncia podrá ser efectuada por cualquier obligado por este Reglamento, y por la UECG, el Auditor Interno o el DPD a partir de sus funciones de supervisión.

Esta denuncia podrá ser efectuada respecto de cualquier obligado por este Reglamento.

El CPLT dispondrá de un canal de denuncias electrónico que permita recibir estas denuncias. Las denuncias serán recibidas por el jefe o jefa del ADGP.

La denuncia será presentada por escrito, y deberá incluir:

- a) Identificación del denunciante con su nombre, y su correo electrónico institucional.
- b) Identificación de la o las personas denunciadas y sus cargos, cuando sea posible.
- c) Narración circunstanciada de los hechos que se denuncian y los datos personales afectados.
- d) Antecedentes y documentos que le sirvan de fundamento.

La identidad del denunciante será mantenida en reserva.

Artículo 98. Procedimiento de investigación y sanción. El procedimiento aplicable para la comprobación de los hechos denunciados, la determinación de las responsabilidades y la aplicación de la sanción se ajustará, en todo lo compatible con este Reglamento, a lo dispuesto en el Título VI (De las sanciones y multas de la

Primera Parte, Normas de Orden), del Reglamento Interno de Orden, Higiene y Seguridad del CPLT o aquel que lo reemplace. Este procedimiento también podrá iniciarse de oficio por parte del Director General.

La investigación constará por escrito y se registrará por los principios de confidencialidad, bilateralidad, profesionalismo, legalidad e imparcialidad.

El Director General, antes de determinar el inicio de un procedimiento de investigación o de la aplicación de una medida, podrá requerir el informe independiente del DPD respecto del caso. Ello no procederá en el caso de una indagatoria iniciada por denuncia del DPD.

El DPD no podrá ser designado para llevar adelante la investigación disciplinaria.

El procedimiento asegurará en todas sus etapas el debido proceso.

Artículo 99. Infracciones al Reglamento y sanciones. La infracción a este Reglamento será sancionada, en los términos previstos en el Reglamento Interno de Orden, Higiene y Seguridad.

Su inobservancia además se considerará incumplimiento grave de las obligaciones que impone el contrato de trabajo a aquella, en los términos del artículo 160 del Código del Trabajo, así como contravención al principio de probidad administrativa.

Las infracciones cometidas por los proveedores se registrarán por los términos de la relación contractual con el CPLT.

El ADGP deberá llevar registro de las sanciones aplicadas por infracción al Reglamento, información que será comunicada al DPD para sus funciones.

Artículo 100. Medidas correctivas. No obstante, el sobreseimiento, la absolución o la aplicación de una sanción disciplinaria, el CPLT podrá adoptar medidas correctivas para prevenir y controlar los riesgos identificados en los hechos que dieron lugar a la denuncia.

Artículo 101. Prevención de infracciones y modelo de prevención. En cumplimiento del artículo 48 de la LPDP, el CPLT adoptará acciones destinadas a prevenir la comisión de las infracciones de los artículos 34 bis, 34 ter y 34 quáter de dicha ley, entre las que se cuentan este Reglamento, el Procedimiento, los demás instrumentos internos que lo complementen, las medidas técnicas de ciberseguridad y seguridad de la información implementadas, las capacitaciones del Título IX y los mecanismos de supervisión, reporte y denuncia del Título X.

Asimismo, el CPLT podrá adoptar el modelo de prevención de infracciones del artículo 49 de la LPDP, en cuyo caso corresponderá al Grupo de PDP, en coordinación con la DJ y el DPD, proponer al Director General su contenido.

TÍTULO XI.

DISPOSICIONES FINALES

Artículo 102. Regla general y adecuación interna. El resguardo de los datos personales tratados por el CPLT se regirá por este Reglamento, el que constituye el principal instrumento normativo de carácter interno relativo a la protección y tratamiento de datos personales. En tal calidad, desde su entrada en vigencia, reemplaza y sustituye cualquier otro reglamento, política, procedimiento escrito, manual, instrucción o cualquier otra medida interna dictada con anterioridad referida a la misma materia, y que resulte contraria o incompatible.

La nueva normativa que sea generada por el CPLT deberá ajustarse a lo dispuesto en este Reglamento en cuanto se refiera al ámbito de la protección de datos personales que trata en calidad de responsable, incluyendo en esto las normativas referidas a ciberseguridad, seguridad de la información, gobernanza de datos, gestión de riesgos, compras, y otras.

En caso de que algún artículo del Reglamento esté en conflicto con la LPDP, prevalecerá la normativa legal no obstante de tener que darse aviso al DPD para coordinar los ajustes que procedan.

Artículo 103. Aplicación preferente. En casos donde exista discordancia o contradicción entre lo dispuesto en este Reglamento y otra política o procedimiento que regule algún aspecto del tratamiento de datos personales en el CPLT, prevalecerá lo dispuesto en este instrumento, salvo respecto del Procedimiento de tramitación de solicitudes de ejercicio de derechos de los titulares de datos personales, el que regirá preferentemente en las materias que regula de modo específico, aplicándose este Reglamento en forma supletoria.

Artículo 104. Adecuación en la implementación de otras leyes. Las medidas que se implementen bajo la LPDP en el CPLT deberán buscar compatibilidad con el debido cumplimiento de otras leyes aplicables al CPLT, tales como las leyes N°21.180 y N°21.663. A su turno, la implementación en el CPLT de las leyes antedichas y otras que resulten relevantes, deberán buscar compatibilidad con la LPDP, este Reglamento y la protección de los derechos de los titulares de datos.

Artículo 105. Modificación. Este Reglamento será revisado para que se encuentre ajustado al entorno normativo, incluyendo los cambios legales, la normativa infralegal aplicable y las mejores prácticas.

Artículo 106. Anexos. Los Anexos del Reglamento forman parte integrante de éste. En caso de contradicción, prevalecerá el texto del Reglamento.

Artículo 107. Entrada en vigencia. Este Reglamento comenzará a regir con la entrada en vigencia de la LPDP.

DISPOSICIONES TRANSITORIAS

Artículo primero transitorio. Dentro de los seis meses siguientes a la entrada en vigencia de este Reglamento, las direcciones y unidades del CPLT, revisarán y adecuarán a sus disposiciones los procesos, políticas, procedimientos, manuales, sistemas, guías e instrucciones internas vigentes que incidan en el tratamiento de datos personales, pudiendo requerir para ello la colaboración del DPD o de la DDD, según corresponda. En el mismo plazo deberán presentar planes de adecuación en el caso que dichos ajustes sólo puedan materializarse en un plazo superior a los seis meses indicados.

Artículo segundo transitorio. Dentro de los tres meses siguientes a la entrada en vigencia de este Reglamento, el DPD consolidará la primera versión del RAT del Consejo, con la información que le remitan las jefaturas de las unidades orgánicas. Recibida la información conforme, el DPD propondrá al Director General los avisos de tratamiento conforme el Título IV o los ajustes a los ya existentes.

Artículo tercero transitorio. El documento formal sobre retención o conservación de datos personales a que se refiere el artículo 85 deberá ser aprobado dentro de los doce meses siguientes a la entrada en vigencia de este Reglamento.

ANEXO I

GLOSARIO DE SIGLAS Y DEFINICIONES

- 1) ADGP: Área de Desarrollo y Gestión de Personas del Consejo para la Transparencia.
- 2) Agencia: La Agencia de Protección de Datos Personales.
- 3) Anonimización: Procedimiento irreversible en virtud del cual un dato personal no puede vincularse o asociarse a una persona determinada, ni permitir su identificación, por haberse destruido o eliminado el nexo con la información que vincula, asocia o identifica a esa persona. Un dato anonimizado deja de ser un dato personal.
- 4) Catastro de Bases de Datos Personales del Consejo: corresponde al catastro de las bases de datos personales que el Consejo trata en calidad de responsable, incluyendo aquellas que utilizan las personas trabajadoras del CPLT y unidades orgánicas en el ejercicio de sus labores.

Este catastro, que constituye un instrumento de identificación vinculado con el RAT del CPLT, considerará la individualización de cada base de datos existente, la unidad responsable interna de ella o de la respectiva actividad de tratamiento, y su aptitud de ser consultada por medios automatizados para la localización de datos personales.
- 5) Cesión de datos personales: Transferencia de datos personales de un responsable a otro responsable de datos.
- 6) Comunicación de datos personales: Dar a conocer por el responsable de datos, de cualquier forma, datos personales a personas distintas del titular, sin llegar a cederlos o transferirlos.
- 7) Consejo o CPLT: El Consejo para la Transparencia, corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, creado por la Ley de Transparencia. Tiene por objeto promover la transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del Estado, y garantizar el derecho de acceso a la información.
- 8) Datos personales sensibles: Los 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, que revelen el origen étnico o racial, la afiliación política, sindical o gremial, la situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.

- 9) Datos personales: Los datos personales que el CPLT trata en calidad de responsable de datos y que corresponden a cualquier información vinculada o referida a una persona natural identificada o identificable.
- 10) DDD: Dirección de Desarrollo Digital del Consejo para la Transparencia.
- 11) Derechos de los titulares: Los derechos que la LPDP reconoce a todo titular para controlar el tratamiento de sus datos personales y que son ejercitables ante el CPLT conforme al Título V de este Reglamento y al Procedimiento.
- 12) DJ: Dirección Jurídica del Consejo para la Transparencia.
- 13) DPD: El Delegado de Protección de Datos Personales del CPLT.
- 14) EIPD: Evaluación de impacto en protección de datos personales.
- 15) Fuentes de acceso público: Aquellas bases de datos o conjuntos de datos personales, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, tales como el Diario Oficial, medios de comunicación o registros públicos que disponga la ley. Su tratamiento en el CPLT se somete a este Reglamento y la LPDP.
- 16) Grupo de PDP: El Grupo de Protección de Datos Personales del CPLT, compuesto por los directores del CPLT, los jefes de la UECG y del ADGP, y el DPD.
- 17) Ley de Transparencia: Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la Ley N°20.285 sobre Acceso a la Información Pública.
- 18) LPDP: La Ley N°19.628, sobre Protección de los Datos Personales, modificada por la Ley N°21.719. En las remisiones a la LPDP, se entenderán, salvo indicación en contrario, incluidos también los reglamentos de la ley y aquellos otros actos administrativos o infralegales que surjan de la misma y sean dictados por la Agencia.
- 19) Mandatario o encargado: La persona natural o jurídica que trate datos personales por cuenta del CPLT y que debe actuar bajo sus instrucciones en los términos que señala este Reglamento y la LPDP.
- 20) NNA: Niños, niñas y adolescentes.
- 21) Las personas trabajadoras del CPLT: Las personas trabajadoras del CPLT incluyendo jefaturas, directores, honorarios, pasantes y practicantes.
- 22) RAT: Registro de actividades de tratamiento de datos personales del CPLT.
- 23) Reglamento: Este Reglamento de Protección de Datos Personales del Consejo para la Transparencia.

- 24) Repositorio de Protección de Datos Personales o de PDP: Repositorio en la intranet institucional para el acceso centralizado a los documentos internos relacionados con la protección de datos personales.
- 25) Responsable de datos: La persona que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario, y que para efectos de este Reglamento corresponde al CPLT.
- 26) SAI: Solicitud de acceso a la información pública regulada por la Ley de Transparencia y mediante la cual se solicita acceder a información que obra en poder del CPLT.
- 27) Seudonimización: Tratamiento de datos personales que se efectúa de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.
- 28) Titular de datos: La persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales que trata el CPLT como responsable.
- 29) Tratamiento de datos: Cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales.
- 30) UAJI: Unidad de Asuntos Jurídicos Internos del Consejo para la Transparencia.
- 31) UAP: Unidad de Administración y Personas del Consejo para la Transparencia.
- 32) UECG: Unidad de Estrategia y Control de Gestión del Consejo para la Transparencia.
- 33) UEE: Unidad de Expediente Electrónico del Consejo para la Transparencia.
- 34) Unidades orgánicas: Son todas las Direcciones, Unidades, Coordinaciones y Áreas del CPLT, conforme el reglamento orgánico vigente, o el acto que en subsidio corresponda.
- 35) UPF: Unidad de Promoción y Formación del Consejo para la Transparencia.
- 36) US: Unidad de Sumarios del Consejo para la Transparencia.
- 37) USD: Unidad de Sistemas y Datos del Consejo para la Transparencia.
- 38) UTC: Unidad de Tecnología y Ciberseguridad del Consejo para la Transparencia.
- 39) Vulneración a medidas de seguridad reportable: Aquella vulneración a medidas de seguridad que genera o produce un riesgo razonable para los derechos y

libertades de los titulares, y que debe ser reportada a la Agencia y, de ser procedente, a los titulares de datos. En el contexto de la ciberseguridad y su legislación, se podría asemejar al incidente de ciberseguridad que puede tener efectos significativos.

- 40) Vulneración a medidas de seguridad: Aquella vulneración que ocasione la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que el CPLT trata como responsable, ya sea de forma directa o a través de un mandatario, o la comunicación o acceso no autorizado a dichos datos.

ANEXO II

MARCO NORMATIVO

Artículo 1°. Marco normativo. El marco normativo relevante en el contexto del tratamiento de datos personales del CPLT, está compuesto principalmente por:

- a) Constitución Política de la República.
- b) Ley N°19.628, sobre Protección de los Datos Personales.
- c) Ley N°21.719, que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales y los reglamentos que se dicten a su respecto.
- d) Ley N°20.285, sobre Acceso a la Información Pública.
- e) Ley N°20.730, que Regula el lobby y las gestiones que representen intereses particulares ante las autoridades y funcionarios.
- f) Ley N°20.880, sobre Probidad en la función pública y prevención de los conflictos de intereses.
- g) Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.
- h) Ley N°19.880, que Establece bases de los procedimientos administrativos que rigen los actos de los Órganos de la Administración del Estado.
- i) Ley N°21.180, sobre Transformación Digital del Estado.
- j) Código del Trabajo.
- k) Ley N°19.886, de Bases sobre contratos administrativos de suministro y prestación de servicios.
- l) Ley N°21.663, Ley marco de ciberseguridad.
- m) Ley N°20.936, que Establece un nuevo sistema de transmisión eléctrica y crea un organismo coordinador independiente del Sistema Eléctrico Nacional.
- n) Ley N°20.915, que Fortalece el carácter público y democrático de los partidos políticos y facilita su modernización.
- o) Ley N°21.000, que Crea la Comisión para el Mercado Financiero.
- p) Ley N°20.922 que Modifica disposiciones aplicables a los funcionarios municipales y entrega nuevas competencias a la Subsecretaría de Desarrollo Regional y Administrativo.
- q) Decreto N°13, de 2009, del Ministerio Secretaría General de la Presidencia, Reglamento de la Ley N°20.285 sobre Acceso a la Información Pública.

- r) Decreto N°20, de 2009, del Ministerio Secretaría General de la Presidencia que Aprueba estatutos de funcionamiento del Consejo para la Transparencia.
- s) Instrucciones generales del Consejo para la Transparencia en ejercicio de la atribución dispuesta en el literal d), del artículo 33, de la Ley de Transparencia, especialmente las referidas al procedimiento de SAI y al régimen de transparencia activa.
- t) Instrucciones generales de la Agencia Nacional de Ciberseguridad.
- u) Aquellas instrucciones generales dictadas por la Agencia de Protección de Datos Personales.

Artículo 2°. Marco normativo interno y jerarquía. La normativa interna sobre protección de datos personales en el CPLT está compuesta por los siguientes instrumentos y tiene la siguiente jerarquía:

- a) El Reglamento.
- b) Otros reglamentos y políticas relacionadas con la protección de datos personales, como, por ejemplo:
 - Aquellas políticas de seguridad de la información y de ciberseguridad del CPLT, incluyendo las de Identidad y Acceso, la de Asignación de Activos Tecnológicos, y otras en el mismo ámbito.
 - El Reglamento interno de Orden, Higiene y Seguridad del CPLT.
 - El Reglamento orgánico del CPLT.
 - El Reglamento especial para empresas contratistas y subcontratistas del CPLT.
 - El Reglamento de funcionamiento del sistema de videovigilancia del CPLT.
 - El Reglamento del Consejo de la Sociedad Civil del CPLT.
 - La Política de Participación Ciudadana del CPLT.
 - La Política de Gestión de Procesos y Riesgos del CPLT.
- c) Procedimientos, como, por ejemplo:
 - Procedimiento de tramitación de solicitudes de ejercicio de derechos de los titulares de datos personales ante el Consejo para la Transparencia.
- d) Manuales, guías y otros similares, como, por ejemplo:
 - La Guía para el uso de fotografías y videos en actividades del Consejo para la Transparencia.

- Manual de Procedimientos de adquisiciones y de gestión de contratos del CPLT.
- Manual de Gestión de Solicitudes de acceso a la información en el CPLT.

La normativa señalada complementa el Reglamento en lo referido al tratamiento de datos personales.

ANEXO III

CATÁLOGO DE CONTROLES

Este corresponde a un catálogo referencial y no exhaustivo de medidas para el cumplimiento de las obligaciones de seguridad que contempla la LPDP. La selección e implementación específica deberá determinarse según el riesgo para los derechos y libertades de los titulares y bajo los parámetros que indica el Reglamento. La ausencia de un control en este catálogo no exime de implementar medidas técnicas y organizativas adecuadas.

Las referencias tecnológicas son ejemplificativas y pueden ser sustituidas por equivalentes con el mismo nivel de seguridad.

a) Como **controles físicos**, se considerarán:

- La seguridad de los equipos tecnológicos, incluyendo los dispositivos móviles que se usen en el ejercicio de funciones,
- La seguridad física de discos duros y otros soportes,
- La incorporación de cerraduras, alarmas o videovigilancia,
- Los controles de acceso a las oficinas del CPLT o sus bodegas,
- La adecuada eliminación de documentos y de equipos en desuso.

b) Como **controles administrativos**, se considerarán:

- Este Reglamento,
- Los procedimientos, guías y demás normativa interna sobre la materia,
- La revisión de las prácticas de seguridad de mandatarios y la gestión de estos,
- Planes de continuidad de negocio y de recuperación ante desastres,
- Guías para el uso de correo o de Internet,
- Proceso y procedimiento para la gestión de incidentes y vulnerabilidades,
- Resguardos contractuales en contratos de trabajo y en otros instrumentos obligatorios,
- Planes de capacitación y concientización de las personas trabajadoras del CPLT,
- Planes de inducción a nuevas personas trabajadoras del CPLT,
- Políticas de identidad y acceso,
- La designación de un DPD,

- La designación de un Delegado de Ciberseguridad,
- Procesos para la evaluación y revisión periódica de controles técnicos,
- Inventario y mapeo de activos con datos personales,
- Planes de respaldo, recuperación y pruebas.

c) Como **controles técnicos**, se considerarán:

- Medidas de limitación en el acceso a datos personales y la gestión de accesos y privilegios,
- Deshabilitación de cuentas y control de sesiones,
- La seudonimización y anonimización,
- El ajuste en formularios del CPLT,
- La mantención de registros de acceso basado en roles y de eliminación,
- El cifrado de datos en reposo y en tránsito,
- Configuración segura de sistemas y control de cambios,
- Los controles de prevención de pérdida de datos,
- Autenticación de doble factor (2FA),
- VPN,
- Antivirus y antimalware,
- Contraseñas,
- Respallos,
- Restricciones a las descargas de aplicaciones,
- Pruebas de penetración,
- Sistemas de recuperación e infraestructura redundante,
- Protecciones técnicas de correo y navegación web,
- Conservación de registros y logs en sistemas que traten datos personales, etc.

ANEXO IV

GUÍA DE USO DE FOTOGRAFÍAS Y VIDEOS EN ACTIVIDADES DEL CPLT

1. ¿Para qué sirve esta guía?

Para señalar a las personas trabajadoras del CPLT el manejo correcto de fotografías y videos en que aparecen personas, y que son tomados durante los eventos y otras actividades del CPLT, sean presenciales o en línea (ej. reuniones por plataforma Teams).

2. ¿A quién aplica esta guía?

Esta guía aplica a todas las personas trabajadoras del CPLT, especialmente aquellos que por sus funciones desarrollan eventos o actividades con terceros ajenos a la institución.

3. ¿Es obligatoria?

Sí, esta guía resulta obligatoria.

4. ¿Por qué esto es importante? Hay varias razones:

- ✓ ¿La imagen de una persona es un dato personal? Sí
- ✓ ¿Se necesita permiso o autorización para **publicar** la imagen de una persona? Sí, al constituir un “tratamiento” de datos, necesitamos una base de legalidad habilitante, como el consentimiento del titular (quien aparece en la imagen).
- ✓ ¿Puede afectar a las personas? Sí, la publicación de una imagen en Internet puede afectar los derechos de las personas. Una vez publicada, ya no podemos controlar su uso.

5. ¿Qué reglas debemos seguir en el CPLT para tomar y **publicar en Internet la fotografía o video de una persona**? Depende de si estamos en el caso I, caso II o caso III:

A. Caso I: Publicación permitida. Podemos tomar y publicar en Internet la fotografía o video cuando la imagen corresponda a autoridades o directivos públicos actuando en el ejercicio de sus funciones, tales como, ministros, senadores, diputados, alcaldes, jefes de servicio, Consejeros del CPLT, directores y jefes del CPLT, etc.

¿Se necesita su consentimiento en este caso? No, pues operamos en virtud de la base de legalidad del artículo 20 de la LPDP.

¿Cuáles son las condiciones para que podamos operar bajo el artículo 20 de la LPDP? Que la captura y publicación de la fotografía sea necesaria para el

cumplimiento de nuestras funciones legales, dentro del ámbito de competencias del CPLT, y de conformidad a las normas de la LPDP.

¿Qué funciones estaríamos realizando generalmente en este caso? Promover la transparencia de la función pública y el derecho de acceso a la información por cualquier medio de publicación; realizar capacitaciones; y realizar actividades de difusión e información al público, sobre materias de nuestra competencia.

B. Caso II: Publicación sujeta a previo consentimiento. Sólo previo consentimiento podemos tomar y publicar en Internet la fotografía o video de funcionarios públicos o terceros, como NNA, que actúen como expositores en eventos del CPLT, han ganado un concurso, se les otorga un reconocimiento, se certifican por el CPLT, o es en el contexto de una actividad similar donde tengan participación directa o una calidad especial.

¿Cómo se obtiene el consentimiento? Mediante un formulario que indique, entre otras cosas, para qué se usarán las fotos o videos, y que cuente con una casilla (no premarcada) para que la persona autorice. Excepcionalmente puede obtenerse mediante una declaración verbal de la persona, efectuada antes de la captura, luego de informarle para qué se usarán su imagen y su nombre, en qué medios se publicarán, que puede negarse a aparecer y cómo puede solicitar posteriormente su retiro. Esta vía no procede respecto de NNA, cuyo consentimiento siempre deberá constar por escrito.

¿Cuándo se debe obtener el consentimiento? Antes de capturar y publicar la imagen, como, por ejemplo, al momento de hacer las invitaciones o registros a la actividad.

¿Hay algún ejemplo de consentimiento que podamos usar? Sí, se puede usar el formato disponible en el Repositorio de PDP y adaptarlo al caso concreto.

¿Y si la persona es extranjera? El consentimiento deberá estar en un idioma que pueda entender.

¿Y si la imagen es de un menor de edad? Depende. Si es menor de catorce años, el consentimiento lo deben otorgar sus padres, representantes legales o quien tenga a su cargo el cuidado personal. Si tiene entre catorce y dieciocho años, el consentimiento lo debe otorgar el propio adolescente; sin embargo, si la imagen revela datos personales sensibles y el adolescente es menor de dieciséis años, el consentimiento lo deben otorgar sus padres, representantes legales o quien tenga a su cargo el cuidado personal. En todo caso, el tratamiento deberá atender al interés superior del niño, niña o adolescente y a su autonomía progresiva.

¿Qué hacer luego de obtener el consentimiento? Se deben conservar los formularios firmados o, en caso de consentimiento verbal, un respaldo de este, como la grabación de la aceptación al inicio de la cña o un registro con la persona, la fecha, la actividad y la información entregada. Debemos poder acreditar que obtuvimos la autorización.

¿Y si no nos dan la autorización o no pedimos el consentimiento? No debemos tomar ni publicar la imagen. Si es necesario informar sobre la actividad podemos buscar alternativas: fotografías sin rostros identificables, difuminación, uso de fotos únicamente de las autoridades presentes, uso de infografías, etc.

C. Caso III. Publicación prohibida. No podemos tomar y publicar en Internet y redes sociales del CPLT la fotografía o video cuando la imagen corresponda a los asistentes en general de eventos, actividades o seminarios del CPLT, sean estos ciudadanos o funcionarios.

¿Hay ejemplos de estos individuos? Sí, por ejemplo, las personas que se les brinda una capacitación, aquellos que participan como público general en el seminario internacional de la semana de la transparencia, o aquellos asistentes a las diversas charlas de los consejeros o jefaturas del CPLT.

¿Qué pasa con las fotografías grupales donde hay mucha gente, como de asistentes a eventos? No se deben publicar estas fotografías ni videos. Una alternativa es tomar fotografías panorámicas donde no se distingan los rostros, difuminarlos, o informar mediante otro mecanismo que sea respetuoso del derecho a la protección de datos personales.

6. Instrucciones finales en el contexto de la publicación en Internet:

- ✓ Antes de publicar una foto o video siempre revisar si hay rostros de personas y si aplican las reglas del caso I, II o III.
- ✓ Si la publicación es requerida por otra Unidad o Área, verificar que han cumplido las reglas que se señalan en esta guía.
- ✓ **¿Qué hacer si tenemos dudas respecto de la publicación de una fotografía o video?** No publicarla, y buscar otras alternativas para informar sobre el evento o actividad.
- ✓ **¿Qué pasa si ya publicamos fotos que no siguen las reglas de esta guía?** Estas fotografías deben eliminarse a la brevedad, incluyendo su copia e informar de esto al DPD.
- ✓ **¿Qué hacer si alguien señala que no desea ser fotografiado o que no quiere que su fotografía se publique o se mantenga publicada?** Respetar su decisión. En el caso de que la fotografía ya esté publicada,

bajarla lo antes posible. Si se desea mantener publicada, difuminar los rostros o buscar alternativas análogas.

- ✓ **¿Qué hacer si tengo más dudas?** Consultar a la jefatura directa o al DPD.

7. Uso de fotografías y su publicación en las redes internas del CPLT

- ✓ **¿Esta publicación es una comunicación o cesión de datos personales?**
En estricto rigor no, pues estamos operando en el marco del mismo responsable: el CPLT.
- ✓ **¿Qué sucede si la imagen es del hijo de una persona trabajadora del CPLT que participa, por ejemplo, como asistente en una actividad interna del CPLT?** Se requiere obtener el consentimiento previo y por escrito de forma de tener un respaldo del mismo. Se puede usar el formato disponible en el Repositorio de PDP.
- ✓ **¿Qué sucede con el uso de la imagen de las personas trabajadoras del CPLT en el ámbito del desarrollo y gestión de personas, o de administración?** En este caso NO se requiere obtener el consentimiento pues el CPLT estará operando en virtud de la base de legalidad del artículo 20 de la LPDP o conforme a una obligación de rango legal.”.

ARTÍCULO SEGUNDO: PUBLÍQUESE la presente resolución en el sitio electrónico de transparencia activa del Consejo para la Transparencia, en el apartado “Potestades y Marco Normativo”; en la intranet institucional, repositorio “Protección de Datos Personales”; y en la página web de este Consejo.

ARTÍCULO TERCERO: NOTIFÍQUESE electrónicamente la presente resolución, mediante copia digital, a todas las personas trabajadoras del CPLT.

ARTÍCULO CUARTO: DERÓGUESE, a contar de la fecha de entrada en vigencia del Reglamento aprobado por el artículo primero de esta resolución, la Resolución Exenta N°151, de 10 de julio de 2020, del Consejo para la Transparencia que Aprueba el reglamento sobre grabación y procedimiento de acceso, resguardo y conservación de la grabación de las sesiones del Consejo Directivo del Consejo para la Transparencia; y la Resolución Exenta N°304, de 30 de noviembre de 2020, del Consejo para la Transparencia que Aprueba el texto actualizado y refundido de las recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado y sustituye texto que indica.

ARTÍCULO QUINTO: ANÓTESE el número y fecha del presente acto, al margen de la Resolución Exenta N°151, de 10 de julio de 2020 y de la Resolución Exenta N°304, de 30 de noviembre de 2020, dejándose constancia de ello en los registros y sistemas internos del Consejo para la Transparencia.

ANÓTESE, NOTIFÍQUESE, PUBLÍQUESE y ARCHÍVESE

DAVID IBACETA MEDINA

Director General

Consejo para la Transparencia

DISTRIBUCIÓN:

1. Todas las personas trabajadoras del Consejo para la Transparencia.
2. Sr. Director General del Consejo para la Transparencia.
3. Sra. Directora Jurídica del Consejo para la Transparencia.
4. Sr. Director de Desarrollo Digital del Consejo para la Transparencia.
5. Sr. Secretario del Consejo Directivo del Consejo para la Transparencia.
6. Sr. Jefe de Gabinete del Presidente del Consejo para la Transparencia.
7. Sr. Delegado de Protección de Datos Personales del Consejo para la Transparencia.
8. Sra. Auditora Interna del Consejo para la Transparencia.
9. Sr. Jefe de la Unidad de Administración y Personas del Consejo para la Transparencia.
10. Sra. Jefa del Área de Desarrollo y Gestión de Personas del Consejo para la Transparencia.
11. Sr. Jefe de la Unidad de Sumarios del Consejo para la Transparencia.
12. Sr. Jefe de la Unidad de Promoción y Formación del Consejo para la Transparencia.
13. Sr. Jefe del Área de Formación del Consejo para la Transparencia.
14. Sr. Jefe de la Unidad de Fiscalización del Consejo para la Transparencia.
15. Sra. Jefa del Área de Fiscalización Aplicada del Consejo para la Transparencia.
16. Sr. Jefe del Área de Fiscalización de Cumplimiento del Consejo para la Transparencia.
17. Sra. Jefa de la Unidad de Estrategia y Control de Gestión del Consejo para la Transparencia.
18. Sra. Jefa de la Unidad de Comunicaciones del Consejo para la Transparencia.
19. Sr. Jefe de la Unidad de Estudios y Relacionamento Institucional del Consejo para la Transparencia.
20. Sr. Jefe de la Unidad de Sistemas y Datos del Consejo para la Transparencia.
21. Sr. Jefe de la Unidad de Tecnología y Ciberseguridad del Consejo para la Transparencia.
22. Sr. Jefe de la Unidad de Portal de Transparencia del Estado del Consejo para la Transparencia.
23. Sr. Delegado de Ciberseguridad del Consejo para la Transparencia.
24. Sra. Jefa de la Unidad de Expediente Electrónico del Consejo para la Transparencia.
25. Sr. Jefe de la Unidad de Análisis y Estrategia Jurídica y Judicial del Consejo para la Transparencia.
26. Sr. Jefe de la Unidad de Normativa y Regulación del Consejo para la Transparencia.
27. Sra. Jefa de la Unidad de Análisis de Admisibilidad y SARC del Consejo para la Transparencia.
28. Sra. Jefa de la Unidad de Asuntos Jurídicos Internos del Consejo para la Transparencia.
29. Archivo.