Ministerio Secretaría General de la Presidencia

Gobierno de Chile

COMISIÓN ASESORA MINISTERIAL

PARA LA IMPLEMENTACIÓN DE LA LEY N° 21.719

RECOMENDACIONES PARA LA IMPLEMENTACIÓN DE LA NUEVA LEY DE PROTECCIÓN DE DATOS PERSONALES

MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA

2025 - 2026

Ministerio Secretaría General de la Presidencia

Gobierno de Chile

COMISIÓN ASESORA MINISTERIAL

PARA LA IMPLEMENTACIÓN DE LA LEY N° 21.719

RECOMENDACIONES PARA LA IMPLEMENTACIÓN DE LA NUEVA LEY DE PROTECCIÓN DE DATOS PERSONALES

MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA

2025 - 2026

La Comisión Asesora Ministerial para la Implementación de la ley N° 21.719 fue creada mediante el decreto N° 12 de de 2025 del Ministerio Secretaría General de la Presidencia.

La Comisión estuvo compuesta por:

Romina Garrido Iglesias, Presidenta
Emilio Oñate Vera
Danielle Zaror Miralles
Marcelo Drago Aguirre
Jessica Matus Arenas
Claudio Magliona Markovicth
Ricardo Arancibia Bustos
Daniel Álvarez Valenzuela
Rodrigo Lavanderos Werner
Beatriz von Loebenstein Weil
José Ruiz Yáñez
Lizzy Seaman Espinosa, Secretaria Ejecutiva de la Comisión

Publicación de la Comisión Asesora Ministerial para la Implementación de la ley N° 21.719
"Recomendaciones para la implementación de la nueva ley de protección de datos personales".

Edición, diseño y publicación:
Ministerio Secretaría General de la Presidencia.
División Jurídico Legislativa.

Primera edición, enero 2026.
Versión digital - 20 ejemplares impresos.
www.minsegpres.gob.cl

ÍNDICE

1° INFORME DE LA COMISIÓN DE IMPLEMENTACIÓN PARA LA LEY DE PROTECCIÓN DE DATOS PERSONALES: Cronograma de instalación y necesidades de fortalecimiento institucional de la agencia de protección de datos personales (apdp). 05

I. INTRODUCCIÓN 06
II. CONTEXTO NORMATIVO Y POLÍTICO 07
III. DIAGNÓSTICO FUNCIONAL DE LA APDP 09
IV. ANÁLISIS PRESUPUESTARIO 11
V. COMPARATIVA CON OTRAS AGENCIAS DE PROTECCIÓN DE DATOS PERSONALES 13
VI. CONCLUSIONES Y RECOMENDACIONES 17

2° INFORME DE LA COMISIÓN DE IMPLEMENTACIÓN PARA LA LEY DE PROTECCIÓN DE DATOS PERSONALES: Recomendaciones relativas al tráfico transfronterizo. 19

I. INTRODUCCIÓN 20
II. CONTEXTO 20
III. METODOLOGÍA DE TRABAJO 21
IV. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES EN LA NUEVA LEY DE PROTECIÓN DE DATOS 22
V. RECOMENDACIONES DE LA COMISIÓN 24

ÍNDICE

3° INFORME DE LA COMISIÓN DE IMPLEMENTACIÓN PARA LA LEY DE PROTECCIÓN DE DATOS PERSONALES: Referido a recomendaciones para la implementación de la ley en la Administración del Estado. — 29

I. ANTECEDENTES — 30
II. CONTEXTO — 30
III. RECOMENDACIONES DE ESTA COMISIÓN DE IMPLEMENTACIÓN — 31

4° INFORME DE LA COMISIÓN DE IMPLEMENTACIÓN PARA LA LEY DE PROTECCIÓN DE DATOS PERSONALES. — 35

I. ANTECEDENTES — 36
II. CONTEXTO — 39
III. RECOMENDACIONES DE LA COMISIÓN DE IMPLEMENTACIÓN — 40

1° INFORME

CRONOGRAMA DE INSTALACIÓN Y NECESIDADES DE FORTALECIMIENTO INSTITUCIONAL DE LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES (APDP).

PRIMER INFORME DE LA COMISIÓN DE IMPLEMENTACIÓN PARA LA LEY DE PROTECCIÓN DE DATOS PERSONALES: CRONOGRAMA DE INSTALACIÓN Y NECESIDADES DE FORTALECIMIENTO INSTITUCIONAL DE LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES (APDP)
21 DE JULIO 2025

I. INTRODUCCIÓN

Chile fue pionero en Latinoamérica en dictar una Ley sobre protección de datos personales con la Ley N°19.628 sobre protección a la vida privada; sin embargo, esta norma quedó rápidamente obsoleta ante el avance vertiginoso de las tecnologías de la información, las redes sociales, el big data y la inteligencia artificial, que permitieron a entidades públicas y privadas almacenar y tratar datos personales sin mecanismos adecuados de tutela para sus titulares. En 2018, mediante la Ley N°21.096, se elevó la protección de los datos personales a rango constitucional en el artículo 19 N°4, reconociéndose no sólo su dimensión negativa (evitar el uso no autorizado), sino también su dimensión positiva: el derecho de toda persona a disponer y controlar sus datos, incluso cuando estos han dejado de estar bajo su dominio directo, consagrando así la autodeterminación informativa como expresión de la libertad sobre los datos. En respuesta al mandato constitucional, el año 2024 el Congreso Nacional aprobó una reforma integral a la Ley N°19.628 sobre protección de la vida privada, mediante la adopción de la Ley N°21.719. Esta reforma eleva sustancialmente el estándar jurídico nacional al incorporar principios internacionales en materia de tratamiento de datos personales, estableciendo nuevos derechos para sus titulares, creando mecanismos efectivos de garantía y control, e instituyendo la Agencia de Protección de Datos Personales -en adelante APDP-, como entidad especializada encargada de velar por el cumplimiento de estas disposiciones.

El 5 de junio del presente año, mediante el Decreto N°12 del Ministerio Secretaría General de la Presidencia, se constituyó la Comisión Asesora Ministerial para la Implementación de la nueva Ley de protección de datos personales, instancia consultiva cuyo objeto es asesorar técnicamente a dicho Ministerio en todas las acciones necesarias para la adecuada implementación de la Ley N°21.719, la que entrará en vigencia el 1° de diciembre del año 2026.

Las tareas que le son asignadas a esta Comisión Asesora son las siguientes: 1) Realizar un diagnóstico general de las acciones necesarias que el Ejecutivo debe impulsar para el cumplimiento de la Ley N°21.719; 2) asesorar al Ministerio Secretaría General de la Presidencia en la dictación de las normas reglamentarias necesarias para la Implementación y cumplimiento de la Ley N°21.719; 3) identificar y proponer al Ministerio todas aquellas materias legales o administrativas que fuere necesario adecuar para la correcta implementación de la Ley N°21.719; y 4) asesorar al Ministerio respecto de la dictación de los actos administrativos o la adopción de las acciones de gestión necesarias para la implementación de la nueva institucionalidad que crea la Ley N°21.719.

En ejercicio de sus funciones, la Comisión ha acordado emitir informes previos a aquél que dispone el artículo 4° del Decreto N° 12, de manera de abordar oportunamente las materias que se han considerado de mayor urgencia.

Es bajo este marco que se evacua este Primer Informe que tiene dos recomendaciones principales:

a) Anticipar la instalación de la Agencia de Protección de Datos Personales, a más tardar al mes de junio del año 2026, con la consiguiente reprogramación de la designación de sus tres consejeros, que será la instancia superior de dicho organismo, junto a un staff administrativo para permitir la puesta en marcha de esta nueva entidad.

b) Fortalecer la estructura institucional, tal como ocurre en la experiencia comparada, de la futura Agencia de Protección de Datos Personales, dotándola de recursos humanos y presupuestarios que le permitan instalar esta nueva institucionalidad para ejercer las funciones normativas, de fiscalización y control, así como de promoción de la protección de datos personales como derecho fundamental.

II. CONTEXTO NORMATIVO Y POLÍTICO

La ley aún vigente presenta importantes deficiencias que, en la práctica, la hicieron inaplicable, especialmente en el ámbito privado. La falta de una autoridad de protección de datos con facultades efectivas para fiscalizar y hacer cumplir la normativa, junto con la ausencia de un catálogo claro de infracciones y sanciones directas, impidió que la regulación alcanzara estándares mínimos de cumplimiento comparables a los exigidos internacionalmente. Esta debilidad estructural se tradujo en una baja capacidad disuasiva y en una limitada eficacia jurídica frente al tratamiento indebido de datos personales.

A pesar de este escenario, el rol asumido por el Consejo para la Transparencia —sobre todo a partir de 2018— permitió dar cumplimiento a la Ley de protección a la vida privada en el sector público. Esta labor, sin embargo, se desarrolló a partir de un marco normativo desactualizado y ampliamente superado por la evolución tecnológica. Este contexto generó un importante rezago normativo e institucional, que no solo afectó el cumplimiento de los estándares internacionales, sino que también dificultó el desarrollo de una verdadera cultura nacional en materia de protección de datos personales. Como consecuencia, múltiples sectores no incorporaron medidas legales, técnicas ni organizativas adecuadas para garantizar el uso legítimo de la información personal bajo su responsabilidad.

La reciente reforma de la Ley N° 21.719, es el resultado de, al menos, tres iniciativas impulsadas por gobiernos de distinto signo político: la primera, durante el primer mandato de la Presidenta Michelle Bachelet (2008); la segunda, en el primer gobierno del Presidente Sebastián Piñera (2012); y la tercera, en el segundo período de la Presidenta Bachelet (2017). Esta última iniciativa fue refundida con una moción parlamentaria que sirvió de base sustantiva del texto que fue objeto, en el Senado,

de una indicación sustitutiva durante el segundo mandato del presidente Piñera y fue finalmente aprobado bajo el mandato del presidente Gabriel Boric.

Durante el segundo trámite constitucional en la Cámara de Diputadas y Diputados, el proyecto fue sometido a una profunda revisión. A lo largo del debate general, se realizaron más de cien

exposiciones y se presentaron 120 indicaciones, presentadas tanto por el Ejecutivo como por parlamentarios de diversas bancadas. El proceso legislativo implicó 27 sesiones de comisión y un informe final de casi 500 páginas para despachar el texto, en el que, la mayoría de las propuestas de modificación fue aprobada por unanimidad, lo que evidencia un inusual consenso político en torno a la necesidad de modernizar esta regulación.

El éxito de esta reforma se explica, en gran medida, por la conformación de una mesa de trabajo técnico-política, integrada por representantes del Ejecutivo, asesores parlamentarios de diversas sensibilidades, y un grupo estable de expertos y expertas en protección de datos. Uno de los objetivos estratégicos fue alinear la regulación chilena con el estándar del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, con miras a que Chile pueda ser reconocido como un país con un "nivel adecuado" de protección, lo cual facilitará las transferencias internacionales de datos y reforzará la competitividad digital nacional.

En el tercer trámite constitucional, el Senado rechazó 22 enmiendas introducidas por la Cámara de Diputadas y Diputados, lo que motivó la conformación de una comisión mixta. Junto a un equipo de técnicos especializados, la comisión revisó y ajustó el proyecto, despachando un texto robusto, transversalmente respaldado. Este proyecto fue aprobado por el Congreso en agosto y promulgado en diciembre de 2024, estableciendo una vacancia legal de dos años para su plena entrada en vigor.

La efectiva operatividad de la nueva Agencia de Protección de Datos Personales constituye una condición imprescindible para la entrada en vigencia de la ley. En el plano inmediato, la APDP deberá asumir la fiscalización del cumplimiento normativo, determinar infracciones, ejercer la potestad sancionadora y resolver los reclamos de los titulares. Sólo mediante una autoridad plenamente constituida y funcional el nuevo marco normativo podrá convertirse en un instrumento disuasivo y eficaz.

Además, la APDP tendrá un rol esencial más allá de la estricta supervisión: deberá diseñar y ejecutar programas y acciones de difusión y capacitación, prestar asistencia técnica a otras entidades del Estado, suscribir convenios de colaboración con organismos públicos y privados, así como promover la cooperación internacional en esta materia, lo que contribuirá a forjar una cultura nacional de protección de datos personales, alineada con el reconocimiento de este derecho como una garantía fundamental del ordenamiento jurídico chileno.

Por último, la puesta en marcha simultánea de la Ley y de la APDP implica que múltiples disposiciones contenidas en la Ley N° 21.719 dependerán de la emisión de instrucciones, normas generales o interpretaciones administrativas, que todavía no existen. Tal es el caso, por ejemplo, de los modelos tipo de cláusulas contractuales en materia de transferencias internacionales de datos, así como otros instrumentos detallados en la tabla contenida en el punto siguiente de este informe.

El hecho de que la Ley entre en vigor de manera simultánea con la puesta en marcha de la APDP implica, por definición, que dichas normas, instrucciones o criterios interpretativos no podrán haber sido dictados con anterioridad. Esta circunstancia somete a los distintos actores —en particular, a los responsables del tratamiento de datos— a una falta significativa de certeza

jurídica, dado que la Ley les exigirá el cumplimiento de obligaciones cuyo contenido normativo específico dependerá de directrices que aún no habrán sido emitidas por la autoridad competente.

III. DIAGNÓSTICO FUNCIONAL DE LA APDP

La plena implementación de la Ley N° 21.719 no puede entenderse sin el fortalecimiento previo y sustantivo de la APDP. Dotar a la Agencia de capacidades técnicas, humanas, presupuestarias y normativas es una condición habilitante esencial para asegurar que los derechos que reconoce la Ley no queden en el papel. La Agencia, como órgano con autonomía legal y competencia nacional, está llamada a ejercer funciones esenciales para la tutela efectiva de los derechos de los titulares y la supervisión del cumplimiento normativo, incluyendo la emisión de instrucciones obligatorias, fiscalización proactiva y reactiva, resolución de reclamos, potestad sancionatoria, promoción de estándares y certificación de modelos de cumplimiento. Estas facultades deben ejercerse bajo la dirección del Consejo Directivo, cuya estructura colegiada y duración escalonada busca asegurar continuidad, independencia y gobernanza técnica. Sin embargo, la disposición tercera transitoria indica que estos Consejeros deben ser nombrados dentro de los 60 días anteriores a la entrada en vigencia de la Ley, esto es, entre el 1º de octubre de 2026 y el 1º de diciembre de 2026. Este plazo resulta insuficiente para garantizar una instalación oportuna y eficaz de la institucionalidad.

En efecto, esta Comisión ha identificado ciertos mandatos legales que deben ser ejercidos cuanto antes para dar viabilidad a la vigencia efectiva de la Ley y otorgar certeza jurídica a los responsables y encargados del tratamiento, particularmente en lo que respecta a la dictación de instrucciones y normas generales obligatorias, la definición de criterios interpretativos sobre principios y obligaciones legales, y la habilitación de procedimientos de certificación y registros oficiales.

A continuación, se detallan 11 medidas críticas y prioritarias que deben resolverse antes de la entrada en vigencia de la Ley, pues se trata de condiciones mínimas para garantizar que los derechos de millones de personas puedan ser ejercidos y protegidos desde el primer día, y para que los responsables puedan operar con certeza jurídica.

Medida Prioritaria	Base Legal	Instrumento necesario	Urgencia
Aprobar y difundir cláusulas contractuales tipo para permitir el tráfico transfronterizo de datos personales.	Art. 28, inc. 3 y 4	Instrucción General	Muy alta
Establecer un mecanismo expedito o de "fast track" para clasificar como países adecuados a aquellos países con dicha calificación por parte de la UE y así evitar realizar un procedimiento de análisis de cada país.	Art. 28	Resolución	Muy alta
Dictar una instrucción general sobre las alternativas para autenticar a los titulares de datos en solicitudes de derechos ARCO.	Art. 11 a)	Instrucción General	Muy alta
Lista orientativa de tratamientos que requieren Evaluación de Impacto. Determinar qué tipos de tratamiento exigen evaluación de impacto en protección de datos personales.	Art. 15 ter, inc. 5	Instrucción General	Muy alta
Orientaciones mínimas para realizar Evaluaciones de Impacto. Emitir lineamientos sobre contenido y metodología de dichas evaluaciones.	Art. 15 ter, inc. 6	Instrucción General	Muy alta
Establecer estándares diferenciados de cumplimiento (en seguridad y transparencia). Determinar estándares mínimos en base al tipo y tamaño del responsable, naturaleza del dato y finalidad del tratamiento.	Art. 14 septies.	Instrucción General	Alta
Dictar y poner en marcha un sistema de notificaciones a la Agencia y a los titulares ante brechas de seguridad de datos personales en conjunto con la ANCI.	Art. 14 sexies LPDP	Instrucción General	Alta
Modelos tipo de contratos entre responsables y encargados. Poner a disposición contratos estándar para el tratamiento de datos mediante terceros mandatarios.	Art. 15 bis, inc. final	Instrucción General	Alta
Dictar una instrucción general sobre los parámetros y mecanismos para determinar los costos derivados del ejercicio de los derechos de acceso y portabilidad.	Art. 10, inc. 7	Instrucción General	Media
Regular el proceso de certificación del modelo de prevención		Instrucción General	Media
Matriz de riesgo para acciones de fiscalización.		Instrucción General	Media

Resulta abiertamente irreal suponer que los mandatos técnicos y normativos urgentes que debe ejercer la Agencia de Protección de Datos Personales a través de su Consejo Directivo puedan ser cumplidos de forma adecuada dentro del ajustado plazo de sesenta días previos a la entrada en vigencia de la Ley. En dicho periodo, además de la nominación y ratificación de los consejeros, deben instalarse las capacidades institucionales mínimas para que el Consejo Directivo pueda sesionar, adoptar acuerdos, y emitir las instrucciones generales, resoluciones y lineamientos fundamentales que permitan a los regulados adecuarse a la nueva normativa. La magnitud y complejidad de tales tareas como las descritas en la tabla, requiere un proceso técnico, en algunos casos participativo y

escalonado, que no puede ser comprimido en tan breve lapso sin afectar la calidad regulatoria ni la legitimidad de las decisiones. En consecuencia, no solo se compromete la eficacia del modelo institucional, sino que se vulnera el principio de seguridad jurídica, al exigir cumplimiento en un escenario de incertidumbre regulatoria y sin instrumentos habilitantes básicos.

A partir del 1º de diciembre de 2026, la Agencia de Protección de Datos Personales se encontrará plenamente habilitada por mandato legal para recibir denuncias, reclamaciones, solicitudes y otros requerimientos en el marco de la Ley N° 19.628. Conforme al principio de inexcusabilidad consagrado en el artículo 14 de la Ley N° 19.880, la APDP estará obligada a dictar resolución expresa en todos los procedimientos, cualquiera sea su forma de iniciación. En ese sentido, la falta de preparación institucional, de estatutos internos, de procedimientos y de normativa operativa básica impediría a la Agencia cumplir con su obligación legal de pronunciarse sobre las materias sometidas a su conocimiento, generando un riesgo de incumplimiento desde el día uno de su funcionamiento. La imposibilidad de atender requerimientos por falta de preparación o de criterios técnicos infringe directamente dicho principio, afectando la confianza legítima de los ciudadanos y la seguridad jurídica de los regulados, pudiendo configurar responsabilidad administrativa por omisión del deber de resolver.

IV. ANÁLISIS PRESUPUESTARIO

La implementación efectiva de la Agencia de Protección de Datos Personales se ve seriamente comprometida por la insuficiencia de los recursos previstos en su informe financiero. El presupuesto asignado para su primer año de funcionamiento asciende apenas a $1.721 millones, y en régimen se reduce incluso a $1.660 millones, cifras significativamente inferiores a cualquier otro órgano regulador con estructuras comparables.

Concepto/Años (Miles $2021)	Año 1	Régimen
Gastos en Personal	989.247	1.367.831
Gastos en Operación	188.088	292.250
Inversión Inicial	464.565	
Terna ADP	79.100	
Total	**1.721.000**	**1.660.081**

A modo comparativo, el Consejo para la Transparencia (CPLT) cuenta con $8.585 millones de presupuesto anual y 138 funcionarios; el Servicio Nacional del Consumidor (SERNAC), con $18.919 millones y una dotación máxima de 420 funcionarios, por mencionar algunos. La Agencia se instalaría con una propuesta de dotación inicial de sólo 19 funcionarios y una planta en régimen de 30 funcionarios más tres Consejeros. Este diseño estructural resulta abiertamente insuficiente para cumplir con los mandatos legales.

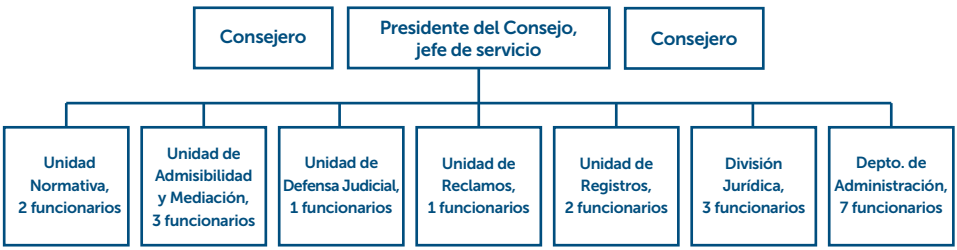
A ello se suma un problema mayor, respecto de las remuneraciones de este nuevo organismo fiscalizador. Esta Comisión de Implementación, considerando datos que han sido facilitados por la Contraloría General de la República, ha analizado las remuneraciones brutas del año 2024 de órganos similares, publicadas en los respectivos portales de transparencia de las siguientes instituciones: la Comisión para el Mercado Financiero, Dirección del Trabajo, SERNAC, Superintendencias de Casinos de Juego; de Educación; de Educación Superior; de Electricidad y Combustibles; de Insolvencia y Reemprendimiento; de Pensiones; de Salud; de Seguridad Social; de Servicios Sanitarios; y del Medio Ambiente. De acuerdo a lo publicado, el promedio del ingreso bruto mensual de los jefes superiores de servicio es de $12 millones, según información consolidada al 23 de junio de 2025. Para la Agencia de Protección de Datos, la Ley previó remuneraciones brutas proyectadas, para el presidente del Consejo, de $7,1 millones, y de $6 millones para los consejeros, las que se encuentran por lejos muy por debajo del promedio de jefaturas de servicio de organismos fiscalizadores comparables.

Esta brecha se vuelve aún más crítica al considerar que los cargos del Consejo Directivo implican dedicación exclusiva, están sujetos a un estricto régimen de inhabilidades y requieren altos niveles de independencia técnica y probidad. Esta situación no solo vuelve poco atractiva la integración de perfiles con la experiencia profesional requerida, sino que también debilita la autonomía institucional y eleva el riesgo de captura regulatoria. La desproporción entre el mandato legal y los medios asignados compromete gravemente la eficacia, legitimidad y sostenibilidad institucional del nuevo órgano garante en protección de datos personales.

Unidad/División	Año 1		Régimen	
	N° Funcionarios	Remuneración	N° Funcionarios	Remuneración
Consejo Directivo	**3**	**278.736**	**3**	**278.736**
Personal Agencia	**19**	**710.511**	**30**	**1.089.095**
Unidad Normativa	2	91.527	2	91.527
Unidad de Admisibilidad y Mediación	3	112.132	4	139.605
Unidad de Defensa Judicial	1	27.473	2	84.659
Unidad de Reclamos	1	27.473	3	108.142
Unidad de Registros	2	71.966	2	71.966
División Jurídica	3	142.360	5	217.741
Departamento de Administración	7	237.580	12	375.455
Total	**22**	**989.247**	**33**	**1.367.831**

El informe financiero que acompaña el proyecto de Ley consideró un organigrama base que no se ajusta a las funciones esenciales que la normativa asigna a la Agencia de Protección de Datos Personales. En particular, omite estructurar adecuadamente dos competencias centrales: la función fiscalizadora y el área encargada de la certificación de modelos de prevención y programas de

cumplimiento. Ambas requieren unidades técnicas especializadas, con personal capacitado, procedimientos definidos y recursos suficientes para operar, considerando que la Agencia tendrá competencia sobre todos los sectores económicos y organismos públicos y privados.



Organigrama previsto en el Informe Financiero. Elaboración propia.

El presupuesto y dotación prevista en el informe financiero se traducen en la carencia de una estructura adecuada para ejercer sus funciones, en particular, la fiscalización y la certificación de modelos de prevención, limitando gravemente la capacidad de la Agencia para prevenir, detectar y sancionar infracciones en el tratamiento de datos personales. Esta debilidad estructural no solo afecta la eficacia del control sino que también impide el desarrollo de mecanismos de cumplimiento preventivo, como los programas de autorregulación y buenas prácticas que deben ser promovidos y supervisados por la Agencia. Además, una dotación insuficiente restringe la capacidad de respuesta ante denuncias de titulares, el ejercicio oportuno de la potestad sancionatoria, y el desarrollo de orientaciones técnicas para los regulados.

V. COMPARATIVA CON OTRAS AGENCIAS DE PROTECCIÓN DE DATOS PERSONALES

Esta Comisión revisó y comparó a la APDP chilena con sus pares de España (Agencia Española de Protección de Datos - AEPD), Reino Unido (Information Commissioner's Office - ICO) y Francia (Commission nationale de l'informatique et des libertés - CNIL), a las que directamente les es aplicable el GDPR de la UE; las agencias de Argentina (Agencia de Acceso a la Información Pública) y Uruguay (Unidad Reguladora y de Control de Datos Personales), países considerados adecuados para la transferencia internacional de datos por la Comisión Europea; y las nuevas agencias de Ecuador (Superintendencia de Protección de Datos Personales) y Brasil (Autoridade Nacional de Proteção de Dados), países que recientemente, al igual que Chile, actualizaron su marco regulatorio en materia de protección de datos personales alineándose con el GDPR. A partir de este análisis, la Comisión concluyó que la APDP, en términos generales, comparte las mismas obligaciones, responsabilidades y facultades, por tanto, tendrá una anticipable y similar carga de trabajo.

Sin embargo, se identifican algunas brechas muy específicas entre las facultades de la APDP en comparación con sus homólogas:

1. No poseería facultades expresas para inspeccionar y realizar por sí misma o externalizar la realización de auditorías en protección de datos personales.

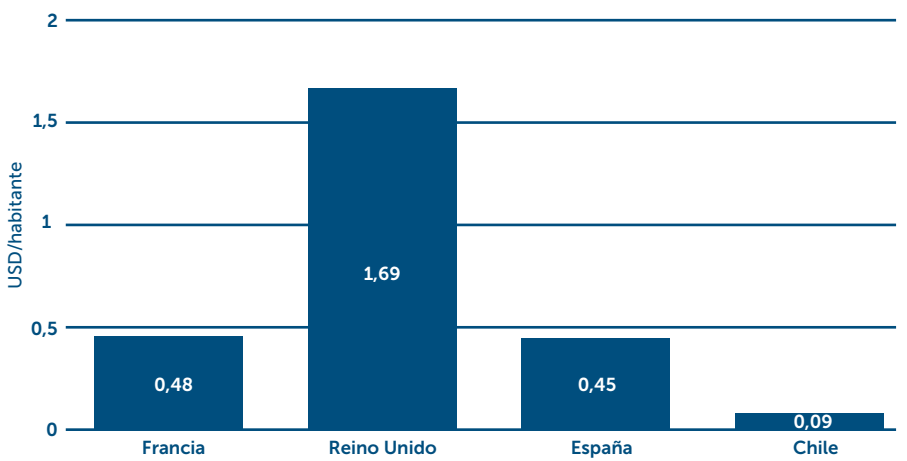
2. Asimismo, se identifica que el rol colaborativo u orientador de la APDP es menos explícito (ej. facultades para dictar orientaciones; guías; etc. para facilitar el cumplimiento de la Ley por parte de los responsables; aprobar códigos de conducta; etc.).

3. Una de las brechas más relevantes es que la APDP será la única entidad facultada para certificar los modelos de prevención de infracciones en Chile. A nivel internacional (España, Francia, Reino Unido, Ecuador) esta función de certificación puede ser externalizada a entidades acreditadas por la autoridad de control para certificar esquemas de estándares o códigos de conducta. Que la APDP sea la única entidad en Chile capaz de certificar aumentará notablemente su carga de trabajo y demandará una mayor cantidad de recursos.

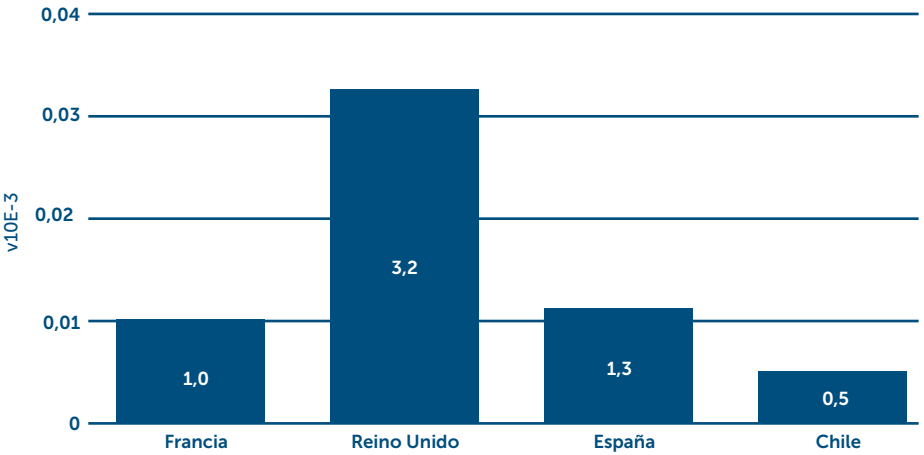
El presupuesto de la APDP es bastante inferior en comparación a las agencias fiscalizadoras homólogas analizadas (generalizado en US$):

Agencia	País	Presupuesto Agencias	Presupuesto Agencias USD	Población	PIB USD (Miles)	Presupuesto Agencias por Población (USD/ habitante)	Presupuesto Agencias como porcentaje del PIB (PIB%) X10E-3
CNIL (FR)	Francia	28,2 millones de Euros	32.851.817	68.516.700	3.162.079.070,0	0,48	1,0%
ICO (UK)	Reino Unido	£ 87,3 millones	116.789.298	69.226.000	3.643.834.190,0	1,69	3,2%
AEPD (ES)	España	18,7 millones de Euros	21.784.716	48.807.140	1.722.745.980,0	0,45	1,3%
APDP	Chile	1721 millones de CLP	1.780.136	19.764.770	330.267.400,0	0,09	0,5%

Presupuesto Agencias por Población (USD/habitante). Elaboración propia.



Presupuesto Agencias como porcentaje del PIB. Elaboración propia.



Habiendo revisado el presupuesto anterior y comparativo de agencias homólogas, el presente apartado tiene como objetivo presentar una propuesta para la Agencia de Protección de Datos Personales chilena, considerando un equipo inicial de 50 funcionarios y 3 Consejeros. Esta propuesta está diseñada para cumplir eficazmente con las funciones asignadas por la Ley N°21.719. El modelo propone un equilibrio entre las funciones fiscalizadoras, jurídicas y las tareas de educación y promoción de derechos. Se reconoce que la instalación de una nueva normativa requiere no solo control, sino también un esfuerzo sistemático y sostenido por educar a la ciudadanía, sensibilizar a los responsables del tratamiento de datos y construir una cultura de cumplimiento voluntario. Por ello, esta propuesta asigna una proporción significativa de recursos a la Unidad de promoción y educación.

Consejo Directivo (4 funcionarias/os) • Funcionamiento (2 funcionarias/os) • Comunicaciones (2 funcionarias/os) **Unidad Jurídica** (10 funcionarias/os) • Asesoría jurídica, procedimientos sancionatorios. • Normativa, consuktas y resolución de conflictos. **Unidad Fiscalización** (8 funcionarias/os) • Supervisión, auditorías y controles. • Investigaciones y aplicación de sanciones. **Unidad de Administración y Servicios** (10 funcionarias/os) • Gestión administrativa, financiera y de recursos humanos. • Apoyo logístico institucional.	**Unidad de promoción y educación** (12 funcionarias/os) • Campañas educativas masivas y programa de concientización. • Formación continua en materia de protección de datos. • Coordinación estratégica con organismos públicos y privados. • Genración de contenidos educativos y recursos digitales. **Unidad Jurídica** (4 funcionarias/os) • Administración del registro de cumplimiento. • Análisis especializado en tecnoñogías emergentes.

La propuesta considera un presupuesto en gasto en personal de 3.157 millones de pesos en régimen, lo que representa casi el doble de los recursos consignados en el informe financiero.

Se considera un mínimo de 50 funcionarios, para el cumplimiento de labores esenciales de la Agencia señaladas en la Ley, de los cuales 5 son directivos y 45 son funcionarios de las distintas áreas. Adicionalmente, se consideran las 3 autoridades, con remuneraciones propuestas por esta Comisión de acuerdo a la Escala Fiscalizadora.

Concepto	N°	Año 1
Gastos en Personal	**53**	*$3.157.546.896*
Consejo Directivo - Presidente	*1*	*$162.000.000*
Consejo Directivo - Consejeros	*2*	*$288.000.000*
Funcionarios Consejo	*4*	*$193.767.648*
Directivos	*5*	*$420.000.000*
Dirección Jurídica y Normativa	*9*	*$473.533.344*
Dirección de Fiscalización	*7*	*$409.198.104*
Dirección de Administración y Servicios	*11*	*$532.861.032*
Dirección de Promoción y Educación	*11*	*$532.861.032*
Dirección de Registro y Auditoría	*3*	*$145.325.736*

En términos de gastos operacionales, también se considera que el informe financiero es insuficiente para el funcionamiento mínimo de la APDP. Se toma como referencia, el funcionamiento de oficinas en un piso arrendado en el barrio cívico de Santiago, para lo que se requiere considerar 351 millones de pesos.

Gastos en Operación	$351.904.242
Arriendo	*$155.660.000*
Servicios	*$82.200.000*
Gastos operacionales	*$32.924.242*
Licencias computacionales	*$81.120.000*

En materia de inversión inicial, para la instalación de la APDP, se consideran recursos adicionales para: la creación de una plataforma informática, de tipo transaccional, para el cumplimiento de las funciones principales de la Agencia; y recursos para la promoción del derecho: difusión y capacitación.

Inversión Inicial	$590.368.000
Vehículos	*$55.028.000*
Mobiliario	*$15.490.000*
Programas computacionales	*$90.000.000*
Equipos Informáticos	*$56.350.000*
Máquinas y equipo	*$23.500.000*
Plataforma y sistema PDP	*$250.000.000*
Campañas difusión y capacitación	*$100.000.000*

En general, se propone un presupuesto mínimo, para el primer año de funcionamiento de la APDP, de 4.178 millones de pesos.

Concepto	Año 1 (Miles $2035)
Gastos en Personal	*$3.157.546*
Gastos en Operación	*$351.904*
Inversión Inicial	*$590.368*
Terna ADP	*$79.100*
Total	***$4.178.918***

Finalmente se propone que las remuneraciones de las autoridades de la APDP puedan sean más altas, por equivalencia con responsabilidades y obligaciones de autoridades de otros organismos comparables. Esto permitiría también, que las remuneraciones de los directivos tengan equivalencia con cargos similares de la administración.

VI. CONCLUSIONES Y RECOMENDACIONES

A la luz del análisis desarrollado, esta Comisión identifica una serie de debilidades estructurales y normativas que comprometen la correcta instalación y el funcionamiento eficaz de la Ley y de la Agencia de Protección de Datos Personales, que pueden comprometer el régimen de protección de datos en Chile. El soporte financiero y organizacional previsto resultan insuficientes para dar cumplimiento oportuno y efectivo a los mandatos básicos que la Ley impone. En este contexto, la Comisión recomienda una serie de medidas correctivas que permitan dotar a la Agencia de las capacidades reales para ejercer su rol garante y cumplir con el estándar de protección de datos personales exigido por la nueva legislación, todas las que deberían ejecutarse vía Ley de Presupuestos 2026 o Ley de reajuste del sector público del mismo año.

1. Anticipar la instalación de la Agencia a más tardar al mes de junio de 2026. En vista de las tareas que la Agencia debe realizar para una adecuada entrada en vigencia de la Ley, es indispensable anticipar su instalación y, por consiguiente, la designación de su Consejo Directivo, a más tardar al mes de junio de 2026, con el fin de permitir una instalación institucional progresiva, técnicamente fundada y operativamente viable. Esto implicaría que en esa fecha deberían asumir los consejeros y un staff inicial de apoyo a sus funciones. El calendario actual es manifiestamente insuficiente para cumplir con los mandatos preparatorios esenciales, tales como la contratación inicial e instalación del personal clave, la elaboración y

aprobación de las instrucciones generales y resoluciones urgentes, y la habilitación de canales de atención y resolución. Este adelanto permitiría a la Agencia y al staff inicial comenzar a ejecutar etapas preparatorias y procesos administrativos previos mencionados en este informe, permitiendo así una transición ordenada y evitando vacíos regulatorios que afecten la seguridad jurídica de los titulares y de los regulados. Asimismo, se alinea con el principio de inexcusabilidad, que impone a los órganos administrativos la obligación de resolver todo requerimiento desde el momento en que entran en funciones.

2. Fortalecimiento institucional urgente, lo que requiere ser reflejado en la Ley de Presupuestos 2026. La actual dotación de recursos humanos y financieros de la AGPD es insuficiente para asumir las funciones sustantivas asignadas por la Ley N° 21.719, en particular las relativas a fiscalización, tramitación de reclamos, dictámenes normativos y coordinación internacional. Se propone una

dotación inicial transitoria durante los meses de junio a diciembre para instalar y poner en funcionamiento la Agencia, lo que implicaría un 30 a 40% del presupuesto inicial proyectado propuesto por esta Comisión, y una dotación en régimen conforme a las estimaciones incluidas en este informe.

3. Equiparar la escala de remuneraciones del presidente y consejeros del Consejo Directivo. Es indispensable que en la misma discusión de la Ley de Presupuestos 2026 o en la Ley de Reajuste del Sector Público para 2026, se modifiquen las escalas remuneracionales previstas para el presidente y los consejeros del Consejo Directivo de la Agencia, a fin de que sean coherentes y alineadas con las exigencias de dedicación exclusiva que es exigida, el alto estándar técnico requerido y el estricto régimen de inhabilidades al que estarán sujetos. Las remuneraciones proyectadas, actualmente de $7,1 millones brutos para el presidente, y de $6 millones para los consejeros, se sitúan muy por debajo del promedio de jefaturas de servicio de organismos fiscalizadores y reguladores comparables, como la CMF, la FNE o las superintendencias en nuestro país, cuyos niveles superan los $12 millones brutos mensuales. Esta Comisión propone establecer una remuneración equiparable a sus homólogos fiscalizadores chilenos, de 12 millones de pesos para los Consejeros y 13.5 millones para el Presidente. Mantener la brecha afectará la capacidad de atraer perfiles idóneos e independientes, y debilitará la autonomía técnica de la Agencia. Una escala adecuada y competitiva no solo resguarda la calidad del órgano colegiado, sino que contribuye a prevenir riesgos de captura regulatoria y asegura el cumplimiento efectivo del mandato legal de la entidad, considerando especialmente la capacidad económica de los regulados.

4. Estrategia de instalación colaborativa desde inicios de 2026. Dada la complejidad y alcance del mandato legal de la Agencia de Protección de Datos Personales, se recomienda implementar una estrategia de instalación colaborativa desde inicios de 2026, liderada por el Ministerio de Economía, Fomento y Turismo (MINECON), con apoyo del Servicio Civil, DIPRES y otras entidades pertinentes. Esta estrategia debiera incluir, entre otras medidas:

> La ejecución temprana de procesos logísticos como el arriendo de oficinas, adquisición de equipamiento y habilitación de sistemas de gestión documental y registro;
> El inicio del diseño de los perfiles de cargo y bases de concurso para la dotación funcional, en coordinación con el Servicio Civil y conforme a las competencias requeridas. Esta fase preparatoria permitiría reducir los tiempos de puesta en marcha efectiva, garantizar continuidad operativa desde la entrada en vigencia de la Ley, y evitar la parálisis institucional que podría derivarse de una implementación tardía o improvisada.
> La creación anticipada del sitio web institucional, permitiría informar al público, habilitar canales de contacto y transparencia activa desde el primer día;

5. Centralidad de un presupuesto aceptable. Este es un elemento estructural para el éxito del nuevo modelo regulatorio. La magnitud del mandato conferido a la Agencia exige capacidades humanas, técnicas y materiales proporcionales. En este contexto, la ampliación presupuestaria es una condición habilitante para que el nuevo régimen de protección de datos personales sea operativo, eficaz y creíble. Sin esta base mínima de sostenibilidad financiera, cualquier intento de implementación se verá limitado en su alcance.

2° INFORME

RECOMENDACIONES RELATIVAS AL TRÁFICO TRANSFRONTERIZO.

SEGUNDO INFORME DE LA COMISIÓN DE IMPLEMENTACIÓN PARA LA LEY DE PROTECCIÓN DE DATOS PERSONALES. RECOMENDACIONES RELATIVAS AL TRÁFICO TRANSFRONTERIZO. 01 DE SEPTIEMBRE DE 2025

I. INTRODUCCIÓN

En un escenario de creciente interdependencia global y de acelerada transformación digital, las transferencias internacionales de datos personales constituyen un eje estratégico para la competitividad y el desarrollo de la economía digital. La capacidad de Chile para insertarse en cadenas de valor digitales, fomentar la innovación y asegurar la confianza de inversionistas y socios comerciales dependerá en gran medida de contar con reglas claras, seguras y alineadas con estándares internacionales. En ese contexto, la Comisión de Implementación de la Ley N° 21.719 identifica un conjunto de recomendaciones críticas para garantizar la seguridad jurídica y la operatividad efectiva de los mecanismos de transferencia internacional de datos personales, antes de la entrada en vigor de la nueva normativa.

En síntesis, las recomendaciones se orientan a lo siguiente:

1. Aprobación de cláusulas contractuales tipo antes de diciembre de 2025.
2. Aprobación de normas corporativas vinculantes presentadas por las Empresas por parte del Ministerio de Economía o la autoridad que se considere competente
3. Declaración de países que proporcionen niveles adecuados de protección de datos personales, de conformidad con el Artículo 28 de la Ley.
4. Explorar flujos de transferencia internacionales de datos con Estados Unidos y otros socios comerciales APEC, mediante un estudio independiente que determine las vías de cumplimiento ante el nuevo régimen legal chileno.
5. Iniciar los trámites de reconocimiento de Chile como país adecuado por la UE.
6. Iniciar el proceso de adhesión al Convenio 108+ del Consejo de Europa

II. CONTEXTO

Durante la discusión de la Ley N° 21.719 (2024), especialmente en su segundo trámite constitucional en la Cámara de Diputadas y Diputados, se explicitó como uno de los objetivos estratégicos de la reforma alinear la normativa chilena con el Reglamento General de Protección de Datos de la Unión Europea (GDPR). Esta orientación fue concebida con el objetivo de que el país obtuviera una decisión de adecuación por parte de la Unión Europea, lo que permitiría el flujo de datos personales desde los Estados miembros de ese bloque económico a Chile sin necesidad de recurrir a garantías adicionales. Para alcanzar este objetivo, la ley chilena incorporó principios sustantivos equivalentes al GDPR, tales como licitud en el tratamiento, finalidad, proporcionalidad en la recolección y uso de datos, exactitud, transparencia, seguridad mediante medidas técnicas y organizativas, y responsabilidad. Asimismo, se reconocieron derechos fundamentales de los titulares de datos personales como: acceso, rectificación, supresión, oposición, portabilidad, limitación del tratamiento y el derecho a no ser objeto de decisiones automatizadas con efectos jurídicos o significativos sin intervención humana. Una declaración de Chile como país adecuado constituye una importante señal de mercado a nivel global. Cualquier empresa chilena podrá exhibir entre sus credenciales el estándar de país adecuado, lo que atraerá demanda de servicios desde jurisdicciones que no cuentan con ese

nivel de protección, pero que necesitan demostrar compromiso con la privacidad frente a sus propios clientes. Esto se traducirá en una nueva ventaja competitiva para Chile.

Por su parte, el reciente Informe sobre Barreras al Comercio Exterior elaborado por la Oficina del Representante Comercial de Estados Unidos (USTR), que sirvió de base para decisiones en política comercial según declaraciones de la Casa Blanca, realizó una mención explícita a la Ley N° 21.719 sobre Protección de Datos Personales. En particular, se refiere a los requisitos aplicables al flujo transfronterizo de datos personales, regulados en los artículos 27 y 28 de la nueva ley.

El informe reconoce que la normativa chilena exigirá que los países receptores de datos personales cuenten con niveles de protección adecuados o similares a los vigentes en Chile, y que mientras no existan decisiones de adecuación dictadas por la autoridad nacional, las transferencias deberán sustentarse en cláusulas contractuales tipo previamente aprobadas por esta. En este contexto el informe señala que "Los actores estadounidenses han expresado preocupación porque las directrices para el uso de estas cláusulas contractuales no son claras, y la falta de definiciones precisas para conceptos clave está generando incertidumbre para las empresas." El informe pone el foco en un diagnóstico compartido, la ausencia de definiciones operativas, orientaciones técnicas y herramientas regulatorias anteriores a la entrada en vigencia de la ley que permitan a las empresas cumplir con certeza jurídica las nuevas exigencias legales.

La Comisión Asesora considera que resulta altamente improbable que una autoridad que comience su instalación en octubre de 2026 cuente con el tiempo suficiente para desarrollar y aprobar instrumentos clave —como las cláusulas contractuales estándar o el listado de jurisdicciones adecuadas— antes del 1º de diciembre de ese mismo año, momento desde el que los responsables de datos que realicen operaciones de transferencia internacional de datos personales deberán comenzar a dar cumplimiento a los requisitos que la ley establece para tales operaciones de tratamiento. Este desfase normativo en transferencias internacionales de datos personales genera incertidumbre jurídica, fricciones comerciales y pérdida de competitividad para Chile en los mercados digitales globales.

III. METODOLOGÍA DE TRABAJO

La Comisión recibió y analizó diversas opiniones y propuestas provenientes de autoridades del sector de Relaciones Exteriores, representantes de otras jurisdicciones y especialistas en la materia. En particular, se contó con la participación de la señora Gloria de la Fuente, Subsecretaria de Relaciones Exteriores; el Embajador Luis Plaza; la señora Claudia Godoy, Asesora de Gabinete de la Subsecretaría de Relaciones Exteriores; el señor Luis Serrano, abogado de la Dirección General de Asuntos Jurídicos del Ministerio de Relaciones Exteriores; el señor Felipe Núñez, abogado de la misma Dirección General; la señora Tania Pierotic, Jefa del Departamento de Inversiones, Servicios y Economía Digital del Ministerio de Relaciones Exteriores; y el señor Piero Guasta, profesional del mismo Departamento.

Asimismo, se contó con la intervención telemática de la señora Estelle Masse, Policy Officer de la Unidad de Asuntos Internacionales y Flujos Transfronterizos de la Dirección General de Justicia de la Comisión Europea, la señora Dolores Dozo, experta para Latinoamérica en el marco del proyecto

Enhanced Data Protection and Data Flows de la Unión Europea y la titular de la Agencia de Acceso a la Información Pública de Argentina, doña Beatriz Anchorena. También participaron, en modalidad telemática, el señor Pablo Palazzi, experto de la Red Iberoamericana de Protección de Datos; el señor Jacobo Esquenazi, Data Protection Officer de HP Inc.; el señor Luis Montezuma, International Data Spaces Facilitator de HP Inc.; y el señor Guillermo Ortiz, BCR & Data Transfers Lead de HP Inc.

IV. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES EN LA NUEVA LEY DE PROTECIÓN DE DATOS

Las transferencias internacionales de datos personales corresponden a operaciones mediante las cuales la información de una persona sale del país en que fue recolectada para ser enviada o puesta a disposición de un destinatario ubicado en otra jurisdicción. Este concepto abarca tanto el envío activo de datos (por ejemplo, el traspaso de una base de datos a una filial extranjera) como el acceso remoto desde el extranjero a información almacenada localmente.

La regulación de estas transferencias resulta necesaria porque, al abandonar el territorio nacional, los datos quedan sujetos a leyes y prácticas distintas, que pueden ofrecer un nivel de protección inferior al garantizado en el país de origen, afectando los derechos y libertades de las personas.

En este marco la nueva regulación busca conseguir los siguientes objetivos:

a) Mantener el nivel de protección: Asegurar que, incluso fuera de Chile, se respeten los principios y derechos reconocidos en nuestra normativa.

b) Prevenir riesgos para los titulares: Reducir la exposición a accesos no autorizados, usos indebidos, vigilancia masiva o tratamientos discriminatorios en jurisdicciones con estándares débiles, incluyendo la limitación de accesos desproporcionados por parte de autoridades extranjeras que puedan afectar la privacidad y otros derechos fundamentales. Del mismo modo, evitar mecanismos de elusión al cumplimiento de la legislación nacional, a través de la exportación y reimportación de datos personales.

c) Exigir garantías adecuadas: Obligar a que el receptor extranjero adopte compromisos jurídicamente vinculantes y mecanismos efectivos de cumplimiento (como contratos, cláusulas modelo o certificaciones) que permitan a los titulares ejercer sus derechos y obtener remedios efectivos.

d) Fomentar la confianza y el comercio internacional: Permitir que los flujos transfronterizos de datos se desarrollen bajo estándares confiables, facilitando operaciones globales sin sacrificar derechos fundamentales.

1. Elementos de atención en el intercambio transfronterizo de datos.

a) Chile como exportador de datos personales

Cuando datos personales recolectados en Chile se transfieren al extranjero, lo crucial es cómo evaluamos las jurisdicciones receptoras. La legislación nacional exige que estas jurisdicciones ofrezcan estándares de protección similares o superiores a los chilenos, de modo que los titulares no

vean disminuido su nivel de resguardo al salir la información del país (Art 28 inc. 1). Esto supone analizar:

> Las leyes vigentes en el país de destino.
> La existencia de garantías efectivas para ejercer derechos y resarcir perjuicios.
> Los mecanismos contractuales, certificaciones u otros instrumentos que aseguren el cumplimiento.
> La existencia de una autoridad encargada de la protección de datos personales.

b) Chile como importador de datos personales

Cuando Chile recibe datos personales desde el extranjero, el foco se desplaza a la evaluación que realizan otras jurisdicciones sobre nuestro marco normativo. En este escenario, para Chile resulta indiferente el estándar de protección de la jurisdicción exportadora; lo que importa es que dicho país nos considera aptos para recibir sus datos personales, evaluando, de ser el caso, si nuestro sistema legal ofrece garantías equivalentes a las que su propia normativa exige.

> Aquí el desafío es lograr que Chile sea reconocido como un país con nivel adecuado de protección, con el fin de facilitar el flujo de datos y el comercio internacional.
> Por tanto, la atención debe centrarse en la percepción externa de nuestro marco regulatorio y en las acciones necesarias para obtener reconocimientos de adecuación o equivalencia (por ejemplo, ante la Unión Europea u otros socios estratégicos).

2. Licitud de las transferencias internacionales bajo la ley chilena.

La normativa nacional establece que las transferencias internacionales de datos personales sólo pueden realizarse cuando existan garantías suficientes para mantener el nivel de protección similar o superior al reconocido en Chile. Estas garantías se estructuran en dos vías principales:

a) Decisión de adecuación (art. 27a, 28 inc. 1)

> La Agencia de Protección de Datos podrá declarar que un país extranjero ofrece un nivel adecuado de protección.
> Se entiende que un país cumple con este requisito cuando sus estándares son similares o superiores a los fijados en la legislación chilena.
> En estos casos, la transferencia se autoriza sin necesidad de condiciones adicionales.

b) Garantías adecuadas (art. 27b, c; 28 inc. 2 y ss.)

Cuando no exista una decisión de adecuación, las transferencias podrán realizarse siempre que el responsable o encargado del tratamiento ofrezca garantías adecuadas. Se consideran garantías adecuadas aquellos instrumentos, mecanismos o cláusulas que contengan similares o mayores principios, derechos y garantías a aquellas que ofrece la ley chilena, y en particular, que otorguen derechos exigibles y acciones legales efectivas a los titulares de los datos. Éstas garantías pueden materializarse en alguno de los siguientes instrumentos:

> Cláusulas contractuales modelo (CCM), previamente aprobadas por la Agencia, que establezcan obligaciones vinculantes para el exportador e importador de datos.
> Normas corporativas vinculantes (BCRs), aplicables a grupos empresariales o conglomerados, que deberán contar con aprobación previa de la Agencia.
> Modelos de cumplimiento o mecanismos de certificación reconocidos por la Agencia,

siempre que incluyan disposiciones suficientes para garantizar la protección de los datos transferidos.

> Autorización caso a caso por la Agencia, aplicable a transferencias específicas, siempre que se ofrezcan garantías adecuadas.

De este modo la regla general señala que las transferencias internacionales de datos requieren una evaluación previa del nivel de protección en el país de destino o, en su defecto, la implementación de garantías jurídicas y organizativas que aseguren el respeto de los estándares chilenos.

c) Excepciones

En ausencia de una decisión de adecuación o de garantías adecuadas, la ley permite únicamente transferencias específicas y no habituales de datos personales, siempre que se enmarquen en alguno de los supuestos del art. 27 inc. 2, letras a–h.

V. RECOMENDACIONES DE LA COMISIÓN

Con el objeto de facilitar la implementación temprana de los mecanismos de transferencia internacional de datos personales previstos en la Ley N° 21.719, y con el fin de brindar seguridad jurídica al momento de entrada en vigencia de la ley recomendamos dictar, a más tardar diciembre de 2025, los actos administrativos necesarios para dar fluidez y certeza a las transferencias internacionales de datos dentro de los siguientes ámbitos:

1. Aprobación de cláusulas contractuales modelo o tipo

Como pudo revisar esta Comisión, la Red Iberoamericana de Protección de Datos (RIPD) elaboró y aprobó Cláusulas Contractuales Modelo con el objetivo de facilitar el tráfico transfronterizo de datos personales em América Latina entre organizaciones que las adopten. Su objetivo es promover la convergencia de estándares de protección a nivel contractual, creando un régimen autónomo de protección de datos, sin requerir necesariamente la armonización normativa entre los países participantes. De esta forma, en algunos aspectos,

incluso pueden ofrecer un nivel de protección superior al exigido en ciertas legislaciones nacionales. Desarrollaron dos modelos de cláusulas:

1. Responsable a Responsable (R>R): para transferencias entre dos responsables del tratamiento.
2. Responsable a Encargado (R>E): para transferencias de un responsable a un encargado del tratamiento.

Estos dos modelos de cláusulas guardan similitud en su estructura y principios con dos módulos de cláusulas contractuales tipo de la Unión Europea aprobadas por la Comisión en junio de 2021 (Decisión de Ejecución (UE) 2021/914), aunque no consideran los módulos de transferencias de encargado del tratamiento a subencargado del tratamiento, y transferencias de encargado del tratamiento a responsable del tratamiento. En lo esencial, comparten los mismos elementos y principios, lo que favorece su reconocimiento no solo a nivel regional, sino también en Europa y en países declarados adecuados por la UE. Las cláusulas y su marco de aplicación se encuentran recogidas en la "Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia

Internacional de Datos Personales" y en su anexo correspondiente. Han sido reconocidas expresamente por Uruguay, Argentina, Ecuador y Perú, por mencionar algunos.

Se recomienda que el Ministerio de Economía, Fomento y Turismo, en ejercicio de la potestad que le otorga el decreto N° 747, que Aprueba el reglamento orgánico de la Subsecretaría de Comercio e Industrias del Ministerio de Economía, y el artículo 1° del DFL N° 88 de 1953, apruebe, antes de la entrada en vigencia de la Ley, las cláusulas contractuales tipo en materia de transferencias internacionales de datos personales siguiendo el modelo de la Red Iberoamericana de Protección de Datos (RIPD) y otras cláusulas modelos de reconocido estándar y aceptación. Dichas cláusulas podrán ser ratificadas, modificadas o incluso descartadas por la Agencia de Protección de Datos Personales una vez que ésta entre en funciones, en atención a que dentro de sus atribuciones se encuentra precisamente su aprobación. No obstante, se espera que, en el período intermedio hasta la plena entrada en vigor de la Agencia, dichas cláusulas otorguen certeza y estabilidad jurídica, evitando que sean desconocidas o dejadas sin efecto.

2. Aprobación de Normas Corporativas Vinculantes

Se recomienda que el Ministerio de Economía, o la autoridad que se estime competente, apruebe las normas corporativas vinculantes que sean presentadas por los grupos empresariales sujetos a ellas. Dichas normas podrán ser posteriormente ratificadas, modificadas o incluso descartadas por la Agencia de Protección de Datos Personales, una vez que ésta entre en funciones, considerando que entre sus atribuciones se encuentra precisamente su aprobación. Sin perjuicio de lo anterior, resulta esperable que, durante el período intermedio hasta la plena entrada en vigencia de la Agencia, dichas aprobaciones otorguen certeza y estabilidad jurídica, evitando que posteriormente sean desconocidas o dejadas sin efecto

3. Avanzar en la declaración de países que proporcionen niveles adecuados de protección de datos personales desde Chile, en conformidad con el Artículo 28 de la Ley.

Esta Comisión sugiere que el Ministerio de Relaciones Exteriores o la autoridad competente estudie y, eventualmente apruebe, con anterioridad a la entrada en vigor de la Ley, un listado de países declarados como adecuados por proporcionar niveles suficientes de protección de datos personales, de conformidad con el inciso segundo del artículo 28 de la ley. Dicho listado podrá ser posteriormente ratificado, modificado o incluso descartado por la Agencia de Protección de Datos Personales, una vez que ésta entre en funciones, considerando que entre sus atribuciones se encuentra precisamente esta determinación. Sin perjuicio de lo anterior, resulta esperable que, durante el período intermedio hasta la plena entrada en vigencia de la Agencia, dichas declaraciones otorguen certeza y estabilidad jurídica, evitando que posteriormente sean desconocidas o dejadas sin efecto.

Este análisis podrá incluir, entre otros:

> Estados parte del Espacio Económico Europeo;
> Países que ya han sido reconocidos como adecuados por la UE;
> Países con los cuales la UE cuente con instrumentos de intercambio de datos personales;
> Países socios estratégicos de Chile, con el objeto de mantener y promover el comercio internacional.

Estas medidas permitirían contar, desde el inicio de la aplicación de la ley, con instrumentos y determinaciones que faciliten el flujo internacional de datos personales sin menoscabo de los derechos de los titulares residentes en territorio nacional.

4. Explorar mecanismos de transferencia de datos con EE. UU, principal socio comercial de nuestro país y países miembros del Foro APEC.

La Comisión considera de importancia estratégica la relación con los Estados Unidos como socio comercial relevante y, en ese sentido, resalta la utilidad de las cláusulas contractuales tipo propuestas en la primera recomendación para facilitar las transferencias internacionales de datos personales en el período intermedio.

Asimismo, sugiere explorar mecanismos de certificación internacionales, tales como el sistema CBPR, encargando un informe jurídico independiente que evalúe su compatibilidad con el nuevo régimen legal chileno. Se recomienda analizar este esquema de certificación a fin de determinar su viabilidad y ajuste a las exigencias de flujo transfronterizo de datos del nuevo marco jurídico nacional, procurando no soslayar la nueva normativa de protección de datos personales y que se mantengan los estándares previstos en ella.

Finalmente, la Comisión estima que, en caso de buscarse un mecanismo de adecuación específico para las transferencias de datos personales con los Estados Unidos, éste podría eventualmente estructurarse, entre otras formas, considerando una fórmula análoga al Data Privacy Framework (DPF), garantizando el cumplimiento estricto de lo dispuesto en el inciso segundo del artículo 28 de la Ley N° 19.628, reformada por la Ley N° 21.719, que exige estándares, principios y derechos similares o superiores a los que reconoce la legislación chilena. Como contexto, el DPF responde a la tercera generación de acuerdos entre la Unión Europea (UE) y Estados Unidos para habilitar transferencias internacionales de datos alcanzado en 2022. Bajo este mecanismo las compañías pueden autocertificarse ante el Departamento de Comercio, comprometiéndose legalmente a cumplir con los principios del DPF. El cumplimiento es exigible por la Federal Trade Commission (FTC) y el Department of Transportation (DOT).

Actualmente, más de 2.800 empresas estadounidenses se han inscrito en el DPF (frente a unas 2.400 bajo el Privacy Shield). Cerca del 70 % son pymes, principalmente en tecnologías de la información, comunicaciones y servicios digitales. Destacan sectores como tecnología y servicios en la nube (AWS, Microsoft, Google), marketing digital y publicidad (Meta, Adobe, HubSpot), servicios financieros y pagos (PayPal, Stripe, Square), salud y biotecnología (23andMe, Thermo Fisher), recursos humanos (Workday, ADP, Indeed), e-commerce (Amazon, Shopify), consultoría y servicios profesionales (Deloitte, PwC, Accenture) y ciberseguridad (CrowdStrike, Palo Alto Networks), lo que refleja la transversalidad del marco en industrias clave de la economía digital.

5. Avanzar en la declaración de Chile como país adecuado por la UE.

De acuerdo con el artículo 45 del GDPR, la Unión Europea (UE) declara como “países adecuados” a aquellos terceros países que, tras un proceso de evaluación técnica, se considera que ofrecen un nivel de protección de datos personales esencialmente equivalente al establecido en el Reglamento

General de Protección de Datos (GDPR). Esta decisión permite que los datos personales puedan transferirse libremente desde la UE hacia dichos países, sin necesidad de cláusulas contractuales, certificaciones u otras garantías adicionales.

Recomendamos que el Ministerio de Relaciones Exteriores inicie las gestiones ante la Comisión Europea para obtener la declaración de "país adecuado" a fin de garantizar que las transferencias internacionales de datos personales que se realicen desde Estados miembros de la UE a Chile puedan realizarse sin requerir garantías adicionales. En este contexto, representantes de la Comisión Europea han confirmado a esta Comisión Asesora que no es necesario esperar la entrada en vigencia de la ley ni la plena operación de la Agencia de Protección de Datos para iniciar el proceso de reconocimiento de Chile como país adecuado.

Resulta claro el beneficio para Chile de obtener una decisión de adecuación por parte de la Unión Europea. Desde una perspectiva económica, ello permitiría a las empresas chilenas integrarse de manera más fluida en cadenas globales de valor, eliminando costos asociados a la implementación de cláusulas contractuales, certificaciones u otros mecanismos de transferencia, y fomentando la llegada de inversión extranjera directa en sectores que dependen intensivamente del flujo transfronterizo de datos. Desde el punto de vista legal, la adecuación reforzaría la certeza y estabilidad regulatoria del país, consolidando la vigencia de derechos fundamentales vinculados a la protección de datos personales y asegurando un marco normativo alineado con los más altos estándares internacionales. En conjunto, estos factores pueden proyectar a Chile como un socio confiable en la economía digital global, con beneficios que abarcan tanto a los ciudadanos como al desarrollo estratégico del país.

6. Adherir al Convenio 108+ del Consejo de Europa.

El Convenio 108 del Consejo de Europa, formalmente conocido como "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", fue adoptado en 1981 y es uno de los instrumentos internacionales más importantes en el ámbito de la protección de datos personales. Establece un marco legal vinculante para la protección de la privacidad y los derechos de las personas en relación con el tratamiento de sus datos personales por parte de los organismos públicos y privados, especialmente en lo que respecta a la transmisión y el tratamiento automatizado de dicha información.

El objetivo principal del Convenio 108 es garantizar que los datos personales sean procesados de manera legal y justa, respetando los derechos de los individuos, y promover la cooperación internacional en este ámbito. Además, promueve que los países signatarios adopten medidas para proteger los datos personales contra el abuso y garantizar la transparencia en el tratamiento de los mismos. En 2018 se adoptó un protocolo adicional (Protocolo 223) llamado "Convenio 108+" que refuerza su aplicación, especialmente en lo que respecta a la transferencia de datos personales entre los países signatarios. Además, el convenio fue uno de los cimientos sobre los que se construyó el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

El procedimiento de suscripción del convenio es similar al de cualquier tratado internacional (firma, ratificación, depósito, etc.) pero requiere un paso previo. Se debe evacuar un informe, (denominado

pre-assessment) de la Secretaría Permanente del Convenio 108 en Estrasburgo que señale que la regulación e institucionalidad del país en materia de protección de datos personales alcanzan los estándares exigidos en el Convenio.

Recomendamos que el Ministerio de Relaciones Exteriores solicite formalmente a la Secretaría Técnica del Convenio 108 la realización de la evaluación previa (pre-assessment), con el fin de identificar eventuales ajustes normativos o institucionales necesarios para cumplir plenamente con los estándares del tratado. Posteriormente, esta Comisión recomienda iniciar los preparativos para que Chile adhiera al Convenio 108+ del Consejo de Europa, como instrumento internacional clave para la protección de datos personales y la cooperación transfronteriza.

3° INFORME

RECOMENDACIONES PARA LA IMPLEMENTACIÓN DE LA LEY EN LA ADMINISTRACIÓN DEL ESTADO.

TERCER INFORME DE LA COMISIÓN DE IMPLEMENTACIÓN PARA LA LEY DE PROTECCIÓN DE DATOS PERSONALES. RECOMENDACIONES PARA LA IMPLEMENTACIÓN DE LA LEY EN LA ADMINISTRACIÓN DEL ESTADO
08 DE SEPTIEMBRE DE 2025

I. ANTECEDENTES

El 05 de junio del presente año, mediante el Decreto N°12 del Ministerio Secretaría General de la Presidencia, se constituyó la Comisión Asesora Ministerial para la Implementación de la nueva Ley de protección de datos personales, instancia consultiva cuyo objeto es asesorar técnicamente a dicho Ministerio en todas las acciones necesarias para la adecuada implementación de la Ley N°21.719, la que entrará en vigencia el 1° de diciembre del año 2026.

En el marco de su cronograma de trabajo, la Comisión ha acordado emitir informes previos a aquél que dispone el artículo 4° del Decreto N° 12, de manera de abordar oportunamente las materias que se han considerado de mayor urgencia.

Es en este contexto que se evacua el presente Tercer Informe, cuyo objeto es recomendar que la Secretaría de Gobierno Digital del Ministerio de Hacienda, en el marco de las atribuciones que le confiere la Ley N° 21.658 como órgano coordinador intersectorial del uso estratégico de tecnologías digitales, datos e información pública en la Administración del Estado, dicte un oficio circular referido a directrices y guías técnicas, y que, asimismo, según corresponda, pueda coordinarse con otras entidades públicas, como la Dirección de Compras Públicas o el Servicio Civil, en los términos indicados en la recomendación, a fin de establecer lineamientos que apoyen la implementación de la Ley N° 21.719 en los órganos de la Administración del Estado, incluidas las municipalidades.

El objetivo de esta recomendación es dotar a la Administración de un marco común, con un enfoque integrado de actuación que facilite la implementación de la Ley N° 21.719 a través de hitos concretos, entregando una hoja de ruta a sus órganos. Lo anterior resulta especialmente relevante considerando la alta sensibilidad de los datos tratados por el sector público, los cuales, en general, se gestionan sobre la base de competencias legales y no del consentimiento de los ciudadanos, lo que exige un nivel máximo de diligencia en la observancia de la normativa.

La Comisión hace presente que abordará en una recomendación específica lo relativo a las empresas públicas reguladas por ley, atendidas las particularidades propias de estas entidades y la necesidad de considerar un tratamiento diferenciado respecto de los órganos de la Administración del Estado.

II. CONTEXTO

La entrada en vigor de la Ley N° 21.719 de Protección de Datos Personales marca un hito en la consolidación de un marco regulatorio robusto en Chile, aplicable de manera transversal tanto al sector privado como al sector público. El Estado, en su calidad de sujeto obligado, y las instituciones públicas, como responsables del tratamiento de datos personales, deben adecuar sus procesos

internos y externos para cumplir con los principios, obligaciones y estándares establecidos en la normativa.

El régimen de infracciones previsto en la ley es aplicable a los órganos públicos, siendo el principal responsable el jefe superior del servicio, a quien se le pueden aplicar multas sobre su remuneración y, respecto a los funcionarios existe la posibilidad de instruir procedimientos disciplinarios, con sanciones que pueden tener un alto impacto reputacional e institucional.

El artículo 44 de la nueva ley establece que los órganos públicos deberán someterse a las medidas tendientes a subsanar o prevenir infracciones que indique la Agencia o a los programas de cumplimiento o de prevención de infracciones del artículo 49. En este contexto, la implementación diligente de medidas de cumplimiento no solo es un imperativo legal, sino también un componente esencial para resguardar la confianza pública en el uso de datos personales, confianza que constituye un activo estratégico para el funcionamiento del Estado y la legitimidad de sus políticas públicas. La ley ofrece alternativas para los órganos del estado, desarrollar un Modelo de Prevención de Infracciones o a las medidas preventivas que señala la Agencia. Mientras eso no suceda, es indispensable implementar un estándar mínimo de cumplimiento antes de la entrada en vigencia de la ley.

La ciudadanía exige que el tratamiento de sus datos personales se realice con apego estricto a la legalidad, transparencia y proporcionalidad. La adopción de un enfoque preventivo y de cumplimiento proactivo permitirá a los organismos de la Administración evitar infracciones, garantizar los derechos de las personas y fomentar un ecosistema digital estatal confiable, interoperable y alineado con estándares internacionales.

El desarrollo de medidas de implementación de la Ley N°21.719 debe ser coherente con la implementación de políticas de Gobernanza e Interoperabilidad de Datos y de Ciberseguridad, procurando una convergencia y optimización en el uso de recursos.

III. RECOMENDACIONES DE ESTA COMISIÓN DE IMPLEMENTACIÓN

Con el fin de facilitar a los órganos de la Administración del Estado la implementación de la Ley N° 21.719, esta Comisión recomienda que la Secretaría de Gobierno Digital del Ministerio de Hacienda, en el marco de las atribuciones que le confiere la Ley N° 21.658, apoye este proceso mediante el despacho de un oficio circular que establezca un conjunto de acciones concretas a ser abordadas e implementadas por los organismos públicos. Asimismo, en estas recomendaciones se formulan sugerencias relativas a la participación de otros órganos gubernamentales, tales como ChileCompra y el Servicio Civil, los cuales pueden colaborar en la adopción de determinadas medidas, con el propósito de dotar al sector público de herramientas efectivas de implementación. Del mismo modo, se contempla la posibilidad de que la Secretaría de Gobierno Digital dicte directrices y guías técnicas que complementen dichas acciones.

Estas recomendaciones recogen los principales y mínimos ámbitos de actuación que deben ser considerados por los órganos de la Administración, sin perjuicio de lo que, en el futuro, establezca la Agencia de Protección de Datos Personales una vez que inicie sus funciones.

1. Designación del Delegado de Protección de Datos (DPO)

> Cada servicio público debe designar formalmente un responsable de la implementación de la nueva ley que estará encargado de gestionar, coordinar y supervisar el cumplimiento de los hitos del plan de implementación que defina la SGD y será la contraparte institucional ante dicha secretaría. Este encargado podrá asumir la forma del Delegado de Protección de Datos de la Ley N°21.719.

> En el caso de ministerios u organismos que cuenten con servicios dependientes o desconcentrados o descentralizados, se recomienda evaluar la posibilidad de designar un único encargado o Delegado de Protección de Datos a nivel central, con competencia sobre la institución matriz y sus órganos dependientes. Este modelo permitiría asegurar criterios uniformes de cumplimiento, optimizar recursos y garantizar un nivel homogéneo de protección de datos en toda la estructura institucional, evitando la dispersión de responsabilidades y facilitando la coordinación con la futura Agencia de Protección de Datos Personales.

> Se recomienda que la SGD pueda establecer una red de DPOs sectoriales, coordinados a nivel central, para homogeneizar criterios y fortalecer capacidades. Para eso podrán evaluar redes existentes, como la Red de Coordinadores de Transformación Digital para compartir buenas prácticas y lineamientos comunes entre órganos de la Administración del Estado, anticipando la función coordinadora de la futura Agencia.

> Tal como dispone la ley, en caso de nombrar un Delegado de Protección de Datos (DPO) este debe designarse dentro de la dotación actual del servicio, según el artículo 5° transitorio de la Ley N°21.719.

2. Crear comités internos de implementación.

> Crear un comité interno de protección de datos en cada ministerio u organismo, integrado, a lo menos, por las áreas jurídicas, de tecnología y de negocio (área que trata datos relevantes).

> Este comité debería reportar periódicamente al nivel directivo. Los acuerdos del comité deberán ser sometidos a la consideración del jefe superior del servicio.

> Recomendable establecer instancias de coordinación interinstitucional, para compartir buenas prácticas y lineamientos comunes entre organismos públicos, anticipando la función coordinadora de la futura Agencia.

3. Política de tratamiento de Datos Personales

- Cada servicio público deberá elaborar y publicar una Política de Protección de Datos en lenguaje claro, accesible y comprensible para la ciudadanía de conformidad al artículo 14 ter de la Ley N°21.719.

- Esta política debe definir el marco de cumplimiento de cada organismo, sus funciones, datos tratados, entre otros aspectos y detallar los mecanismos de ejercicio de derechos.

- Esta política debe revisarse periódicamente y estar alineada con las políticas de seguridad de la información y gestión documental del organismo.

- Se recomienda que para la mejor ejecución de las medidas anteriores la SGD pueda disponer de un documento tipo de referencia, tal como el que ha sido dispuesto por ejemplo por la Agencia de Acceso a la Información Pública y Protección de Datos de Argentina[1].

4. Procedimiento de Derechos ARCO (Acceso, Rectificación, Supresión, Oposición)

> Cada entidad deberá diseñar un procedimiento administrativo interno que permita responder, dentro de los plazos legales, a las solicitudes de titulares de datos de los derechos ARCO que sean aplicables al sector público.

> Integrar la gestión de los derechos de ARCO en una plataforma unificada para el Estado, al estilo del Portal de Transparencia o dentro de los canales ya existentes de Oficinas de Información, Reclamos y Sugerencias (OIRS). Esto permitiría utilizar un canal conocido por la ciudadanía, evitando confusión y duplicidad de instancias.

> Debe garantizarse la coordinación entre las OIRS y el Delegado de Protección de Datos, de modo que las solicitudes recibidas sean derivadas y gestionadas de forma adecuada.

> Se recomienda que la Secretaría de Gobierno Digital defina los estándares y sistemas de autenticación a que se refiere el artículo 11, letra a), para los organismos de la Administración del Estado, los cuales podrán ser posteriormente ratificados por la Agencia de Protección de Datos Personales.

> Capacitar a funcionarios responsables para asegurar respuestas oportunas y fundamentadas, evitando riesgos de incumplimiento.

5. Ajustes contractuales con proveedores que actúen como encargados del tratamiento

> Se recomienda elaborar cláusulas tipo para encargados del tratamiento, de conformidad con lo dispuesto en el artículo 15 bis, regulando aspectos tales como obligaciones de sujeción a la finalidad, seguridad, confidencialidad, subcontratación, auditoría y mecanismos de supervisión. El diseño de estas cláusulas podrá ser propuesto por la Dirección de Compras Públicas, a fin de asegurar que se ajusten a las mejores prácticas y a las particularidades de la Administración del Estado.

> Se recomienda que los organismos de la administración pública diseñen procesos de evaluación previa, auditoría y control sobre proveedores, incluyendo la obligación de reportar incidentes de seguridad y brechas de datos.

> Considerar de manera expresa los flujos transfronterizos de datos personales dentro de procesos de compra pública, exigiendo garantías equivalentes a las establecidas en la legislación chilena.

[1] ANEXO I RESOLUCION POLITICA MODELO DE PROTECCION DE DATOS PERSONALES PARA ORGANISMOS PUBLICOS https://www.argentina.gob.ar/sites/default/files/5554233a01.pdf

6. Levantamiento del Registro de Actividades de Tratamiento (RAT)

> Se recomienda fomentar la elaboración voluntaria de RAT por parte de los organismos públicos, aun cuando no sea exigible por la ley, en la medida en que constituyen una buena práctica de gestión que facilita la trazabilidad de los tratamientos, y la identificación de los aspectos fundamentales que requiere la normativa. El RAT permite identificar tratamientos realizados, sus finalidades, las bases de licitud invocadas, los destinatarios de datos y las transferencias internacionales entre otros aspectos.

> Como se indicó la elaboración de los Registros de Actividades de Tratamiento (RAT) no es obligatoria, se sugiere que la Secretaría de Gobierno Digital elabore un modelo de RAT tipo, simplificado y ajustado a la Administración Pública, que permita a los organismos públicos documentar sus procesos de tratamiento de datos, facilitando con ello distintos aspectos del cumplimiento

7. Implementación de Medidas de Seguridad

> Se recomienda que los servicios públicos verifiquen la adopción de medidas de seguridad organizativas, técnicas y administrativas acordes a la naturaleza de los datos tratados y a los riesgos identificados.

> Establecer protocolos para la gestión de incidentes y brechas de seguridad, con planes de contingencia y notificación a los titulares y autoridades competentes, en coordinación con las exigencias de otros marcos sectoriales como la ley marco de ciberseguridad.

8. Plan interno de Capacitación y Cultura de Protección de Datos

> Se recomienda que los servicios públicos puedan considerar programas de formación en protección de datos para sus funcionarios públicos, diferenciando niveles de profundidad según roles, autoridades, directivos, funcionarios operativos.

> Se recomienda que el Servicio Civil, en el marco de sus funciones, pueda incorporar módulos formativos y normativos que permitan alinear la implementación de la Ley N° 21.719 con los principios propios de la gestión pública, incluyendo la transparencia, la rendición de cuentas y la probidad administrativa, así como las obligaciones propias de la Administración del Estado. Dichos módulos podrían ser integrados en la plataforma Campus de dicho servicio a partir de 2026, facilitando la capacitación y estandarización en todos los órganos de la Administración antes de diciembre de 2026.

4° INFORME

DE LA COMISIÓN DE IMPLEMENTACIÓN PARA LA LEY DE PROTECCIÓN DE DATOS PERSONALES.

CUARTO INFORME DE LA COMISIÓN DE IMPLEMENTACIÓN PARA LA LEY DE PROTECCIÓN DE DATOS PERSONALES. 14 DE ENERO DE 2026

I. ANTECEDENTES

El 05 de junio del año 2025, mediante el Decreto N°12 del Ministerio Secretaría General de la Presidencia, se constituyó la Comisión Asesora Ministerial para la Implementación de la nueva Ley de Protección de Datos Personales, instancia consultiva cuyo objeto es asesorar técnicamente a dicho Ministerio en todas las acciones necesarias para la adecuada implementación de la ley N°21.719, la que entrará en vigencia el 1° de diciembre del año 2026.

En el marco de su cronograma de trabajo, la Comisión ha acordado emitir informes previos a aquél que dispone el artículo 4° del Decreto N° 12, de manera de abordar oportunamente las materias que se han considerado de mayor urgencia.

Es en este contexto que se evacua el presente Informe, el que se enmarca en el proceso participativo el cual recibió insumos de distintos actores, los que sirvieron de base para las recomendaciones de esta Comisión con respecto a la implementación de la Ley, asegurando la incorporación de las visiones y propuestas de todos los participantes .

A fin de resguardar un proceso ordenado y productivo, se definieron ejes temáticos tales como estándares de transparencia y seguridad para Pymes, tipos especiales de datos, tratamiento de datos para prevención del fraude, flujo transfronterizo de datos y coordinación regulatoria.

Los lineamientos de participación establecieron que las sesiones se realizaron de forma presencial en el auditorio del Edificio Bicentenario, ubicado en Teatinos 92, y en salón Pablo Neruda del Palacio de La Moneda, Santiago. Se invitó a un máximo de dos entidades participantes por sesión y la duración de las presentaciones se acotó a veinte minutos para dar espacio al intercambio y diálogo entre los invitados y la comisión. El enfoque de las intervenciones se centró en aportes sustantivos, identificación de nudos críticos, vacíos regulatorios, interpretaciones y propuestas de mejora del tema indicado. Se solicitó la entrega de una minuta con la propuesta escrita, como insumo para la consolidación de aportes, las que tienen carácter público. El espacio de participación se enmarcó en un diálogo constructivo, ya que la Comisión de Implementación es una instancia asesora cuyo rol fue formular recomendaciones y proponer insumos para la implementación de la Ley, sin poseer funciones ejecutivas o resolutivas.

El objetivo de esta recomendación es proponer interpretaciones a algunos nudos críticos que fueron planteados, propuestas de mejora a la legislación que en el futuro podrán ser considerados por la futura Agencia de Protección de Datos Personales, tomando de base el sentir de la industria y la opinión de expertos. Asimismo, de conformidad con el Decreto N° 12 que creó esta Comisión, se proponen los tiempos asociados a la ejecución de las medidas propuestas.

Las instituciones recibidas por la comisión fueron las siguientes:

FECHA	TEMA	INVITADOS
02.10.2025	Nudos críticos de la Ley de Protección de Datos y la implementación del sistema de finanzas abiertas (REDEC). Tratamiento de datos socioeconómicos, financieros, bancarios y comerciales.	ABIF FINTEChile
09.10.2025	Propuesta de estándares diferenciados de transparencia y seguridad para las micro, pequeñas y medianas empresas que deberían ser considerados por la futura Agencia de Protección de Datos.	AGPD Chiletec
23.10.2025	Interés legítimo en el uso de fuentes públicas. Prevención de delitos y compliance empresarial. Plazos de implementación de la ley; Relación con los proyectos de gobernanza de datos e IA en tramitación legislativa.	ACEC Amazon
30.10.2025	Consideraciones sobre la puesta en marcha de los instrumentos que permiten los flujos transfronterizos de datos personales. Control de cláusulas abusivas y nueva Ley de Protección de Datos Personales.	Prof. Pablo Trigo Prof. María Elisa Morales
06.11.2025	Coordinación regulatoria.	ACTI Consejo para la Transparencia
13.11.2025	Interpretación sobre la normativa infra legal y el tratamiento de datos personales. Opinión jurídica sobre las facultades inspectivas de la Agencia de Protección de Datos.	Prof. Pablo Contreras Prof. Brigitte Leal
20.11.2025	Desafíos técnicos y jurídicos de la supresión de datos personales. Propuesta de estándares diferenciados de transparencia y seguridad para las micro, pequeñas y medianas empresas que deberían ser considerados por la futura Agencia de Protección de Datos.	REDIAC CCS
27.11.2025	Observaciones y comentarios sobre el proceso de implementación de la Ley de Protección de Datos. Desafíos de la industria aseguradora.	AACH Retail Financiero

FECHA	TEMA	INVITADOS
04.12.2025	Coordinación regulatoria. Aplicación de la ley en empresas públicas Interpretaciones y nudos críticos en la seguridad social.	CMF SEP SUSESO

Todo el detalle de las presentaciones de cada uno de los invitados está disponible en https://www.minsegpres.gob.cl/comision-asesora-ministerial

Asimismo, se abrió un proceso de recepción de aportes por escrito mediante una Consulta pública en línea cuya caracterización la siguiente:

CONSULTA PÚBLICA	
Mecanismo de participación	Consulta pública en línea
Plataforma utilizada	Sitio web de la Secretaría de Gobierno Digital del Ministerio de Hacienda.
Período de realización	20 de octubre al 30 de noviembre de 2025
Visitantes únicos	4.426
Total de visitas	5.883
Personas participantes	152
CARACTERIZACIÓN DE PARTICIPANTES	
Género masculino	61,6 %
Género femenino	32,1 %
Otro género	1,3 %
No responde	5 %
Región Metropolitana	40,9 %
Otras regiones	59,1 %
CARACTERIZACIÓN DE PARTICIPANTES	
Sector privado	39 %
Gobierno	20,1 %
Empresa	17,6 %
Academia	5 %
ONG	1 %
Otro	9,4 %
ESTRUCTURA Y CONTENIDOS DE LA CONSULTA	
Modalidad de participación	Selección múltiple de temas propuestos y texto libre
Principios del tratamiento de datos	18,9 %
Tratamiento de datos en el sector público	17 %
Datos sensibles	12,6 %
Agencia de Protección de Datos Personales	11,9 %

La mayoría de los aportes está dirigido a pedir más claridad sobre aspectos específicos de la ley, y guías para su implementación. Se tratarán en conjunto con las recomendaciones generales extraídas desde el periodo de audiencia presencial.

Adicionalmente al proceso de participación ciudadana descrito, la Comisión recibió una minuta elaborada por la Policía de Investigaciones de Chile, en la cual se expusieron observaciones y consideraciones técnicas relevantes en relación con materias del tratamiento de datos dentro de su ámbito. Asimismo, la Comisión sostuvo una reunión con representantes del Departamento de Comercio de los Estados Unidos y con personeros de la Embajada de dicho país en Chile, instancia en la que se intercambiaron antecedentes y visiones respecto de las materias abordadas en el presente informe.

Finalmente, cabe señalar que la totalidad de los aportes recibidos —tanto aquellos provenientes del proceso de participación ciudadana como los remitidos por instituciones y actores especializados— fueron debidamente analizados y ponderados por la Comisión. En ejercicio de sus facultades y conforme a los criterios técnicos, jurídicos y de política pública definidos para el cumplimiento de su mandato, la Comisión resolvió cuáles de dichas observaciones acoger y cuáles no, decisión que se refleja en las recomendaciones de implementación contenidas en el presente informe.

II. CONTEXTO

La realidad actual en Chile se fundamenta en una práctica de manejo y uso de datos que se asentó durante años, pero que, con la inminente entrada en vigor de la nueva Ley de Protección de Datos Personales, deberá alinearse con las expectativas de los titulares y sus derechos, y las exigencias de la legislación. Existe conciencia de que la Agencia de Protección de Datos Personales (APDP), una vez operativa, deberá abordar diversos ámbitos de interpretación normativa que aún no han sido definidos y que por ende generan incertezas en la aplicación de la ley.

Si bien los criterios de las autoridades de protección de datos europeas se consideran un modelo relevante, no es posible desconocer la realidad de Chile y la forma en que el tratamiento de datos se ha regulado históricamente mediante legislaciones dispersas y en ciertos casos inexistentes, las interpretaciones de nuestros tribunales de justicia, y de los organismos administrativos con competencias sectoriales, lo que hace esencial compatibilizar la libre circulación de la información, considerando las necesidades de uso de datos del mercado y los derechos de las personas. Aunque se espera una alineación a mejores prácticas, esta debe ser ponderada y realista, por esta razón, esta Comisión de expertos cree necesario plasmar propuestas y criterios para que la APDP pueda iniciar su labor con una visión que considere la realidad local, las particularidades de las distintas industrias y los diversos tamaños de las organizaciones obligadas.

Dado que no es viable esperar hasta la entrada en vigor completa de la Ley en diciembre de 2026 para iniciar esta labor de armonización, esta Comisión propone una visión anticipada que se espera sirva como base para la futura APDP considerando la realidad local, las particularidades de las distintas industrias y los diversos tamaños de las organizaciones.

III. RECOMENDACIONES DE LA COMISIÓN DE IMPLEMENTACIÓN

Las recomendaciones del informe abordan distintos ejes temáticos que fueron definidos en las audiencias presenciales y que también se plasmaron a través del proceso de participación remoto. Estos ejes temáticos, que buscan estructurar los aportes recibidos, son cruciales para el desarrollo de criterios, los cuales se abordan a continuación.

1. Coordinación Regulatoria

El análisis realizado por la Comisión pone de manifiesto que la efectiva implementación del nuevo régimen de protección de datos personales requiere de una coordinación regulatoria sistemática y permanente entre la futura Agencia de Protección de Datos Personales y aquellos órganos públicos que, por la naturaleza de sus funciones, ya ejercen potestades reguladoras, fiscalizadoras o interpretativas que inciden directamente en el tratamiento de datos personales, tanto para el sector público como para el privado.

En particular, se observa que existen ámbitos sectoriales —como los mercados financieros, la protección de los derechos de los consumidores, la transparencia y acceso a la información pública, y la supervisión de industrias reguladas— en los que confluyen normas especiales, autoridades técnicas y regímenes de fiscalización propios, que deben articularse de manera coherente con la Ley de Protección de Datos Personales. En estos espacios, la coexistencia de normas generales y especiales, así como de competencias concurrentes o complementarias, puede generar incertidumbre jurídica si no se establecen criterios claros de coordinación institucional.

La Comisión estima que la futura Agencia debe considerar la especialidad normativa existente en determinados sectores, sin perjuicio de afirmar el carácter general y supletorio de la Ley de Protección de Datos Personales respecto de todas aquellas materias que no hayan sido reguladas de manera expresa por legislaciones sectoriales, o que no hayan hecho excepción expresa a su aplicabilidad a una materia determinada. Este equilibrio resulta especialmente relevante en contextos de innovación regulatoria, donde nuevos modelos de negocio, tecnologías o sistemas de intercambio de información plantean riesgos específicos para los derechos de las personas y exigen claridad en la asignación de responsabilidades.

Asimismo, se constata la necesidad de una coordinación funcional entre la Agencia y aquellos organismos que ejercen competencias en defensa de derechos colectivos, fiscalización de mercados o control de la legalidad administrativa, de modo que cada institución actúe dentro de su ámbito de especialidad, evitando duplicidades, vacíos regulatorios o decisiones contradictorias. En este sentido, la delimitación entre la determinación de la licitud de los tratamientos de datos y las acciones destinadas a la reparación de perjuicios o sanción de prácticas abusivas resulta clave para una tutela efectiva de los derechos fundamentales.

En el ámbito del sector público, la coordinación adquiere una relevancia adicional, dado que los órganos del Estado tratan datos personales en cumplimiento de mandatos constitucionales y legales, bajo principios propios de la Administración, como la legalidad, probidad y transparencia. La implementación de la ley debe, por tanto, considerar estas particularidades, asegurando que las

directrices, guías e interpretaciones que emita la Agencia sean coherentes con el marco constitucional y con los principios que rigen la función pública, promoviendo continuidad y certeza jurídica.

En el marco de esta temática, la Comisión estima prioritario que la futura Agencia de Protección de Datos Personales establezca mecanismos de coordinación temprana, sistemática y permanente con la ANCI, la Secretaría de Gobierno Digital, el Consejo para la Transparencia, la Comisión para el Mercado Financiero, la Superintendencia de Seguridad Social, el Servicio Nacional del Consumidor, así como con otras entidades fiscalizadoras como las Superintendencia de Salud y la Dirección del Trabajo, entre otras. Dicha coordinación resulta indispensable para armonizar criterios interpretativos, delimitar adecuadamente las competencias respectivas, evitar solapamientos regulatorios y asegurar una aplicación coherente del régimen de protección de datos personales, tanto en el sector público como en los mercados regulados, considerando la coexistencia de normas generales y especiales y la incidencia directa que las decisiones de estos organismos tienen en la licitud y condiciones del tratamiento de datos personales.

Dicha coordinación no es sólo necesaria para asegurar la correcta aplicación de la ley, sino para tender a un actuar eficiente y eficaz, que permita avanzar hacia una coherencia regulatoria que otorgue certeza a las entidades reguladas respecto de la legalidad de sus actuaciones, evitando interpretaciones contradictorias de la legislación aplicable, especialmente considerando que la mayoría de los organismos con competencias eventualmente concurrentes tiene potestades interpretativas de la legislación que les corresponde aplicar. Por otra parte, una actuación coordinada debería permitir a los organismos prever y abordar coordinadamente eventuales situaciones en que corresponda aplicar más de una sanción por la comisión de una infracción en razón de vulnerar distintos estatutos legales aplicables. Esta coordinación debe realizarse sobre la base de que la Agencia de Protección de Datos es el órgano público competente, con las funciones y atribuciones legales para interpretar y aplicar la Ley de Protección de Datos en el país, con independencia del ámbito de actividad de que se trate.

Asimismo, respecto de los organismos con los cuales se propone establecer mecanismos de coordinación, debe tenerse presente que dichos entes se encuentran igualmente sujetos a la regulación y fiscalización de la Agencia de Protección de Datos Personales, en cuanto realizan tratamientos de datos personales en el ejercicio de sus funciones. En este marco, tales organismos actúan como responsables del tratamiento de los datos personales que procesan por mandato legal, debiendo cumplir íntegramente con las obligaciones y principios establecidos en la Ley de Protección de Datos Personales, sin perjuicio de las competencias sectoriales que les han sido conferidas.

Recomendaciones

En virtud de lo anterior, la Comisión recomienda que la Agencia de Protección de Datos Personales establezca una gobernanza de coordinación interinstitucional, mediante mecanismos formales y permanentes con los principales organismos reguladores y fiscalizadores cuyos ámbitos de competencia se intersectan con la protección de datos personales. Entre dichos mecanismos se sugiere considerar:

> Mesas de trabajo permanentes o periódicas, destinadas a armonizar criterios interpretativos, coordinar actuaciones fiscalizadoras y anticipar eventuales conflictos de competencia.

> Memorandos de entendimiento u otros instrumentos de cooperación interinstitucional, que definan ámbitos de actuación, flujos de información, criterios de derivación de casos y coordinación en la dictación de normas de carácter general.

> Instancias conjuntas de elaboración de directrices, guías o instrucciones, especialmente en materias donde confluyen regímenes generales y especiales, o donde exista una alta incidencia de tratamientos de datos personales.

> La Comisión recomienda que, en el marco de la coordinación regulatoria, se avance en la implementación de una plataforma única de notificación de incidentes de seguridad y vulneraciones de datos personales, que permita a los responsables y encargados del tratamiento cumplir de manera integrada con las obligaciones de reporte establecidas en la Ley de Protección de Datos Personales y en la normativa sectorial en materia de ciberseguridad. Dicha plataforma debiera operar bajo un régimen de notificaciones unificado, tomando como referencia los criterios técnicos y procedimentales definidos por el regulador sectorial en el ámbito de la ciberseguridad, en particular aquellos desarrollados por la Agencia Nacional de Ciberseguridad (ANCI). Asimismo, se recomienda que los plazos de notificación que se definan y apliquen en el marco de la Ley de Protección de Datos Personales sean coherentes y armónicos con los plazos establecidos por la ANCI, con el objeto de evitar duplicidades, inconsistencias regulatorias y cargas innecesarias para los sujetos obligados, fortaleciendo así la eficacia del sistema de gestión de incidentes y la protección oportuna de los derechos de las personas.

> Sin perjuicio de las atribuciones de la Agencia, la Comisión recomienda mantener cierta deferencia hacia los reguladores sectoriales que cuenten con facultades específicas en materia de protección de datos personales, reconociendo su competencia en la aplicación y fiscalización de las normas dentro de sus respectivos ámbitos de actuación. Lo anterior no obsta a que dichas entidades, así como los sujetos regulados, puedan consultar a la Agencia de Protección de Datos Personales en su calidad de autoridad técnica especializada, con el objeto de obtener orientaciones generales, criterios interpretativos o buenas prácticas que contribuyan a una aplicación coherente y armónica del régimen de protección de datos personales a nivel intersectorial.

> De igual forma, la APDP debe propender de manera gradual y progresiva a que a través de sus actuaciones, se generen criterios y directrices comunes entre los diferentes organismos reguladores con competencias en protección de datos personales, contribuyendo a morigerar la dispersión regulatoria, fortaleciendo la certeza jurídica hacia los diferentes sectores regulados.

Estas recomendaciones resultan particularmente aplicables respecto de organismos reguladores de mercados financieros y de seguridad social, autoridades encargadas de la protección de los consumidores , entidades responsables de la transparencia y acceso a la información pública, y otros órganos sectoriales con potestades normativas y fiscalizadoras relevantes. Una coordinación efectiva con estas entidades permitirá fortalecer la protección de los datos personales, asegurar coherencia regulatoria y facilitar una implementación armónica del nuevo marco legal.

Cronograma de implementación

La Comisión estima que la implementación efectiva de las medidas y recomendaciones contenidas en este punto pueda iniciarse a partir del cuarto mes contado desde la instalación formal de la Agencia de Protección de Datos Personales. Ello, atendido que, durante los primeros meses de funcionamiento, resultará prioritario que la Agencia aborde definiciones iniciales y particulares respecto de materias que son de su competencia exclusiva, tales como la organización interna, la adopción de criterios interpretativos básicos y el establecimiento de lineamientos generales para el ejercicio de sus potestades. Solo una vez consolidadas dichas definiciones iniciales, será razonable avanzar de manera progresiva en la implementación de acciones de coordinación regulatoria y en la dictación de instrumentos de carácter general.

2. Flujo Transfronterizo de Datos Personales

Dada la relevancia y complejidad del régimen de transferencias internacionales de datos personales, la Comisión estimó necesario abordar esta materia de manera específica, elaborando un informe dedicado exclusivamente a esta materia . Dicho trabajo examinó los mecanismos jurídicos disponibles para habilitar las transferencias internacionales —incluidas las decisiones de adecuación, las cláusulas contractuales tipo y otros instrumentos de garantía—, así como las condiciones institucionales y técnicas necesarias para otorgar certeza jurídica y operativa al régimen de las transferencias internacionales de datos personales.

En este contexto, la Comisión considera de suma importancia que la futura Agencia de Protección de Datos Personales establezca de manera temprana un marco claro, técnico y operativo que permita facilitar el flujo legítimo de datos personales hacia terceros países, sin debilitar las garantías de los derechos de las personas. La experiencia comparada muestra que, en la práctica, la mayoría de las transferencias internacionales se sustentan en el uso de cláusulas contractuales tipo, instrumento ampliamente difundido por su carácter estandarizado, adaptable y reconocido internacionalmente, especialmente relevante en entornos de servicios digitales, tecnológicos y de computación en la nube.

No obstante, la Comisión advierte que el mecanismo que otorga mayor certeza estructural al sistema de transferencias internacionales sigue siendo la decisión de adecuación, mediante la cual la Agencia determinará que un país, territorio u organización internacional ofrece un nivel de protección adecuado. La ausencia o demora en la adopción de dichas decisiones genera impactos prácticos relevantes, influyendo en decisiones empresariales y de inversión que buscan mayor certeza regulatoria, lo que puede afectar la competitividad del país y su alineación con la estrategia nacional de desarrollo digital y de atracción de infraestructura tecnológica, incluyendo iniciativas vinculadas al desarrollo de centros de datos.

Recomendaciones

En virtud de lo anterior, la Comisión formula las siguientes recomendaciones:

> Que la Agencia de Protección de Datos Personales ratifique las cláusulas contractuales tipo aprobadas mediante la Resolución Exenta 3748/2025 del Ministerio de Economía, que toman como

base las cláusulas desarrolladas en el marco de la Red Iberoamericana de Protección de Datos, como mecanismo estándar y ampliamente reconocido para habilitar dichas transferencias.

> Que la Agencia defina y publique un procedimiento claro, simple y expedito para la adopción de decisiones de adecuación, estableciendo criterios objetivos de evaluación, etapas definidas del proceso y mecanismos de revisión periódica, conforme a lo dispuesto en el artículo 29 de la Ley de Protección de Datos Personales.

> Que dicho procedimiento considere la posibilidad de decisiones de adecuación recíproca, mediante acuerdos bilaterales que reconozcan mutuamente niveles adecuados de protección y faciliten la circulación de datos personales en ambos sentidos.

> Que la Agencia inicie oportunamente las acciones identificadas en el Informe N° 2 de esta Comisión, como parte de una hoja de ruta integral para la implementación del régimen de transferencias internacionales de datos personales.

Cronograma de implementación

La Comisión recomienda que la implementación de las medidas señaladas en esta temática se inicie de manera inmediata a la instalación formal de la Agencia de Protección de Datos Personales, atendida la urgencia de dotar de certeza jurídica al régimen de transferencias internacionales de datos personales. En particular, la definición del procedimiento para la adopción de decisiones de adecuación y la aprobación de cláusulas contractuales tipo debieran constituir acciones prioritarias desde el inicio del funcionamiento de la Agencia, por su impacto directo en la competitividad económica, la continuidad operativa de las actividades productivas y la protección efectiva de los derechos de las personas.

3. Necesidad de Regulación Especial

3.1. Tipos de datos:

La Comisión analizó el tratamiento de los datos personales relativos a la situación socioeconómica de las personas, los cuales han sido expresamente calificados como datos sensibles a partir de las modificaciones introducidas por la Ley N° 21.719. Conforme a la historia de la ley, esta categoría puede ejemplificarse en el tratamiento de datos referidos a la situación de vulnerabilidad socioeconómica, incluyendo la condición de pobreza, así como los instrumentos utilizados para su caracterización social. El resguardo reforzado de esta información se vincula directamente con el principio de igualdad ante la ley, en cuanto busca evitar que la condición socioeconómica de una persona se traduzca en tratos discriminatorios o desiguales.

En este contexto, la Comisión examinó asimismo la incorporación, en el artículo 17, de los datos relativos al cumplimiento de obligaciones de carácter económico, financiero, bancario o comercial, constatando que dicha norma se inserta en un régimen específico y taxativo destinado a regular la comunicación de información sobre incumplimientos, más que a configurar una categoría general de datos sensibles o socioeconómicos. Esta disposición delimita de manera precisa los supuestos en

que los responsables de registros o bancos de datos personales pueden comunicar información referida a incumplimientos de obligaciones económicas, financieras o comerciales, circunscribiéndolos a hipótesis expresamente establecidas por la ley.

Sin perjuicio de lo anterior, el ordenamiento jurídico reconoce determinados supuestos en los cuales el tratamiento de datos socioeconómicos puede realizarse sin el consentimiento del titular, siempre que se cumplan las condiciones legales establecidas. En particular, se contempla como hipótesis habilitante el tratamiento de dichos datos para fines de análisis de riesgo crediticio y evaluación de morosidad, conforme a la legislación vigente en materia de protección de datos personales, en la medida que ello resulte necesario y proporcional para el desarrollo de actividades económicas legítimas.

Asimismo, la Comisión analizó el tratamiento de datos personales provenientes de fuentes de acceso público, respecto de los cuales se constató que su uso no se encuentra prohibido por el solo hecho de su origen, siempre que se respeten estrictamente los principios de finalidad, proporcionalidad y licitud, y se implementen garantías adecuadas para la protección de los derechos de las personas.
Finalmente, respecto de los datos personales sensibles relativos a la salud, la Comisión hace presente que las leyes N° 21.719 y N° 20.584 sobre derechos y deberes del paciente son consistentes entre sí en cuanto a que, junto con dar una protección reforzada a este tipo de datos personales, ambas permiten la interoperabilidad y portabilidad de dicha información, y el correcto funcionamiento de las fichas clínicas reguladas en la ley

Recomendaciones

> La Comisión recomienda que la futura Agencia de Protección de Datos Personales emita una guía interpretativa que precise que el dato socioeconómico, en los términos de la Ley N° 21.719, debe entenderse como aquel referido a la situación de vulnerabilidad socioeconómica de una persona, incluyendo la condición de pobreza, evitando interpretaciones extensivas que amplíen indebidamente esta categoría de datos sensibles.

> Asimismo, la interpretación que se realice de los datos relativos al cumplimiento de obligaciones económicas, financieras, bancarias o comerciales debiese de realizarse de manera coherente con el contexto normativo y la finalidad del artículo 17, el cual regula de forma específica y taxativa los supuestos de comunicación de información sobre incumplimientos, circunscribiéndolos a las categorías expresamente previstas por la ley. En consecuencia, el concepto de "cumplimiento" no debe entenderse de forma amplia o autónoma, sino en directa relación con el régimen especial de comunicación de incumplimientos establecido respecto de las obligaciones expresamente señaladas en dicha disposición, resguardando así la coherencia sistemática del marco legal y la protección de los derechos de las personas titulares de datos, interpretación que también es concordante con el principio de proporcionalidad del tratamiento de datos.

Cronograma de implementación

La Comisión recomienda que la elaboración y publicación de la guía interpretativa referida al tratamiento de datos socioeconómicos, datos provenientes de fuentes de acceso público y datos

relativos al cumplimiento de obligaciones económicas, financieras, bancarias o comerciales se realice a partir de los seis meses siguientes a la entrada en vigor de la Ley de Protección de Datos Personales.

3.2. Derechos de los titulares

Durante el período de audiencias, la Comisión analizó los desafíos asociados al ejercicio de ciertos derechos de las personas titulares de datos personales, en la medida en que estos fueron relevados por los distintos intervinientes. Con todo, la Comisión estima que la futura Agencia de Protección de Datos Personales deberá, en el ejercicio de sus funciones, emitir guías interpretativas que fijen criterios y límites respecto de otros derechos cuyo análisis no fue planteado de manera expresa durante las audiencias, pero que igualmente presentan nudos críticos relevantes para su aplicación práctica.

La Comisión constató que el ejercicio efectivo de los derechos de supresión y portabilidad de los datos personales presenta desafíos operativos y técnicos relevantes.

En el caso de la supresión, resulta necesario distinguir entre distintos tipos de datos, considerando su finalidad, origen y contexto, así como la existencia de obligaciones legales o contractuales que justifican su conservación por un período determinado. No todos los datos pueden ser objeto de eliminación inmediata, lo que exige criterios claros que eviten incertidumbre jurídica y cargas operativas desproporcionadas. La supresión de datos personales puede presentar importantes desafíos, que van desde detectar en qué entornos se encuentran almacenados esos datos (incluyendo aquellos que hayan sido comunicados a terceros encargados) y con qué finalidades, hasta contar con la tecnología y las capacidades humanas necesarias para dar cumplimiento al deber de supresión de la manera y en la oportunidad en que la ley lo dispone. Esto es especialmente relevante si se tiene en consideración que el deber aplica por igual a todos los responsables de datos, independientemente de su capacidad económica.

Respecto de la portabilidad, se identificaron desafíos vinculados a la determinación de los datos comprendidos en este derecho y a las condiciones en que la ley permite el cobro de costos asociados a su ejercicio. En particular, se advierte la necesidad de precisar su alcance, distinguiendo entre los datos facilitados directamente por el titular y aquellos inferidos o creados por el responsable del tratamiento.

Adicionalmente, si bien durante las audiencias se abordaron algunos derechos de las personas titulares, la Comisión observa que otros derechos relevantes —como el derecho de acceso, la rectificación y la oposición a decisiones automatizadas— también presentan nudos críticos para su aplicación práctica, aun cuando no hayan sido objeto de un análisis específico en dichas instancias. Especialmente relevante, a propósito del derecho de oposición, es precisar que si los titulares de los datos tienen la facultad de conocer los fundamentos de las decisiones automatizadas que les afecten que emanen de entidades privadas, también deberían tener esa atribución respecto de las decisiones algorítmicas que adopten los organismos del Estado, de lo contrario se configuraría una discriminación arbitraria que afecta los derechos de las personas.

Finalmente, y aunque la Comisión considera que su aplicabilidad puede reconstruirse a partir de diversas normas presentes en la Ley, con el fin de otorgar certeza a los titulares de datos, se recomienda hacer explícita a los organismos del Estado la regulación relativa al tratamiento automatizado de datos personales contenida en el artículo 8 bis.

Recomendaciones

> La Comisión recomienda que la futura Agencia de Protección de Datos Personales ejerza sus atribuciones para interpretar el sentido y alcance del ejercicio de estos derechos, siguiendo criterios y buenas prácticas desarrolladas en la experiencia internacional, que permitan fijar parámetros claros, uniformes y técnicamente viables para el ejercicio de los derechos de las personas titulares de datos personales. El pronunciamiento debiera abordar, de manera transversal, el alcance y los límites de los derechos de supresión, portabilidad, acceso, rectificación y oposición a decisiones automatizadas, con el objeto de otorgar certeza jurídica y facilitar una aplicación homogénea de la ley.

> En particular, se considera necesario que esta interpretación aborde el alcance y los límites del derecho de acceso, la rectificación de datos y el derecho de oposición a decisiones automatizadas, mediante la emisión de orientaciones prácticas que permitan una aplicación uniforme y técnicamente viable de la ley. La Comisión subraya que la ausencia de estas instrucciones generales o guías interpretativas no suspenden ni limitan la exigibilidad de dichos derechos, los cuales deberán ser plenamente respetados y garantizados desde la entrada en vigor de la Ley de Protección de Datos Personales, fijada para el 1 de diciembre de 2026.

> En particular, para abordar las dificultades que representa la supresión de datos personales, se recomienda que la APDP entregue lineamientos que distingan la supresión de datos en entornos productivos y entornos de respaldo, de manera de establecer medidas proporcionales para uno y otro caso. Así, mientras en los entornos productivos debería tenderse a la supresión o anonimización de los datos, en entornos de respaldo, en que la integridad del sistema es necesaria para asegurar su funcionalidad, debería propenderse a medidas graduales tales como la seudonimización y la segregación de datos, además de establecer y documentar políticas claras de retención de bases de datos de respaldo.

> La Comisión recomienda que la Agencia de Protección de Datos Personales promueva una modificación legal, para que los titulares puedan ejercer el derecho de oposición previsto en el artículo 8° bis, sobre las decisiones automatizadas que adopten los organismos públicos. Específicamente se propone la modificación del inciso final del artículo 21 incorporando dicho derecho.

Cronograma de implementación

> La Comisión recomienda que la elaboración y publicación de estas guías interpretativas se realice a partir de los seis meses siguientes a la entrada en vigor de la Ley de Protección de Datos Personales, sin perjuicio de que los derechos de las personas titulares sean plenamente exigibles desde la fecha de inicio de vigencia de la ley.

3.3. Tipos de finalidad en el tratamiento.

3.3.1. Pequeñas y medianas empresas.

La Comisión analizó el régimen especial aplicable a las micro, pequeñas y medianas empresas, destacando que el artículo 14 septies de la Ley N° 21.719 introduce una innovación relevante al permitir la modulación de los estándares de cumplimiento en función del tamaño, capacidades y riesgos asociados al tratamiento de datos personales. Este enfoque de proporcionalidad regulatoria busca compatibilizar la protección efectiva de los derechos de las personas con la viabilidad operativa y económica de organizaciones de menor escala, sin afectar el núcleo esencial del derecho a la protección de datos.

Dicha disposición faculta a la futura Agencia de Protección de Datos Personales a dictar instrucciones generales que establezcan estándares diferenciados, particularmente en materias como el deber de información y el principio de seguridad, considerando el tipo, volumen, naturaleza y finalidad de los datos tratados, así como la estructura y capacidades reales de los responsables. La Comisión observa que este régimen diferenciado no constituye una exención general de obligaciones, sino un ajuste proporcional que debe fundarse en una evaluación de riesgos, excluyendo de su aplicación a aquellos tratamientos que, por su naturaleza, impliquen un riesgo elevado para los derechos de las personas.

En este contexto, la Comisión advierte la necesidad de contar con criterios claros y homogéneos que permitan determinar cuándo resulta procedente la aplicación de estándares diferenciados, evitando interpretaciones extensivas o usos instrumentales del concepto de PYME, y asegurando una aplicación coherente, gradual y basada en riesgo del régimen especial.

Recomendaciones

> Precisar los criterios objetivos para determinar la procedencia de estándares diferenciados, considerando no solo umbrales económicos, sino también factores como el riesgo del tratamiento, la naturaleza de los datos tratados y la capacidad organizacional y técnica del responsable, para las consideraciones del régimen diferenciado y no solo los umbrales de facturación.

> Establecer orientaciones proporcionales en materia de seguridad, promoviendo un enfoque práctico y escalonado que permita a las PYMES implementar controles esenciales adecuados a su nivel de riesgo y complejidad operativa, considerando de manera coherente y complementaria los criterios y lineamientos definidos por la Agencia Nacional de Ciberseguridad (ANCI), con el objeto de asegurar consistencia técnica y regulatoria en el ecosistema nacional.

> Definir estándares mínimos de transparencia, asegurando que los titulares cuenten con información suficiente, clara y accesible focalizándose en las prácticas reales del tratamiento de sus datos, sin imponer cargas desproporcionadas.

> Incorporar ejemplos y casos orientativos que faciliten una aplicación uniforme del régimen diferenciado, reforzando la certeza jurídica y la cultura de cumplimiento.

> La Comisión recomienda fomentar la participación activa de las entidades gremiales y organizaciones representativas de micro, pequeñas y medianas empresas en el desarrollo de políticas y puesta a disposición de herramientas de cumplimiento y apoyo operativo en materia de protección de datos personales, promoviendo su colaboración en la elaboración, adaptación y difusión de instrumentos prácticos que faciliten la implementación de la ley en organizaciones de menor escala.

> Asimismo, se recomienda que la Agencia de Protección de Datos Personales cuente con una unidad especializada de atención a PYMES, orientada tanto al desarrollo y puesta a disposición de herramientas de cumplimiento simplificadas como a la atención preferente de consultas, dudas y requerimientos específicos de este segmento. Dicha unidad debería adoptar un enfoque preventivo y de acompañamiento, contribuyendo a reducir brechas de cumplimiento, fortalecer capacidades internas y promover una cultura de protección de datos proporcionado y sostenible en el sector PYME.

Cronograma de implementación

La Comisión recomienda que la elaboración y publicación de estas guías interpretativas generales se inicie dentro de los primeros seis meses siguientes a la entrada en vigor de la Ley de Protección de Datos Personales, de modo de acompañar tempranamente a las PYMES en el proceso de adecuación normativa, sin perjuicio de la plena exigibilidad de las obligaciones legales desde la fecha de inicio de vigencia de la ley.

3.3.2. Marketing directo

La Comisión analizó el tratamiento de datos personales con fines de marketing directo, captación de clientes y generación de oportunidades de negocio, constatando que estas actividades constituyen un interés lícito de las empresas, amparado por el derecho constitucional a desarrollar actividades económicas, siempre dentro del marco legal vigente. En el ordenamiento jurídico chileno, tanto la normativa de protección al consumidor como la legislación de protección de datos personales han optado históricamente por un modelo de opt-out, en virtud del cual las comunicaciones promocionales se encuentran permitidas por defecto, siempre que se garantice al titular un mecanismo claro, accesible y efectivo para oponerse o solicitar la suspensión de dichos envíos.

Este enfoque se refleja en la regulación sectorial aplicable a las comunicaciones comerciales y se ve reforzado por la nueva Ley de Protección de Datos Personales, que reconoce expresamente el derecho de oposición frente al marketing directo, permitiendo armonizar ambos cuerpos normativos. La Comisión observa que este modelo resulta coherente con las expectativas razonables de los titulares en el contexto nacional, quienes se encuentran habituados a recibir comunicaciones comerciales, en la medida en que éstas respeten los principios de transparencia, proporcionalidad y minimización de datos, y no generen consecuencias relevantes o intrusivas.

A diferencia de otros ordenamientos que adoptan un régimen de opt-in más estricto, el sistema chileno permite fundar estos tratamientos en el interés legítimo del responsable, siempre que exista una ponderación adecuada entre dicho interés y los derechos de los titulares, y que se asegure el ejercicio expedito de los derechos ARSOP, en particular los derechos de oposición y supresión cuando no exista una relación vigente que justifique la conservación de los datos.

Recomendaciones

> La Comisión recomienda que la futura Agencia de Protección de Datos Personales ejerza sus facultades interpretativas y considere la posibilidad de fundar en el interés legítimo los tratamientos de datos personales vinculados al marketing directo y a la promoción comercial, de conformidad con el modelo opt-out vigente en el ordenamiento chileno.

> Dichas guías deberían establecer criterios claros para asegurar que estos tratamientos se realicen de manera proporcional y no intrusiva, precisando la necesidad de contar con mecanismos efectivos, visibles y sencillos para el ejercicio del derecho de oposición y la baja de las comunicaciones, así como orientaciones sobre la supresión de datos cuando no exista una relación vigente entre las partes. Asimismo, debieran promover prácticas de transparencia reforzada y la adopción de medidas que eviten envíos excesivos o desalineados con las expectativas razonables de los titulares.

Cronograma de implementación

La Comisión recomienda que la elaboración y publicación de estas guías interpretativas generales se realice a partir de los seis meses siguientes a la entrada en vigor de la Ley de Protección de Datos Personales, con el objeto de otorgar certeza temprana a los responsables del tratamiento y asegurar una aplicación coherente del régimen de marketing directo, sin perjuicio de la exigibilidad inmediata de los derechos de las personas titulares desde la vigencia de la ley.

3.3.3 Compliance, prevención de delitos y fraudes.

La Comisión analizó el uso del interés legítimo como base de licitud para el tratamiento de datos personales con fines de prevención del fraude, del lavado de activos y de infracciones normativas, constatando que se trata de una finalidad ampliamente reconocida en el derecho comparado y en la práctica regulatoria internacional. En particular, se observa coherencia con los criterios del Comité Europeo de Protección de Datos y con el Considerando 47 del Reglamento General de Protección de Datos, que reconocen la prevención del fraude como un interés legítimo del responsable, siempre que su aplicación no sea automática y se ajuste a los principios de necesidad, proporcionalidad y finalidad determinada.

La Comisión constata que el ordenamiento jurídico chileno impone, en múltiples ámbitos, deberes de verificación, monitoreo y control que requieren necesariamente el tratamiento de datos personales, tanto en el sector público como en sectores regulados del ámbito financiero, comercial y administrativo. En estos casos, el tratamiento puede encontrar fundamento directo en una obligación legal o bien en un interés legítimo complementario a dicha obligación, cuando el uso de datos personales resulte indispensable para su cumplimiento efectivo.

Asimismo, se advierte que la realidad institucional chilena presenta una alta exposición a riesgos de fraude y una dependencia significativa de fuentes públicas y sectoriales para cumplir deberes legales de control, lo que refuerza la necesidad de contar con criterios claros que orienten el uso legítimo de esta base de licitud. No obstante, la Comisión enfatiza que solo los fraudes de entidad sustancial y

aquellos tratamientos estrictamente necesarios pueden justificar una injerencia relevante en los derechos de las personas titulares, debiendo siempre implementarse salvaguardas adecuadas.

Recomendaciones

> La Comisión recomienda que la futura Agencia de Protección de Datos Personales emita guías interpretativas generales que reconozcan y orienten la aplicación del interés legítimo en la prevención del fraude, del lavado de activos y de infracciones normativas, siguiendo criterios consolidados en la experiencia internacional y adaptándolos al contexto regulatorio nacional.

> Dichas guías deberían establecer, de manera clara y proporcional, que esta finalidad puede constituir una base de licitud válida siempre que el tratamiento sea estrictamente necesario, limitado a los datos indispensables, fundado en una finalidad específica y documentada, y sometido a una ponderación razonada frente a los derechos de los titulares. Asimismo, deberían promover la documentación del análisis de interés legítimo, la adopción de medidas de seguridad acordes al nivel de riesgo, la incorporación de supervisión humana en decisiones automatizadas relevantes y la integración de estos criterios en los modelos generales de cumplimiento y prevención de infracciones.

> La Comisión considera especialmente relevante que estas orientaciones distingan el rol de los prestadores de servicios de compliance y debida diligencia, precisando cuándo actúan como encargados del tratamiento y cuándo como responsables independientes, así como el eventual reconocimiento del interés legítimo de terceros especializados, siempre que se acrediten finalidades preventivas claras, proporcionalidad y garantías adecuadas.

Cronograma de implementación

La Comisión recomienda que la elaboración y publicación de estas guías interpretativas generales se realice a partir de los seis meses siguientes a la entrada en vigor de la Ley de Protección de Datos Personales, permitiendo a la Agencia desarrollar criterios técnicos consistentes y coordinados con el ecosistema regulatorio nacional, sin perjuicio de la exigibilidad inmediata de la ley una vez iniciada su vigencia.

3.3.4. Empresas públicas.

La Comisión analizó los desafíos que enfrenta la implementación del régimen de protección de datos personales en las empresas públicas, considerando que estas entidades desarrollan actividades de carácter empresarial bajo un mandato legal específico y, al mismo tiempo, forman parte de la Administración del Estado. Esta doble naturaleza implica que las empresas públicas tratan grandes volúmenes de datos personales en contextos operativos complejos, frecuentemente asociados a servicios esenciales, actividades económicas reguladas y relaciones contractuales masivas con personas naturales.

Asimismo, la Comisión constató que las empresas públicas presentan heterogeneidad relevante en cuanto a tamaño, giro, nivel de madurez institucional y capacidades técnicas, lo que dificulta una

aplicación uniforme de las obligaciones previstas en la Ley de Protección de Datos Personales sin orientaciones específicas. La ausencia de lineamientos sectoriales claros podría generar interpretaciones dispares, riesgos de incumplimiento y dificultades prácticas en la adecuación de sus procesos internos, especialmente en materias como gobernanza de datos, seguridad de la información, atención de derechos de los titulares y gestión de incidentes.

En este contexto, se estima necesario que la implementación de la ley en las empresas públicas considere su rol estratégico, su inserción en mercados regulados y las particularidades de su régimen jurídico, promoviendo una aplicación coherente y proporcional del marco normativo.

Recomendaciones

> Respecto de las empresas públicas o empresas con participación mayoritaria del Estado, se sugiere tomar medidas oportunas para determinar si estos organismos cuentan con los recursos materiales y humanos y la madurez digital necesarios para la correcta implementación de la ley.

> La Comisión recomienda que la futura Agencia de Protección de Datos Personales emita lineamientos sectoriales específicos para las empresas públicas, para lo cual podrá coordinarse con el Sistema de Empresas Públicas (SEP), orientados a apoyar su proceso de implementación y adecuación al nuevo régimen de protección de datos personales. Dichos lineamientos deberían proporcionar criterios claros y prácticos sobre la aplicación de las obligaciones legales en el contexto de actividades empresariales desarrolladas bajo mandato público, resguardando la coherencia con los principios de legalidad, eficiencia y continuidad del servicio.

> Asimismo, se recomienda que estas orientaciones faciliten la adopción de modelos de gobernanza de datos, políticas internas y medidas de seguridad acordes al nivel de riesgo y a la naturaleza de las operaciones de las empresas públicas, promoviendo estándares homogéneos y evitando soluciones fragmentadas. Estas directrices debieran contribuir a fortalecer la certeza jurídica, la rendición de cuentas y la protección efectiva de los derechos de las personas titulares de datos personales.

> Asimismo, y teniendo presente la recomendación de neutralidad competitiva de la OCDE respecto de las empresas públicas, esta Comisión considera que el régimen de protección de datos aplicable a las empresas de propiedad del Estado, incluso a aquellas que tengan la calidad de empresas públicas creadas por ley, es el régimen general aplicable a los responsables de datos, y no el régimen especial establecido en el capítulo IV de la ley N° 19.628 en su texto reformado. Esta conclusión es consistente, además, con lo establecido en el artículo 6° inciso segundo de la LOCBGAE.

Cronograma de implementación

La Comisión recomienda que la elaboración y publicación de los lineamientos sectoriales para empresas públicas se realice a partir del sexto mes contado desde la entrada en vigor de la Ley de Protección de Datos Personales, permitiendo a la Agencia contar con una base inicial de experiencia y criterios generales, y otorgando a las empresas públicas orientaciones oportunas para una implementación gradual y ordenada del nuevo régimen.

4. Agencia de Protección de Datos y sus Potestades.

4.1. Certificación del modelo de prevención de infracciones:

La Comisión analizó el diseño institucional del régimen de certificación del Modelo de Prevención de Infracciones, previsto como un instrumento clave para fortalecer el cumplimiento preventivo de la Ley N° 19.628 y su modificación por la Ley N° 21.719. Dicho modelo constituye, por su naturaleza, un mecanismo de gestión de riesgos corporativos, construido sobre información interna altamente sensible, incluyendo matrices de riesgo, controles internos, indicadores y procesos estratégicos.

En este contexto, la Comisión advirtió que concentrar en la propia Agencia de Protección de Datos Personales la revisión detallada de los componentes internos del modelo podría generar tensiones con su rol fiscalizador y sancionador, afectando la percepción de imparcialidad, objetividad y confianza del sistema. Esta situación resulta comparable a los riesgos que se habrían producido si, en el ámbito penal, la aprobación de los modelos de prevención de delitos hubiese recaído directamente en el órgano persecutor. Desde la perspectiva del principio de objetividad administrativa, se estima preferible que la Agencia ejerza un rol de supervisión y certificación final, sobre la base de evaluaciones técnicas previas realizadas por terceros independientes.

Recomendaciones

> La Comisión recomienda que la instrucción general que regule el régimen de certificación del Modelo de Prevención de Infracciones reconozca expresamente la posibilidad de incorporar terceros evaluadores independientes como parte del proceso, bajo estándares definidos y supervisados por la propia Agencia.

> En particular, se recomienda que dicha instrucción general:

- Establezca un régimen de terceros evaluadores habilitados para revisar y evaluar los componentes del modelo de prevención, conforme a los criterios técnicos y metodológicos que determine la Agencia.
- Defina requisitos claros de independencia, idoneidad y competencia técnica para dichos evaluadores, ya sean personas naturales o jurídicas, quienes deberán emitir informes de evaluación previa.
- Cree un sistema de acreditación o registro de evaluadores, administrado y supervisado por la Agencia, que permita asegurar estándares homogéneos y confiables.
- Mantenga a la Agencia de Protección de Datos Personales como autoridad certificadora final, encargada de verificar la suficiencia formal y técnica de los antecedentes presentados y de emitir la resolución de certificación correspondiente.

> La Comisión recomienda que la Agencia de Protección de Datos Personales promueva una modificación legal que consolide y otorgue estabilidad al sistema de certificación del Modelo de Prevención de Infracciones, entregando la evaluación técnica de dichos modelos a entidades privadas acreditadas, bajo estándares definidos y supervisados por la propia Agencia. Este enfoque permitiría que la Agencia concentre sus recursos y capacidades en su rol esencial de supervisión,

orientación regulatoria y fiscalización, evitando sobrecargar su estructura con funciones de auditoría técnica u operativa, y fortaleciendo al mismo tiempo la confianza, imparcialidad y eficiencia del sistema de cumplimiento.

Cronograma de implementación

La Comisión recomienda que la instrucción general que regule el régimen de certificación del Modelo de Prevención de Infracciones sea elaborada y puesta en vigencia a partir del primer mes contado desde la instalación de la Agencia de Protección de Datos Personales.

4.2. Interpretación de la norma infra legal como base de licitud

La Comisión analizó el problema relativo a si la normativa reglamentaria o infra legal puede constituir una base de licitud suficiente para el tratamiento de datos personales cuando dicha normativa se funda en una habilitación legal previa. En los casos examinados, la obligación cuyo cumplimiento se exige por vía de una norma infra legal tiene su origen en una ley, correspondiendo a la regulación infra legal determinar las modalidades, medios o condiciones específicas para dar cumplimiento a dicho mandato legal.

En este sentido, la operación de tratamiento de datos que impone o desarrolla la norma infra legal no constituye una obligación autónoma, sino que se inserta como un instrumento necesario para ejecutar la finalidad establecida por la norma legal de base. La regulación infra legal suele detallar categorías de datos, procedimientos, plazos o mecanismos de reporte indispensables para la aplicación práctica de la ley.

La Comisión constata que este debate se vincula con una de las cuestiones clásicas del derecho público chileno: el alcance de la reserva legal en materia de derechos fundamentales. Bajo una concepción de reserva legal absoluta, la autoridad administrativa sectorial carecería de competencia para regular, incluso de manera complementaria, las condiciones del tratamiento de datos personales, por tratarse de una materia constitucionalmente reservada al legislador. En cambio, bajo una concepción de reserva legal relativa, resulta admisible la colaboración normativa de la administración para complementar, desarrollar o detallar la regulación legal, tanto en la Ley N° 19.628 como en las leyes sectoriales que atribuyen competencias a las autoridades administrativas. Al respecto, esta Comisión ha tenido presente el hecho de que el propio Tribunal Constitucional ha señalado que, incluso respecto de la regulación relativa a derechos fundamentales no excluye la colaboración reglamentaria, por lo que el legislador puede delegar en normas infralegales la regulación de deberes y del ejercicio de potestades que se relacionen con aquéllos[1], salvo en los casos en que la Constitución lo haya dispuesto expresamente[2].

El tratamiento de datos personales que se habilite a través de una norma infralegal o de la potestad normativa de la Administración, que faculta a la autoridad administrativa para dictar normas que sean coadyuvantes de la ley, que permitan una mejor aplicación de la misma, tales como los reglamentos,

[1] STC 1453-2023.
[2] STC 480-2006.

las resoluciones y las instrucciones. Configurando una atribución de la que gozan diversos órganos de la Administración del Estado o servicios públicos, tales como las superintendencias, la Comisión para el Mercado Financiero u otras entidades regulatorias precisamente como la futura Agencia de Protección de Datos Personales.

La Comisión subraya que este debate incide principalmente en la juridicidad y constitucionalidad de la normativa infra legal que ordena realizar determinados tratamientos de datos, y no necesariamente en la licitud del tratamiento mismo. En efecto, la licitud del tratamiento deriva de la ley habilitante, mientras que la norma infra legal, derivada de la potestad normativa de la Administración, cumple una función de especificación operativa lo que debe ser determinado caso a caso. A mayor abundamiento, los regulados están obligados a dar cumplimiento a las instrucciones de los reguladores los que, a su vez, ejercen sus atribuciones por disposición de la ley.

Recomendaciones

> La Comisión recomienda que la futura Agencia de Protección de Datos Personales ejerza sus atribuciones para interpretar las autorizaciones generales y especiales de tratamiento de datos personales aplicables a los regulados y definir el alcance en virtud del cual la ley, detallada y complementada por una norma reglamentaria, constituye base de licitud suficiente para tratar los datos personales como se instruya en el ejercicio de sus competencias.

> Esta interpretación permite compatibilizar el respeto al principio de legalidad con la necesidad de contar con regulaciones técnicas y operativas dictadas por autoridades sectoriales competentes, evitando vacíos normativos y asegurando la eficacia de políticas públicas que requieren tratamiento de datos personales.

Cronograma de implementación

La Comisión recomienda que la Agencia de Protección de Datos Personales emita estos criterios interpretativos dentro de los tres meses siguientes a su instalación, atendida la relevancia transversal de esta definición para la aplicación del régimen de licitud del tratamiento de datos personales y para la coordinación con la normativa sectorial vigente.

4.3. Potestades de fiscalización

En el sistema chileno, los órganos de control con facultades sancionadoras o lo que en la experiencia comparada se denominan las agencias regulatorias independientes, tienen un alto grado de especialización, encontrándose circunscrito su ámbito de intervención sobre un mercado, industria o interés específico o general, el que puede o no ser transversal. En este caso, la Agencia de Protección de Datos Personales tiene como interés específico a regular, la autodeterminación informativa, que además es transversal porque consideraría tanto el tratamiento de datos que realicen entidades públicas como privadas en cualquier actividad o sector.

La Comisión analizó las potestades de fiscalización administrativa atribuidas a la Agencia de Protección de Datos Personales, entendiendo que la fiscalización no se reduce a una mera

observación o monitoreo de hechos, sino que constituye una actividad jurídica destinada a verificar el cumplimiento efectivo de marcos normativos definidos por parte de los sujetos regulados, dentro del ámbito de competencia del órgano fiscalizador. En este sentido, la fiscalización configura una relación jurídica específica entre funcionarios fiscalizadores, entidades fiscalizadas y un objeto claramente delimitado, consistente en el tratamiento y protección de los datos personales.

El análisis de la Ley N° 21.719 permite constatar que la Agencia ejerce una fiscalización de carácter transversal y horizontal, no asociada a un sector económico específico, sino definida por el objeto regulado y por el amplio ámbito de aplicación territorial de la ley. Este diseño habilita a la Agencia a fiscalizar tratamientos de datos personales realizados tanto en el territorio nacional como en contextos transfronterizos, cuando se verifiquen los supuestos establecidos por la ley, lo que amplía significativamente el espectro de sujetos y operaciones fiscalizables.

Asimismo, la Comisión observa que el centro de gravedad de la actividad fiscalizadora de la Agencia es de carácter documental, en la medida en que la ley le otorga expresamente la facultad de requerir documentos, antecedentes y toda información necesaria para verificar el cumplimiento normativo. A diferencia de otros organismos sectoriales, la ley no contempla de manera explícita potestades de inspección in situ o intrusivas, lo que resulta coherente con la naturaleza intangible del objeto fiscalizado —el tratamiento de datos personales—, el cual no necesariamente se encuentra asociado a un lugar físico determinado.

La Comisión advierte, además, que la Agencia combina funciones de fiscalización y sanción, lo que exige que el ejercicio de la potestad fiscalizadora se desarrolle bajo estándares estrictos de legalidad, objetividad y debido proceso, especialmente considerando que la fiscalización puede dar lugar a procedimientos sancionatorios. En este contexto, se estima relevante distinguir conceptualmente entre las funciones de fiscalización, sanción y asistencia al cumplimiento, cada una de las cuales responde a lógicas y objetivos distintos.

Asimismo, la Comisión observa que la Agencia también se encuentra dotada de potestades relativas a la promoción del cumplimiento de la ley, la que requiere de un trabajo conjunto y colaborativo entre la APDP y las entidades sujetas a su fiscalización. Para que este trabajo colaborativo sea eficaz y constituya una verdadera ayuda para que los responsables de datos adecuen sus actividades de tratamiento a la ley, podría ser conveniente que la APDP adopte una organización interna que permita separar sus actividades de cumplimiento de aquellas dirigidas a la fiscalización y aplicación de sanciones, tal como sucede en otros organismos fiscalizadores, como la Fiscalía Nacional Económica.

Finalmente, se constató que la ley no establece un estatuto especial para el personal fiscalizador de la Agencia, ni regula de manera específica potestades inspectivas, deberes reforzados o calidades especiales de los funcionarios, lo que refuerza la necesidad de dotar de claridad procedimental y predictibilidad al modelo de fiscalización, en coherencia con una cultura del cumplimiento de carácter preventivo. El otorgamiento de potestades inspectivas y de calidades especiales a los funcionarios, requeriría tanto de una modificación legal como de la asignación de mayores recursos para la APDP.

Recomendaciones

> La Comisión recomienda que la Agencia de Protección de Datos Personales emita instrucciones generales que desarrollen y precisen el ejercicio de sus potestades de fiscalización, con el objeto de otorgar certeza jurídica a las entidades reguladas y fortalecer una aplicación coherente y proporcional del marco normativo.

> En particular, se recomienda que la Agencia defina y publique criterios generales sobre el modelo de fiscalización, distinguiendo claramente entre fiscalizaciones individuales y planes de fiscalización sectoriales o temáticos, así como los alcances del requerimiento de información documental como principal herramienta fiscalizadora.

> Asimismo, se sugiere que dichos instrumentos clarifiquen la relación entre promoción del cumplimiento, fiscalización y procedimiento sancionatorio, reforzando la separación funcional entre ambas etapas y promoviendo una aproximación preventiva orientada a la mejora del cumplimiento normativo.

> En el mismo sentido, la Comisión recomienda que, en ejercicio de sus actividades de difusión y promoción del cumplimiento, la Agencia dicte instrucciones generales en materias tales como notificación de incidentes, estándares de seguridad, anonimización y seudonomización, uso secundario de datos obtenidos a través de consentimiento del titular. Asimismo, se considera útil, especialmente en el primer período de aplicación de la ley, una instrucción que aborde específicamente el interés legítimo y de cuenta de algunos casos paradigmáticos de su concurrencia, a modo de ilustración. Asimismo, se sugiere que la APDP considere la conveniencia de dictar instrucciones para sectores especialmente sensibles, como el ámbito de la salud, laboral, el tratamiento de datos de niños, niñas y adolescentes, y el otorgamiento de ayudas sociales, así como del interés legítimo en el tratamiento de datos personales para uso científico. Respecto del tratamiento de datos en el sector público, se estima especialmente relevante emitir orientaciones respecto de la interoperabilidad de los datos que los organismos públicos tratan y la adopción de medidas de minimización y seguridad del tratamiento.

> Adicionalmente, la Comisión estima deseable que la Agencia adopte una planificación explícita de su actividad fiscalizadora, mediante la publicación de planes o políticas de fiscalización, que permitan anticipar prioridades, criterios de selección y enfoques de riesgo, contribuyendo así a la promoción de una cultura de cumplimiento y a la eficiencia en el uso de los recursos institucionales.

> Una planificación similar debería producirse respecto de la difusión de la nueva regulación, la que podría realizarse en coordinación con municipalidades y establecimientos educacionales, como una vía directa de contacto con la ciudadanía.

> La Comisión estima necesaria, en el mediano plazo, una modificación legal que incorpore expresamente facultades inspectivas a la Agencia de Protección de Datos Personales, atendida la naturaleza y complejidad creciente de los tratamientos de datos personales y las limitaciones inherentes a un modelo de fiscalización basado predominantemente en el requerimiento de

información documental. En un contexto caracterizado por operaciones digitales, tratamientos automatizados, infraestructuras distribuidas y servicios transfronterizos, la sola revisión de antecedentes escritos o de declaraciones, puede resultar insuficiente para verificar de manera efectiva el cumplimiento de las obligaciones legales, especialmente en materias técnicas como seguridad de la información, control de accesos, trazabilidad y gestión de incidentes. Sin perjuicio de la facultad para requerir a quienes realicen tratamiento de datos personales la entrega de cualquier documento, libro o antecedente y toda la información que fuere necesaria para el cumplimiento de su función fiscalizadora, ausencia de otras potestades inspectivas expresas limita la capacidad de la Agencia para constatar directamente situaciones de incumplimiento que solo pueden evidenciarse a través de verificaciones técnicas u operativas, reduciendo la eficacia preventiva y disuasiva del sistema de protección de datos personales. La incorporación de estas facultades permitiría alinear el marco institucional con estándares comparados aplicables a autoridades de fiscalización transversal, fortalecer la credibilidad del régimen de cumplimiento y otorgar mayores garantías de protección efectiva de los derechos de las personas, siempre bajo una regulación legal expresa que resguarde los principios de legalidad, proporcionalidad y debido proceso.

Cronograma de implementación

La Comisión recomienda que la elaboración y publicación de los instrumentos que regulen y orienten el ejercicio de la potestad fiscalizadora de la Agencia se realice dentro de los tres meses siguientes a la instalación de la Agencia de Protección de Datos Personales, permitiendo dotar tempranamente de predictibilidad y coherencia al modelo fiscalizador, sin perjuicio del ejercicio inmediato de las facultades legales de fiscalización desde el inicio de sus funciones.

WWW.MINSEGPRES.GOB.CL

Ministerio Secretaría General de la Presidencia

Gobierno de Chile

WWW.MINSEGPRES.GOB.CL