

PARA: Ministra Macarena Lobos Palacios.

ASUNTO: Cuarto informe de la Comisión de Implementación para la Ley de Protección de Datos personales

FECHA: 16 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.	REDIAC CCS

	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.	
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
04.12.2025	Coordinación regulatoria. Aplicación de la ley en empresas públicas Interpretaciones y nudos críticos en la seguridad social.	CMF SEP SUSESO
11.12.2025	Régimen de adecuación y las transferencias internacionales de datos, las exigencias de localización de datos, los mecanismos de intercambio de información y cooperación con otros organismos, los desafíos de implementación incluida la capacidad técnica y de dotación para la investigación y fiscalización.	U.S. Department of Commerce

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 %

Actividad laboral o económica	
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.

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 aquéllos¹, salvo en los casos en que la Constitución lo haya dispuesto expresamente².

¹ STC 1453-2023.

² STC 480-2006.

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, 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.