IMPACTOS OPERACIONALES DE LA NUEVA LEY DE PROTECCIÓN DE DATOS CHILENA

El Proyecto de Ley que "Regula la protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales" (la "**Nueva Ley**"), modifica casi íntegramente la antigua Ley sobre Protección de la Vida Privada del año 1999 ("**LPD**"), modernizando la regulación nacional de datos personales, y estableciendo, por primera vez, una autoridad directamente encargada de velar por su cumplimiento. Su entrada en vigor obliga a las empresas a ajustar o diseñar nuevos procesos operacionales, técnicos y organizacionales, para cumplir con un renovado conjunto de obligaciones**.**

En concreto, la Nueva Ley modifica por completo los principios, las fuentes de licitud que autorizan y habilitan el tratamiento de datos, establece nuevos derechos para los titulares de datos, junto con nuevas sanciones y procedimientos para los incumplidores, que, en definitiva, imponen inéditas cargas y obligaciones a las entidades responsables del tratamiento de datos personales.

Este documento presenta los principales impactos en la operación de las empresas que la entrada en vigor de la Nueva Ley trae consigo, con la finalidad de asistirlos en la planificación del proceso de adecuación de sus prácticas, procedimientos, controles y normativa interna de tratamiento de datos.

NOTA: A la fecha de publicación de este documento, el Proyecto de Ley ha terminado su discusión en tercer trámite constitucional y ha sido aprobado en las salas del Senado y la Cámara de Diputadas y Diputados; estando pendiente solamente el control de constitucionalidad ante el Tribunal Constitucional, antes de ser promulgada y publicada. (26 de agosto de 2024)

Contacto:
Paulina Silva | psilva@bitlaw.cl
Javiera Sepúlveda | jsepulveda@bitlaw.cl

1. NUEVAS BASES DE LICITUD PARA TRATAR DATOS PERSONALES

La actual LPD contemplaba como bases de licitud únicamente a la autorización legal y el consentimiento del titular. Uno de los cambios protagonistas en la Nueva Ley es la consagración de nuevas "bases de licitud" o habilitantes legales que permiten el tratamiento de datos personales:

i. **Consentimiento** libre, específico e informado del titular, que deberá manifestarse de forma previa e inequívocamente mediante una declaración verbal, escrita o por un medio electrónico equivalente o mediante un acto afirmativo del titular.
ii. **Ejecución o cumplimiento de una obligación legal** o cuando exista directamente una autorización legal para el tratamiento;
iii. Tratamiento de **datos relativos a obligaciones de carácter económico, financiero, bancario o comercial**, incluyendo los datos referidos a la situación socioeconómica del titular, siempre que se haga en conformidad con lo dispuesto en el Titulo III de la Nueva Ley;
iv. Tratamiento de datos necesario para la **celebración o ejecución de un contrato** entre el responsable y el titular, incluyendo medidas precontractuales;
v. Tratamiento de datos necesario para la satisfacción de **intereses legítimos** que no afecten los derechos y libertades del titular; y
vi. Tratamiento de datos necesario para la **formulación, ejercicio o defensa de un derecho** ante los tribunales de justicia u órganos públicos.

IMPACTOS OPERACIONALES DE LAS NUEVAS BASES DE LICITUD

✓ ***Clasificación de datos y asignación de bases de legalidad.*** **En** términos prácticos, los responsables deberán **identificar sus tratamientos de datos, para luego asociarlos a la base de legalidad correspondiente**, que justifica el uso del dato para una determinada finalidad.

La clasificación de las actividades de tratamiento, los propósitos de uso y las distintas categorías de datos personales que el responsable trata, asociada a las bases de licitud que correspondan, es una operación técnica compleja que puede tomar tiempo y recursos considerables para las organizaciones que no tengan inventarios o catálogos de datos actualizados. Esta actividad de clasificación, más que una "buena práctica" es un requisito legal derivado, entre otros, del nuevo artículo 14 ter (d), que al enumerar los elementos de un aviso de privacidad en el deber de transparencia, señala que se debe comunicar "*d) Las categorías, clases o tipos de datos que trata; (…), las finalidades de los tratamientos que realiza; la base de legitimidad del tratamiento; y en caso de tratamientos que se basan en la satisfacción de intereses legítimos, cuáles serían estos*".

✓ ***El consentimiento pierde protagonismo.*** La diversidad de bases de licitud que ofrece la Nueva Ley llevará a que, **en la práctica, los responsables del tratamiento de datos puedan, en ciertas actividades de tratamiento, prescindir de la recogida del consentimiento**. Así, por ejemplo, los tratamientos que antes sólo podían ser amparados en el consentimiento bajo la Nueva Ley podrían justificarse, por ejemplo, en el cumplimiento de un contrato (como podría ser el contrato de trabajo, o un contrato de prestación de servicios donde el tratamiento de datos sea consustancial al cumplimiento del contrato), o en el interés legítimo (como podría suceder con los tratamientos necesarios para la prevención de fraude o por motivos de seguridad). Sin perjuicio de ello, **las nuevas bases de legalidad deben siempre cumplir con requisitos para su validez.**

✓ ***Cuando la base de legalidad deba ser el consentimiento,*** su nuevo requisito de libertad puede ponerse en riesgo

- en escenarios de recogida atada o condicional para múltiples propósitos,
- en escenarios donde el desequilibrio de las partes permita cuestionar la libertad del titular en consentir,
- o cuando se requiera el consentimiento para propósitos que no son consustanciales al objeto del contrato o la prestación del servicio con ocasión del cual se requiere este consentimiento, como suele ocurrir con los fines de marketing.

2.NUEVOS PRINCIPIOS Y SU RELEVANCIA PRÁCTICA

La Nueva Ley recoge, en forma expresa y detallada, un listado de principios que regulan el tratamiento de los datos personales, que buscan orientar a responsables y encargados en *cómo* cumplir las obligaciones, y guiar la interpretación de las autoridades en su supervisión y fiscalización.

PRINCIPIO DE LICITUD Y LEALTAD

Los datos personales sólo pueden tratarse de manera lícita y leal.

✓ ***¿Cómo impacta en la operación?*** El responsable de datos debe poder demostrar que cuenta con una base de licitud que justifica el tratamiento que realiza. Por ello, será indispensable **que los responsables de datos identifiquen** las fuentes de recolección de los datos personales, los propósitos de los tratamientos, y las bases de licitud asociadas a cada tratamiento. Una herramienta útil para este propósito será la elaboración de un **Registro de Actividades de Tratamiento** ("RAT").

PRINCIPIO DE FINALIDAD

Los datos personales sólo se pueden recolectar con fines específicos, explícitos y lícitos.

✓ ***¿Cómo impacta en la operación?*** No se podrán tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que se trate de algún fin claramente compatible. Los fines del tratamiento deben informarse claramente al titular y deben ser específicos, sin declaraciones genéricas o abiertas en los avisos de privacidad.

Para ello, la organización debe ser capaz de identificar o etiquetar sus datos en relación con los propósitos autorizados para ellos, e implementar medidas para evitar que los datos se usen para fines diferentes.

PRINCIPIO DE PROPORCIONALIDAD

Los datos personales deben limitarse estrictamente a los necesarios, adecuados y pertinentes a los fines del tratamiento, y no deben conservarse por más tiempo que el necesario cumplir con esos fines.

✓ ***¿Cómo impacta en la operación?*** Bajo la Nueva Ley se considera una infracción grave (multa de hasta 10.000 UTM) efectuar tratamientos innecesarios en relación con los fines correspondientes, por lo que los responsables deberán **asegurarse que los datos utilizados en cada operación sean siempre los estrictamente necesarios, adecuados y pertinentes en relación con los fines respectivos**. Para ello, será altamente recomendable que las empresas implementen procesos que favorezcan la **minimización de datos,** preparar e implementar **políticas de control de acceso** para evitar el acceso y comunicaciones excesivas o innecesarias de datos personales durante la ejecución de procesos internos de la empresa.

PRINCIPIO DE RESPONSABILIDAD

Quien realiza el tratamiento es legalmente responsable del cumplimiento y debe acreditarlo

✓ ***¿Cómo impacta en la operación?*** La carga de la prueba del cumplimiento de las obligaciones recaerá siempre en el responsable, quien **debe no solo cumplir, sino estar preparado para demostrar que cumple.**

- En el principio de legalidad: El responsable deberá ser capaz de acreditar la licitud del tratamiento de datos personales que realiza (Art. 3 letra a).
- En las bases de licitud: El responsable deberá acreditar la licitud del tratamiento de datos (Art. 13).
- En obligaciones de seguridad: el responsable debe acreditar la existencia y el funcionamiento de las medidas de seguridad (Art. 14 quinquies)
- En transferencia internacional: Corresponderá al responsable de datos que efectuó la transferencia internacional de datos, acreditar que ésta se practicó de conformidad a las reglas (Art. 28)

PRINCIPIO DE TRANSPARENCIA: EL AVISO DE PRIVACIDAD

El responsable debe entregar al titular toda la información necesaria para el ejercicio de sus derechos y que les permita entender en detalle las prácticas del tratamiento de sus datos.

✓ ***¿Cómo impacta en la operación?*** La entrega y facilitación de esta información se traduce en la redacción y disponibilización de sus políticas de tratamiento de datos, la principal de ellas (pero no la única) el aviso de privacidad. La redacción debe ser clara e inequívoca y la accesibilidad debe ser permanente y gratuita. Así, por ejemplo:

- Las políticas de privacidad de clientes deben estar disponibles en los sitios web de un e-commerce
- Las políticas de privacidad de trabajadores deben estar disponibles en la intranet de la organización
- Las políticas de aplicación corporativa deben ser conocidas, accesibles y sencillas

✓ ***Contenido mínimo de las políticas de privacidad.*** La Nueva Ley establece un contenido mínimo – bastante extenso – de la información a entregar al titular en la política de privacidad (Art. 14 ter). Esto incluye, entre otros: la individualización del responsable y sus datos de contacto, su representante legal y la identificación del encargado de prevención, si existiere; la identificación del medio tecnológico mediante el cual los titulares puedan realizar sus solicitudes; las medidas de seguridad; el periodo durante el que se conservarán los datos personales; la existencia de decisiones automatizadas, incluida la elaboración de perfiles.

PRINCIPIO DE CONFIDENCIALIDAD

El responsable y quienes tengan acceso a los datos deben guardar secreto de estos incluso aun después de finalizar la relación con el titular.

✓ ***¿Cómo impacta en la operación?*** Los responsables deben establecer controles para que sus dependientes o proveedores que accedan a los datos, cumplan el deber de secreto o confidencialidad. Lo anterior implica, por ejemplo, adecuar las cláusulas de confidencialidad con trabajadores y proveedores que traten datos personales en calidad de mandatarios.

El principio de confidencialidad se encuentra íntimamente relacionado con los deberes de seguridad, y su no observancia se sanciona como infracción grave (multa de hasta 10.000 UTM).

3. NUEVO CATÁLOGO DE DERECHOS DE LOS TITULARES

Los derechos de los titulares (antiguamente llamados derechos ARCO) son la piedra angular de una regulación esencialmente protectora como la de privacidad. La Nueva Ley modifica este catálogo reconociendo nuevos derechos y robusteciendo otros.

DERECHO DE ACCESO

Para saber si sus datos están siendo objeto de tratamiento, su origen, la finalidad del tratamiento, las categorías de destinatarios, el plazo de conservación y la lógica aplicada a la toma de decisiones automatizadas si aplicare.

Los responsables deben siempre entregar la información solicitada, salvo disposición legal en contrario.

DERECHO DE RECTIFICACIÓN

Para solicitar la modificación de datos inexactos, desactualizados o incompletos.

Rectificados que sean los datos, los responsables deberán comunicar la rectificación a los terceros a los que los hubiese comunicado o cedido, salvo cuando aquello represente un esfuerzo desproporcionado.

DERECHO DE CANCELACIÓN

Para solicitar la eliminación ("cancelación" o "supresión") de los datos, bajo ciertas circunstancias.

El titular puede solicitar la eliminación de sus datos cuando éstos ya no sean necesarios para los fines que fueron recopilados; cuando se revoque el consentimiento; cuando los datos sean obtenidos o tratados ilícitamente; cuando los datos estén caducos; cuando deban suprimirse para el cumplimiento de una sentencia u obligación legal y cuando se hubiese ejercido el derecho de oposición y no exista otra base de licitud para su tratamiento.

Bajo ciertos escenarios **no procederá este derecho**, incluyendo cuando el tratamiento sea necesario (i) para ejercer el derecho a las libertades de emitir opinión y de informar; (ii) para el cumplimiento de una obligación legal o contractual; (iii) por razones de interés público en el área de la salud pública; o (iv) para el ejercicio de una reclamación administrativa o judicial.

DERECHO DE OPOSICIÓN

Para oponerse a un tratamiento específico o determinado de sus datos, bajo ciertas circunstancias.

Puede un titular oponerse a un tratamiento específico de sus datos, cuando éste se fundamente en el interés legítimo del responsable de datos; cuando se realice solo con fines

de marketing directo; o respecto de datos obtenidos de una fuente de acceso público, sin otra base de licitud.

DERECHO DE OPOSICIÓN A DECISIONES INDIVIDUALES AUTOMATIZADAS Y ELABORACIÓN DE PERFILES

Para no ser objeto de decisiones, basadas en el tratamiento automatizado de sus datos personales, cuando produzca efectos jurídicos en él o le afecten significativamente.

No existirá este derecho cuando

- La decisión sea necesaria para la celebración o ejecución de un contrato
- Exista consentimiento del titular
- Lo señale la ley

Sin embargo, el responsable siempre debe facilitar el derecho del titular a obtener una explicación, la intervención humana, a expresar su punto de vista y a solicitar la revisión de la decisión.

DERECHO DE BLOQUEO

Para solicitar la suspensión temporal del tratamiento cuando se formule una solicitud de rectificación, supresión u oposición, y mientras ésta no se resuelva.

DERECHO A LA PORTABILIDAD

Para solicitar una copia de sus datos en un formato electrónico genérico e interoperable, y a comunicarlos o transferirlos a otro responsable.

▪ IMPACTOS OPERACIONALES DEL EJERCICIO DE ESTOS DERECHOS

✓ Se deberán preparar protocolos para la recepción de solicitudes de ejercicio de derechos ARCO, identificando a los stakeholders involucrados la recepción, calificación, procesamiento y respuesta de las solicitudes

✓ La información relativa a los titulares debe estar debidamente organizada y clasificada, para permitir responder oportunamente a las solicitudes.

✓ Se deberá establecer medidas de autenticación para asegurarse que no ocurran brechas de seguridad por el ejercicio de derechos ARCO de parte de titulares fraudulentos.

✓ La Nueva Ley requiere que los responsables implementen "*mecanismos y herramientas tecnológicas*" que permitan que el titular ejerza sus derechos en forma expedita, ágil y eficaz. De este modo, por ejemplo, **la exigencia al titular de ejercer sus derechos en forma presencial en una sucursal será ilegal.**

✓ *Plazo*. Los responsables de datos deben acusar recibo y pronunciarse por escrito **en 30 días corridos** desde el ingreso de la solicitud, teniendo en consideración además que el titular podría solicitar el bloqueo temporal de sus datos.

4. CIBERSEGURIDAD: ADOPCIÓN DE MEDIDAS DE SEGURIDAD

La Nueva Ley impone importantes y estrictas obligaciones a los responsables y mandatarios de adoptar medidas de seguridad apropiadas al tratamiento específico (Art. 14 quinquies).

La elección de estas medidas debe tomar en cuenta la naturaleza de los datos, el estado actual de la técnica y los costos de aplicación; la naturaleza, alcance, contexto y fines del tratamiento, la probabilidad de ocurrencia de riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados.

Las medidas de seguridad deben ser no solo **técnicas**, sino también **organizativas**, que permitan garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas para evitar la alteración, destrucción, pérdida, tratamiento o accesos no autorizados.

Los obligados directos a implementar medidas de seguridad son **tanto responsables como encargados.**

La falta de adopción de medidas de seguridad puede considerarse una **circunstancia agravante de la responsabilidad** en caso de infracciones (bajo la hipótesis de "*haber puesto en riesgo la seguridad de los derechos y libertades de los titulares en relación a sus datos personales*") lo que se tomará en cuenta al determinar el monto de las multas.

▪ IMPACTOS OPERACIONALES DE LA OBLIGACIÓN DE IMPLEMENTAR MEDIDAS DE SEGURIDAD

✓ ***La prueba es del responsable.*** La carga de la prueba de la existencia y el funcionamiento de las medidas de seguridad será siempre del responsable.

✓ ***La ley sugiere medidas de seguridad,*** como la seudonimización y el cifrado de datos; la capacidad de garantizar la confidencialidad, disponibilidad, integridad y resiliencia de los sistemas y servicios de tratamiento; restaurar la disponibilidad y el acceso a los datos en casos de incidentes de seguridad; llevar a cabo procesos de verificación, evaluación y valoración de las medidas, entre otras.

✓ ***Coordinación desde el origen con equipos de TI y de seguridad de la información.*** En estas obligaciones se requiere identificar las sinergias entre los equipos de compliance o

legales, y los equipos técnicos; pues el trabajo de una sola de las áreas no será suficiente para acreditar una diligencia integral.

✓ ***Revisión de Políticas de Seguridad de la Información.*** Será necesario revisar y actualizar las políticas de seguridad de la información y sus procedimientos o protocolos asociados, para hacerlas coherentes con el cumplimiento de las nuevas obligaciones.

5. OBLIGACIÓN DE REPORTAR BRECHAS DE SEGURIDAD

La Nueva Ley impone un deber concreto de informar a la Agencia –y también directamente a los titulares cuando se afecten datos sensibles, de menores de 14 años o relativos a obligaciones de carácter económico, financiero, bancario o comercial– por los medios más expeditos posibles y sin dilaciones indebidas, de las vulneraciones a las medidas de seguridad que impliquen un riesgo razonable para los derechos y libertades de los titulares y que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que se traten o la comunicación o acceso no autorizados a dichos datos.

El incumplimiento de esta obligación configura una infracción grave cuya sanción es de multa de hasta 10.000 UTM y, en caso, de que el incumplimiento sea deliberado, se puede configurar una infracción gravísima con una multa de hasta 20.000 UTM.

▪ IMPACTOS OPERACIONALES DE LA NOTIFICACIÓN DE BRECHAS

✓ ***Plan de respuesta a incidentes.*** Se deben implementar o actualizar los procedimientos y planes de respuesta a incidentes de seguridad, coordinando a priori las etapas de comunicación interna y externa, los equipos involucrados y sus responsabilidades. Esto permitirá minimizar el impacto de una brecha, y facilitará el cumplimiento de las obligaciones de notificación.

✓ ***Documentación.*** La Nueva Ley requiere registrar las comunicaciones, describir la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

6. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO Y EVALUACIONES DE IMPACTO DE PRIVACIDAD

6.1. PRIVACIDAD POR DISEÑO Y POR DEFECTO. La Nueva Ley consagra un deber general de **protección desde el diseño y por defecto**, instaurando una norma que exigirá a los

responsables la adopción de una perspectiva transversal, proactiva y preventiva en materia de protección de datos personales (Art. 14 quáter).

▪ IMPACTOS OPERACIONALES DE LA PRIVACIDAD POR DISEÑO

✓ ***Adopción de medidas técnicas y organizativas desde el diseño de todas las iniciativas que involucren tratamiento de datos.*** La privacidad se transforma en un factor determinante en de cualquier modelo de negocios. Los responsables quedan obligados a **adoptar medidas específicas** que resguarden transversal y proactivamente la privacidad de los titulares, durante todas las etapas que involucre la actividad, negocio o proyecto correspondiente. Para determinar LAS medidas se atenderá a: (i) estado de la técnica; (ii) costos de implementación; (iii) naturaleza, ámbito, contexto y fines del tratamiento de datos; y (iv) riesgos asociados.

✓ ***Elaboración de una Política de Privacidad desde el Diseño y por Defecto***, que permita trazar internamente las directrices que definirán el actuar de la empresa en materia de privacidad, abarcando el antes, durante y después de cualquier actividad, negocio o proyecto que involucre tratamiento de datos personales. Esta política establece directrices de actuación, identifica fases de control, establece niveles de actuación según la criticidad de los riesgos, define la aplicación de evaluaciones de impacto de privacidad, y fijar criterios para implementar medidas de mitigación, entre otras materias.

6.2. EVALUACIONES DE IMPACTO DE PRIVACIDAD ("PIA"). La Nueva Ley exige que, cuando una actividad de tratamiento de datos **por su naturaleza, alcance, contexto, tecnología utilizada o fines, involucre un alto riesgo para los derechos de los titulares**, se realice en forma previa una **evaluación de impacto en protección de datos personales** (Art. 15 ter).

La Agencia publicará una lista orientativa de los tipos de tratamiento que requerirán PIA. **La infracción a esta obligación es altísima** pues es sancionada como infracción gravísima, con una **multa asociada de hasta UTM 20.000**.

▪ IMPACTOS OPERACIONALES DE LA OBLIGACIÓN DE EFECTUAR EVALUACIONES DE IMPACTO DE PRIVACIDAD

✓ ***Deberán crearse los procesos que permitan elaborar un PIA***, cumplidos que sean ciertos criterio de alto riesgo que se deberán establecer en la Política de Privacidad desde el Diseño y por Defecto.

La Nueva Ley establece que estas evaluaciones deberán realizarse, entre otras, en los siguientes casos:

i. En proyecto de evaluaciones sistemáticas de aspectos personales de los titulares basados en tratamientos automatizados, como la elaboración de perfiles.
ii. En los escenarios de tratamiento masivo de datos o a gran escala.
iii. Iniciativas que involucren el monitoreo o supervisión de los titulares en zonas de acceso público.

7. CESIÓN Y COMUNICACIÓN DE DATOS PERSONALES

CESIÓN O TRANSFERENCIA DE DATOS PERSONALES (DE RESPONSABLE A RESPONSABLE)

Para transferir o ceder datos personales, el responsable debe contar con el **consentimiento** del titular, o estar frente a una cesión necesaria para el cumplimiento de un contrato o para la satisfacción de un interés legítimo del cedente o del cesionario (Art. 15).

La cesión debe constar en un acuerdo escrito (*Data Transfer Agreement*) en el que se individualice a las partes, los datos que son objeto de la cesión, las finalidades del tratamiento y las demás estipulaciones que acuerden el cedente y el cesionario.

COMUNICACIÓN DE DATOS PERSONALES (DE RESPONSABLE A ENCARGADO)

El lícito tratar datos personales a través de un tercero encargado o mandatario, usualmente, prestadores de servicios del responsable. Este deberá ceñirse a las instrucciones del responsable y al objeto del encargo que se regule entre ambos. Si el mandatario actúa en contravención de lo instruido por el responsable, se considerará como responsable directo para todos los efectos legales (Art. 15 bis).

Para la comunicación responsable y encargado o mandatario, estos **deberán celebrar un acuerdo de procesamiento de datos** (*Data Processing Agreement*) en el que al menos consignen: el objeto del encargo, su duración, la finalidad del tratamiento, el tipo de datos personales tratados, las categorías de titulares, y los derechos y obligaciones de las partes.

El encargado **no podrá delegar su mandato a terceros** (sub-encargados) salvo que cuente con una autorización específica y por escrito del responsable.

▪ IMPACTOS OPERACIONALES DE LA CESIÓN Y COMUNICACIÓN

✓ ***Identificación de las operaciones de cesión y comunicación de datos.*** Deberán identificarse todas las operaciones en que el responsable transfiere y comunica datos y

clasificarlas debidamente, junto al contenido mínimo que deberá integrarse a los acuerdos de cesión y procesamiento.

✓ ***Gestión de proveedores.*** Las organizaciones deberán clasificar sus proveedores críticos y no críticos en relación con la intensidad y criticidad de su tratamiento de datos, e insertar en su relación las cláusulas, anexos o contratos independientes necesarios para regular el tratamiento de datos. Se deberán establecer las condiciones mínimas dictadas por el responsable, que deberá cumplir el encargado, particularmente las restricciones de uso de los datos, las medidas de seguridad, y las obligaciones de eliminación de los datos una vez termine la relación contractual que motiva el encargo.

8. TRANSFERENCIA INTERNACIONAL DE DATOS

La Nueva Ley regula por primera vez la transferencia internacional de datos personales, estableciendo un listado cerrado de hipótesis en que se permite y otorgando a la Agencia amplias facultades para fiscalizar las operaciones, formular recomendaciones, adoptar medidas conservativas y en casos calificados, suspender temporalmente el envío de los datos.

Las operaciones de transferencia internacional de datos solo estan autorizadas en los escenarios de:

i. Cuando la transferencia se realiza a un **país que proporcione niveles adecuados de protección**. La Agencia determinará cuales son esos países, en una "decisión de adecuación" (Art. 27 (a) y 28).

ii. Quede amparada por **cláusulas contractuales** o **normas corporativas vinculantes,** y se establezcan **garantías adecuadas** -i.e., que contengan similares o mayores principios, derechos y garantías a aquellas que ofrece la Nueva Ley, y en particular, que otorguen derechos exigibles y acciones legales efectivas a los titulares de los datos (Art. 27 (a) y 28).

iii. Quede amparada un **modelo de cumplimiento o mecanismo de certificación** con garantías adecuadas adoptados entre el responsable y el tercero receptor de datos.

iv. En ausencia de estos elementos, se podrán realizar transferencias específicas y no habituales sólo cuando (entre otras):

- Exista **consentimiento expreso** para una transferencia internacional específica y determinada.
- Se refiera a **transferencias bancarias**, financieras o bursátiles específicas.
- Haya autorización expresa de la ley y para una finalidad determinada.

- Sea necesaria para la **celebración o ejecución de un contrato**.

v. Cuando no se verifique ninguna de las hipótesis señaladas, previa resolución fundada de la Agencia, y sólo para un caso particular, cuando transmisor y receptor otorguen garantías adecuadas de protección.

▪ IMPACTOS OPERACIONALES DE ESTAS NUEVAS REGLAS SOBE TRANSFERENCIA INTERNACIONAL DE DATOS

✓ ***Identificación de las transferencias internacionales,*** lo que debería luego permitir "alojar" cada grupo de transferencia en la causal o justificación que corresponda, dependiendo el país donde se dirigen los datos y sus circunstancias.

✓ ***La prueba es del responsable.*** Aun cuando existan variadas hipótesis para realizar la transferencia internacional de datos, el responsable de datos siempre tendrá la carga de probar ante la agencia que esta ha sido practicada de conformidad con la ley.

✓ ***Medidas de seguridad.*** El responsable deberá adoptar medidas y mecanismos de seguridad adecuados.

✓ ***Normas corporativas vinculantes.*** Para el caso de sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador y siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales, las transferencias podrán quedar amparadas en normas corporativas vinculantes previamente aprobadas por la Agencia.

9. LOS MODELOS DE PREVENCIÓN DE INFRACCIONES

La Nueva Ley establece **la posibilidad, más no la obligación** de adoptar modelos de prevención de infracciones consistentes en un **programa de cumplimiento que puede ser certificados por la Agencia** en cuanto estos reúnan los requisitos establecidos en la ley.

La adopción de un programa de cumplimiento exige el cumplimiento de elementos mínimos, entre ellos: la designación de un delegado de protección de datos personales (también conocido como "**DPO**"); la identificación del tipo de información que se trata, su ámbito territorial, categoría, clase o tipos de bases de datos administradas y caracterización de los titulares; el establecimiento de protocolos, reglas y procedimientos específicos que permitan el cumplimiento de la Nueva Ley; establecimiento de una organización interna que contemple sanciones y procedimientos de denuncia o castigo de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.

En este contenido mínimo **destaca la figura del delegado, como un punto de contacto con la Agencia**, quien deberá ser designado por la máxima autoridad directiva o administrativa y contar con autonomía para efectos de asesorar al responsable de datos, a los encargados y a los dependientes del responsable sobre las disposiciones de protección de datos; promover y participar en la política adoptada por el responsable de datos para garantizar una correcta y efectiva protección de datos; asistir en la identificación de riesgos; preocuparse de la formación permanente de las personas que participen en actividades de tratamiento al interior de la entidad que se trate, entre otras.

- **¿QUÉ BENEFICIOS REPORTA SU ADOPCIÓN PARA LAS EMPRESAS?**

✓ ***Medio de acreditación del cumplimiento.*** La adopción de un modelo de prevención de infracciones es un **modo útil para establecer y demostrar el cumplimiento con los estándares legales**, pues implica que el responsable ha identificados los riesgos que su actividad genera, ha evaluado su origen, su habitualidad, su naturaleza y las situaciones que los incrementan para luego determinar la manera de prevenir la comisión de infracciones o situaciones que pongan en riesgo los derechos de los titulares.

✓ ***Atenuante de responsabilidad.*** La adhesión de un modelo de prevención certificado ante la Agencia constituye una **circunstancia atenuante de la responsabilidad**.

10. DATOS SENSIBLES Y CATEGORÍAS ESPECIALES DE DATOS

- **DATOS SENSIBLES: REGLA GENERAL**

Se establece en la Nueva Ley un **catálogo cerrado de datos sensibles**, entendiendo estos como *aquellos relativos a las características físicas o morales de las personas o a circunstancias de su vida privada, que revelen su origen étnico o racial, su afiliación política, sindical o gremial, su situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, sus datos de salud, sus datos biométricos, y la información relativa a su vida y orientación sexual, a la identidad de género.*

Por regla general su tratamiento **sólo puede realizarse con consentimiento del titular, salvo escenarios particulares** según sean los tipos de datos tratados como parte de su negocio habitual (Art. 16). Cuando se traten datos sensibles sin consentimiento, se requerirá siempre una Evaluación de Impacto de Privacidad.

- **DATOS DE SALUD Y RELATIVOS AL PERFIL BIOLÓGICO HUMANO**

Por regla general sólo pueden tratarse para los fines previstos por leyes especiales en materia sanitaria y con el consentimiento expreso del titular, sin perjuicio de que se establezcan escenarios donde no es necesario el consentimiento - p.ej., cuando resulte indispensable para salvaguardar la vida o integridad física o psíquica del titular (Art 16 bis).

Queda prohibido el tratamiento y cesión de este tipo de datos o sus muestras biológicas, cuando éstos han sido recolectados en un contexto laboral, educativo, deportivo, social, de seguros, de seguridad o identificación salvo texto expreso del legislador.

- **DATOS BIOMÉTRICOS**

Las condiciones de su tratamiento son similares a los datos personales relativos a la salud y al perfil biológico humano, pero atendidas sus características particulares, se impone una **obligación de informar al titular** ciertos elementos adicionales sobre el sistema biométrico utilizado, la finalidad específica de los datos recolectados, el período por el cual serán utilizados, entre otros aspectos.

- **DATOS DE MENORES**

Los datos personales relativos a niños, niñas y adolescentes, al ser una categoría especial, sólo podrán tratarse atendiendo a su interés superior y al respeto de su autonomía progresiva, lo que implica el establecimiento de una clara y amplia limitación a las finalidades por las cuales las empresas podrán realizar su tratamiento.

El consentimiento sólo será válido si es prestado por adolescentes mayores de 14 años, salvo que se trate de datos sensibles – en cuyo caso la edad de consentimiento se eleva a 16. Los menores de 14 años solo pueden actuar representados en el otorgamiento del consentimiento.

La Nueva Ley introduce un criterio objetivo (i.e. la edad) pero no lo erige como una presunción de derecho de la validez del consentimiento, por lo que podría probarse que un tratamiento determinado carece de base de licitud en cuanto este no respete los principios del interés superior del niño y autonomía progresiva. **Al recabarse el consentimiento deberá tenerse en cuenta su edad y el grado de desarrollo psicológico**, lo que se traduce (siguiendo al art. 33 de la Ley N°21.430) en que el documento donde se solicite el consentimiento habrá de presentarse en un **lenguaje fácilmente comprensible**.

11. LA NUEVA AUTORIDAD DE PROTECCIÓN DE DATOS

Se crea la **Agencia de Protección de Datos Personales** para velar por la efectiva protección de los derechos que garantizan la vida privada y los datos personales junto con la fiscalización del cumplimiento de la ley.

La Agencia tendrá entre sus potestades el dictar instrucciones y normas generales obligatorias para regular las operaciones de tratamiento de datos personales; aplicar e interpretar administrativamente las disposiciones legales y reglamentarias, así como también las normas e instrucciones generales que dicte; fiscalizar el cumplimiento de la Nueva Ley; determinar infracciones e incumplimientos en que incurran los responsables; y desarrollar programas para difundir, promover e informar a la ciudadanía en relación con el respeto por la protección de datos entre otras funciones.

✓ ***¿Cómo impacta la creación de la Agencia?*** Las empresas deberán adaptarse a una nueva realidad que exige el relacionamiento con la autoridad, lo que bajo el mandato de la LPD era prácticamente inexistente o bien de carácter disperso y específico. También, la creación de la Agencia se relaciona la creación de un sistema de procedimientos administrativos y judiciales inéditos en Chile.

12. NUEVO RÉGIMEN DE RESPONSABILIDAD, INFRACCIONES Y SANCIONES

La Nueva Ley establece un nuevo y riguroso régimen de responsabilidades, infracciones y sanciones, que contará con mecanismos de supervisión, fiscalización y ejecución efectiva.

Se exige a los responsables de datos **adoptar una actitud y responsabilidad proactiva** para garantizar que los tratamientos de datos ocurran en condiciones que prevengan o mitiguen potenciales daños.

Si bien se establece un catálogo de infracciones que permiten orientar el accionar de los obligados, los contornos de éste serán delimitados por la propia Agencia mediante la dictación de normativa reglamentaria y de su actividad interpretativa, cuestión que exigirá una constante revisión de los criterios que se adopten.

▪ NUEVA TARIFICACIÓN DE LAS INFRACCIONES

La Nueva Ley define tres niveles de infracciones, en función de su gravedad.

i. **LAS INFRACCIONES LEVES** incluyen, entre otras
   - incumplimientos al deber de información y transparencia;

- la falta de canales de comunicación y para el ejercicio de derechos;
- respuestas tardías o incompletas a solicitudes de titulares;
- incumplimiento de instrucciones generales de la Agencia.

➢ Sanción a las infracciones leves: **Multa de hasta 5.000 UTM** (app USD $363.000) o amonestación escrita

ii. **LAS INFRACCIONES GRAVES** incluyen, entre otras
- el tratamiento de datos sin fundamento legal, o con finalidades diversas a las informadas;
- la comunicación o transferencia de datos para fines no autorizados;
- obstaculizar el ejercicio de los derechos ARCO;
- tratar datos de menores con infracción a la ley;
- infringir las obligaciones de seguridad de la ley en el tratamiento de los datos;
- omitir las notificaciones de brechas de medidas de seguridad;
- realizar operaciones de transferencia internacional de datos en incumplimiento de la ley

➢ Sanción a las infracciones graves: **Multa de hasta 10.000 UTM** (app USD $726.000).

iii. **LAS INFRACCIONES GRAVÍSIMAS** incluyen, entre otras
- el tratamiento de datos personales en forma fraudulenta;
- tratamiento a sabiendas de datos personales sensibles o de menores en contravención a la ley;
- la omisión deliberada de la comunicación de las brechas de seguridad;
- incumplir la obligación de efectuar una evaluación de impacto de privacidad;
- realizar, a sabiendas, transferencia internacional de datos en contravención a la ley;

➢ Sanción a las infracciones gravísimas: **Multas de hasta 20.000 UTM** (app USD $1.450.000).

- **AUMENTO DE MULTAS POR REINCIDENCIA Y SUSPENSIÓN DE LAS OPERACIONES**

REGLA GENERAL DE LA REINCIDENCIA. En caso de reincidencia (dos o más sanciones en 30 meses), la Agencia podrá **multiplicar hasta por tres la multa**.

REINCIDENCIA POR INFRACCIONES GRAVÍSIMAS. Si se imponen multas por infracciones gravísimas reiteradas, la Agencia podrá **disponer la suspensión parcial o total de las operaciones y actividades de tratamiento de datos del responsable infractor hasta por 30 días**, salvo que se afecten los derechos de los titulares.

REINCIDENCIA DE GRANDES EMPRESAS. La reincidencia en infracciones graves de las **grandes empresas** podrá sancionarse con una multa de hasta el 2% de los ingresos anuales por ventas y servicios. La multa por **reincidencia en infracciones gravísimas de las grandes empresas podrá llegar a un 4% de los ingresos anuales por ventas y servicios**.

Durante los primeros 12 meses de vigencia de la Nueva Ley, la Agencia podrá aplicar como sanción una amonestación por escrito a las PYME, con el objeto de permitir un cambio cultural gradual.

- **RECARGO A LAS MULTAS EN UN 50% POR NO SUBSANAR LAS INFRACCIONES**

Al imponer una sanción, la Agencia indicará las medidas para subsanar las causales que la motivaron, las que deberán ser adoptadas en un plazo no mayor a 60 días. En caso de incumplir dicha obligación, la multa podrá ser recargada en un 50%.

- **CIRCUNSTANCIAS ATENUANTES Y AGRAVANTES Y PARÁMETROS PARA LA DETERMINACIÓN DEL MONTO DE LAS MULTAS**

Para la determinación de las multas o sanciones, la Nueva Ley contempla un listado de circunstancias atenuantes (p.ej., la colaboración o la autodenuncia) y agravantes (p.ej., la reincidencia o el carácter continuado de la infracción).

Asimismo, la Nueva Ley establece los criterios que la Agencia deberá aplicar para la determinación del monto de las multas, que incluyen la gravedad de la conducta; la falta de diligencia; el perjuicio provocado, el número de titulares afectados; las circunstancias atenuantes y agravantes que concurran, entre otros.

******