

Actualidad Legal

Protección de Datos Personales: Lo que todo empleador necesita saber

Abril, 2026

Las modificaciones introducidas por la nueva Ley N°21.719 a la Ley N°19.628 sobre Protección de la Vida Privada (la “Ley”), que entran en vigencia el 1 de diciembre del presente año, tendrán un impacto relevante para el empleador en materia de recursos humanos. Las entidades empleadoras deberán adecuar sus prácticas y propender a un cambio relevante en la forma en que se gestionan los datos personales de candidatos, trabajadores y extrabajadores.

Es importante tener presente que muchas de las obligaciones que establece esta reforma no son completamente nuevas, dado que la ley vigente ya consagra principios básicos de protección de datos y derechos de los titulares. Sin embargo, la diferencia fundamental radica en que, hasta ahora, no existía una autoridad especializada encargada de fiscalizar su cumplimiento. Las modificaciones introducidas en la Ley crean la Agencia de Protección de Datos Personales (la “Agencia”), un organismo autónomo con amplias facultades para fiscalizar, instruir procedimientos sancionatorios, ya sea de oficio o a petición de parte, y aplicar sanciones significativamente más severas que las contempladas en la normativa actual. En la práctica, esto significa que los empleadores que ya trataban datos personales sin ajustarse plenamente a la ley vigente ahora enfrentarán un riesgo real de fiscalización y sanción.

1. El empleador como responsable de datos

Toda entidad empleadora tiene la calidad de responsable de datos, lo que significa que es ella quien define los fines y los medios con los que se tratan los datos personales de las personas vinculadas a su organización. En virtud de esta condición, el empleador asume responsabilidad directa sobre el tratamiento de los datos personales de sus trabajadores durante todo el ciclo de la relación laboral, desde el proceso de selección hasta su término. Esta responsabilidad se extiende también a los datos de aquellos candidatos que participen en un proceso de selección y no resulten elegidos para el cargo. Como consecuencia de lo anterior, el empleador debe dar cumplimiento a todos los principios, obligaciones y derechos establecidos por la Ley en materia de protección de datos personales.

2. ¿Qué se entiende por dato personal y dato sensible?

- Un dato personal es cualquier información que permita identificar, directa o indirectamente, a una persona. Por ejemplo, su nombre, el número de cédula de identidad, datos de contacto, datos asociados a su identidad física, entre otros.
- Los datos sensibles son datos personales que incluyen información sobre origen étnico o racial, afiliación sindical o gremial, estado de salud, datos biométricos, orientación sexual e identidad de género, entre otros. El tratamiento de estos datos es similar al de los datos personales en general, pero goza de algunas particularidades que hacen de su protección mayor.

3. Principios que rigen el tratamiento de datos personales y debe conocer el empleador

El tratamiento de datos se rige por principios que aplican a todas las operaciones de recursos humanos, siendo los más relevantes para estos efectos:

- a) Licitud y lealtad:** Solo se pueden tratar datos de forma lícita y leal, y el empleador debe poder acreditarlo. Lo anterior implica tratar los datos cuando se está amparado por una base de licitud establecida por la Ley.
- b) Finalidad:** Los datos deben recolectarse con fines específicos, explícitos y lícitos, y no pueden usarse para propósitos distintos.
- c) Proporcionalidad:** Solo deben tratarse los datos estrictamente necesarios, y conservarse únicamente por el tiempo requerido.
- d) Seguridad y confidencialidad:** Se deben implementar medidas técnicas y organizativas adecuadas, y quienes accedan a los datos deben guardar reserva, incluso tras el término de la relación laboral.
- e) Transparencia:** Los titulares deben tener acceso permanente a información clara sobre cómo se tratan sus datos.

4. Bases de licitud: ¿cuándo pueden tratarse los datos personales?

La Ley establece que el consentimiento del titular es la regla general para tratar los datos personales. Sin embargo, también reconoce otras bases de licitud que permiten el tratamiento sin consentimiento, por lo que, en la práctica, lo recomendable es utilizar el consentimiento cuando ninguna de las otras bases de licitud sea aplicable. Algunas de estas bases de licitud operan para todo tipo de datos personales y otras, sólo para datos que no tengan el carácter de sensibles.

Las más relevantes para el empleador son:

- Ejecución o cumplimiento de una obligación legal, o si la ley establece el tratamiento.
- Ejecución de un contrato entre titular y responsable, o medidas precontractuales adoptadas a solicitud del titular (por ejemplo, la ejecución del contrato de trabajo y los procesos de selección).
- Satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades del titular (por ejemplo, el interés legítimo del empleador de poner cámaras de vigilancia en las oficinas, en casos en que la naturaleza de los servicios prestados lo haga necesario y no afecte los derechos y libertades del trabajador).
- Ejercicio de derechos y cumplimiento de obligaciones en el ámbito laboral o de seguridad social, cuando se realice en el marco de la ley.

5. Derechos de los trabajadores sobre sus datos

Los trabajadores, como titulares de datos, cuentan con derechos de carácter irrenunciable que el empleador debe facilitar a través de mecanismos sencillos y, por regla general, gratuitos:

- **Acceso:** Saber si sus datos están siendo tratados y obtener copia de ellos.
- **Rectificación:** Corregir datos inexactos o incompletos.
- **Supresión:** Solicitar la eliminación de datos cuando ya no sean necesarios o se hayan tratado ilícitamente.
- **Oposición:** Oponerse a determinadas actividades de tratamiento.
- **Portabilidad:** Recibir sus datos personales en formato electrónico estructurado y solicitar su transferencia a otro responsable.
- **Bloqueo:** Suspender el tratamiento mientras se resuelve una solicitud de rectificación, supresión u oposición.

La falta de respuesta, una respuesta fuera de plazo o una respuesta inadecuada ante el ejercicio de estos derechos expone a la entidad empleadora a reclamaciones ante la Agencia, que podrían derivar en sanciones.

6. Aspectos relevantes a tener en cuenta

- a) Transparencia:** La empresa debe publicar y mantener permanentemente disponible su política de tratamiento de datos, cumpliendo con las menciones requeridas por la Ley.
- b) Seguridad:** Los empleadores deben implementar medidas técnicas y organizativas adecuadas para resguardar la confidencialidad, integridad, disponibilidad y resiliencia de sus sistemas de información. Dichas medidas pueden incluir, entre otras, la seudonimización y el cifrado de los datos personales. En caso de una vulneración de seguridad que afecte datos de los trabajadores, el empleador está obligado a reportar el incidente ante la Agencia. Asimismo, cuando la vulneración involucre datos sensibles u otras circunstancias establecidas por la ley, el empleador deberá también notificar directamente a los trabajadores afectados.
- c) Protección desde el diseño y por defecto:** Desde la planificación de cualquier proceso que involucre datos personales, se deben adoptar medidas para que solo se traten los datos estrictamente necesarios. Esto aplica, por ejemplo, al diseñar formularios de postulación, encuestas internas o sistemas de evaluación.
- d) Evaluación de impacto:** Cuando el tratamiento pueda generar un alto riesgo para los derechos de los trabajadores, se debe realizar una evaluación de impacto previa. Esto es obligatorio en casos de elaboración de perfiles con efectos jurídicos significativos, tratamiento masivo de datos, monitoreo sistemático de zonas de acceso público o tratamiento de datos sensibles, cuando se ha hecho por una base de licitud distinta del consentimiento.

e) Procesos de selección: Las obligaciones de protección de datos aplican también respecto de los candidatos. Una vez finalizado el proceso, los datos deben eliminarse cuando ya no sean necesarios para la finalidad que justificó su recolección. Para almacenar la información recopilada durante el proceso de selección y considerar al candidato en un proceso futuro, será necesario obtener su consentimiento.

f) Afiliación sindical: La Ley clasifica la afiliación sindical como dato sensible, lo que exige que los empleadores deben poner especial énfasis en las medidas de protección al gestionar esta información y que a su tratamiento sólo le son aplicables las bases de licitud para datos sensibles.

g) Datos biométricos y de geolocalización: La Ley establece regulación específica para ambas categorías. Las entidades empleadoras que utilicen sistemas biométricos de control de asistencia o que monitoreen la ubicación de sus trabajadores deberán aplicar medidas de seguridad más estrictas en virtud de la naturaleza de los datos.

h) Datos de extrabajadores: La gestión de datos personales no termina con la relación laboral. La Ley exige que los datos se conserven solo por el tiempo necesario para cumplir los fines del tratamiento, luego de lo cual deben ser suprimidos o anonimizados. Esto obliga a los empleadores a definir políticas claras de retención y eliminación de datos de extrabajadores, considerando los plazos legales de conservación que imponen otras normativas (por ejemplo, obligaciones tributarias, previsionales o laborales). Además, regulaciones específicas como la normativa sobre sistemas de registro electrónico de asistencia establecen plazos determinados para que el empleador elimine los datos una vez que ya no son necesarios. Para el empleador, es recomendable mapear los datos que se conservan tras el término de la relación laboral, identificar las bases legales que justifican su retención y establecer un calendario de eliminación periódica.

i) Externalización de servicios y datos de trabajadores: La Ley distingue dos figuras clave cuando los datos de trabajadores son tratados por terceros:

- Mandato: Ocurre cuando el empleador encomienda a un tercero, por ejemplo, un proveedor de payroll, un software de gestión de personas o un servicio de exámenes preocupacionales, que trate datos en su nombre y bajo sus instrucciones. El tercero no adquiere la calidad de responsable, porque actúa como mandatario o encargado del empleador, debiendo usar los datos exclusivamente para los fines del encargo.
- Cesión: Implica transferir datos personales a otro responsable, quien los tratará para sus propios fines. En este caso, el cesionario adquiere la calidad de responsable de datos para todos los efectos legales. La cesión requiere consentimiento del titular, salvo excepciones legales, y debe constar por escrito. En el ámbito de recursos humanos, esta figura puede presentarse, por ejemplo, cuando se comparten datos de trabajadores con una empresa relacionada que los utilizará para sus propios fines de gestión, o bien, en el ámbito de la subcontratación laboral, cuando la empresa principal solicita datos en ejercicio del derecho de información.

j) Transferencias internacionales: Si la empresa transfiere datos de trabajadores a una matriz o filiales en el extranjero, deberá ampararse en la regulación que permite dicha transferencia al extranjero. Así, se deberá verificar que el país receptor cuente con niveles adecuados de protección o que existan garantías apropiadas (cláusulas contractuales, normas corporativas vinculantes o certificaciones), entre otras. Las empresas de un mismo grupo pueden ampararse en normas corporativas vinculantes aprobadas por la Agencia.

7. Modelo de prevención de infracciones: una oportunidad

La Ley permite adoptar voluntariamente un modelo de prevención de infracciones, cuya regulación debe incorporarse en los contratos de trabajo, contratos de prestación de servicios y/o en el Reglamento Interno de Orden, Higiene y Seguridad. Contar con un modelo certificado por la Agencia genera un efecto reputacional positivo, al quedar inscrito en el Registro Nacional de Sanciones y Cumplimiento, y constituye una circunstancia atenuante al momento de determinarse sanciones. El programa de cumplimiento debe contener, entre otras cosas, la designación de un delegado de protección de datos personales, identificación de los tipos de datos tratados y las actividades de riesgo, establecimiento de protocolos específicos para prevenir infracciones, implementación de mecanismos de reporte interno y ante la Agencia en caso de vulneraciones de seguridad y sanciones administrativas internas y procedimientos de denuncia para quienes incumplan el sistema.

8. Sanciones

La Ley establece un régimen sancionatorio en tres niveles:

Nivel de infracción	Sanción	Ejemplos
Leve	Amonestación escrita o multa de hasta 5.000 UTM (aprox. USD 382.000)	Políticas de privacidad incompletas; falta de respuesta oportuna a solicitudes de datos de trabajadores.
Grave	Hasta 10.000 UTM (aprox. USD 764.000)	Tratamiento sin base de licitud o consentimiento; transferencia no autorizada de datos; medidas de seguridad inadecuadas.
Gravísima	Hasta 20.000 UTM (aprox. USD 1.528.000)	Tratamiento fraudulento; vulneración deliberada de la confidencialidad de datos sensibles; tratamiento a sabiendas y en contravención a ley de datos de menores.

En caso de reincidencia, la Agencia puede aplicar hasta tres veces el monto de la multa. Para empresas que no califiquen como de menor tamaño, la reincidencia en infracciones graves o gravísimas puede alcanzar multas de hasta el 2% o 4% de los ingresos anuales, respectivamente. Adicionalmente, ante infracciones gravísimas reiteradas dentro de 24 meses, la Agencia puede ordenar la suspensión de operaciones de tratamiento de datos por hasta 30 días, renovable indefinidamente. La Ley también contempla responsabilidad civil por daños patrimoniales y extrapatrimoniales.



www.bye.cl