

GUÍA

Guía sobre la Ley de Protección de Datos y Buenas Prácticas



Contexto

El 1 de diciembre de 2026 entra en plena vigencia la Ley 21.719 que modifica la ley 19.628, la cual pasará a llamarse “Sobre Protección de Los Datos Personales”. Como plataforma que administra datos de tu empresa, en Buk queremos ayudarte a prepararte para cumplir con la normativa. Esta guía resume, en lenguaje simple, qué cambia y qué buenas prácticas puedes empezar a aplicar hoy en el uso diario de la plataforma.

1 ¿Por qué te afecta esto?

Todas las empresas tratan datos personales, ya sean de clientes, colaboradores, postulantes o proveedores. La nueva ley exige saber exactamente dónde están estos datos, cómo se están tratando, cómo protegerlos y cómo ejecutar los derechos de los titulares en caso de que lo soliciten y eleva de forma importante las exigencias sobre cómo se recolectan, almacenan, usan y eliminan esos datos, y crea una Agencia con poder real de fiscalización y sanción.

Las empresas no deben solo cumplir con esta nueva ley, sino también demostrar que cumplen, por lo que exige también una evaluación de riesgos activa y evidencia.

2 ¿Cómo facilita Buk este proceso?

Si tu empresa usa Buk, guardas datos críticos como remuneraciones, contratos, licencias y evaluaciones. Tener tus datos de RRHH centralizados en Buk es tu principal ventaja para gestionar este cumplimiento de forma eficiente y segura.

3 ¿Cuál es mi rol y el de Buk?

Tu empresa, como Responsable de los datos personales que gestiona, es quien escoge cómo y con qué fin va a tratar los datos que maneja, en ese sentido escogieron Buk para ejecutar los pagos de nómina, los procesos de selección, las capacitaciones o tu gestión de finanzas, lo que nos convierte en el Encargado de tratar los datos personales necesarios para este proceso.

Son los Responsables quienes deben cumplir los requisitos legales y ejecutar los derechos de los titulares, en ese sentido debes registrar dónde están los datos personales y para qué los usas, darle una base de licitud (justificar por qué tienes ese dato) y evaluar los riesgos de su uso.



Esta guía no reemplaza la asesoría de tu equipo legal en la implementación de los requerimientos de la ley.

Los principios que rigen el tratamiento de datos

La Ley 21.719 fija principios que deben guiar cualquier tratamiento de datos personales, sin importar el tamaño de la empresa. Son la base sobre la que se construyen todas las obligaciones, referidas a los derechos de los titulares, que revisaremos más adelante en esta guía.

Licitud y lealtad

Los datos sólo pueden tratarse con una base legal habilitante (consentimiento, contrato, obligación legal, entre otras) y de forma transparente con el titular, nunca de forma engañosa.

Finalidad

Los datos deben recolectarse para fines específicos y explícitos, y no pueden usarse después para un propósito distinto sin informar. Por ejemplo, datos recolectados para liquidar sueldos no deberían reutilizarse sin más para fines de marketing interno.

Proporcionalidad

Solo se debe recolectar y tratar lo estrictamente necesario para la finalidad declarada. Pedir más datos "por si acaso" incumple este principio.

Calidad

Los datos deben ser exactos, completos y estar actualizados. Mantener información obsoleta o incorrecta también es un riesgo bajo la ley.

Responsabilidad (accountability)

La empresa debe poder demostrar que cumple, no solo declararlo. Esto implica documentar decisiones, mantener registros y tener evidencia disponible ante una eventual fiscalización.

Seguridad

Se deben implementar medidas técnicas y organizativas adecuadas al riesgo, como control de accesos, cifrado y protocolos ante incidentes.

Transparencia e información

Los titulares deben poder saber, de forma clara y accesible, qué datos se tratan, con qué fin y por cuánto tiempo.

Confidencialidad

Quienes acceden a los datos en el marco de su trabajo deben mantener reserva sobre ellos, incluso después de terminada la relación laboral.

Los derechos de los titulares sobre su información

La Ley 21.719 (artículo 4° y siguientes) reconoce seis derechos sobre los datos personales, conocidos como derechos ARCOP + bloqueo. Son personales, intransferibles e irrenunciables: no se pueden limitar ni renunciar por contrato, ni siquiera en el contrato de trabajo. Como empresa que usa Buk, debes estar en condiciones de recibir y responder estas solicitudes de parte de todos los titulares que están contenidos en la plataforma: colaboradores, postulantes e inclusive contactos comerciales de proveedores.

1

Acceso

Pedir confirmación de si tratas sus datos y, si es así, un detalle de ellos junto con información sobre su origen, la finalidad del tratamiento, a quién se han comunicado y por cuánto tiempo se conservarán.

Buk Tip: en Buk puedes revisar toda la información de tus titulares en tiempo real para responder a su solicitud.

2

Rectificación

Permite exigir la corrección de datos inexactos, incompletos o desactualizados (por ejemplo, un cambio de dirección o de estado civil no reflejado en el sistema). La ley obliga además a notificar la corrección a terceros a quienes esos datos se hayan comunicado previamente.

Buk Tip: en Buk, puedes actualizar la información del perfil de tus colaboradores de forma centralizada al interior de la plataforma. Revisa y documenta tus integraciones con terceros, propias o contratadas por Buk para poder notificar las rectificaciones.

3

Supresión (antes "cancelación")

Es el derecho a exigir la eliminación de los datos cuando ya no son necesarios para la finalidad que justificó su recolección, cuando se revoca el consentimiento, cuando fueron tratados de forma ilícita, o cuando han caducado. No procede, sin embargo, cuando existe una obligación legal de conservar la información —por ejemplo, los plazos de guarda de documentos laborales y previsionales.

Buk Tip: una vez eliminas un dato de la ficha del colaborador, o del postulante, esta se elimina de toda la plataforma, centralizando la gestión. Recuerda que puedes necesitar ejecutar eliminaciones también en tus integraciones.

4

Oposición

El titular puede oponerse a un tratamiento específico de sus datos, por ejemplo a que se use su información para fines distintos a los estrictamente laborales, o a decisiones basadas únicamente en tratamiento automatizado o perfilamiento que le generen efectos significativos.

Buk Tip: Buk te permite gestionar y restringir el acceso a módulos específicos, asegurando que los datos se traten sólo para fines específicos.

5

Portabilidad

Da derecho a recibir una copia de sus datos en un formato electrónico estructurado y de uso común, para que pueda ser utilizado por otro sistema, y a solicitar su transferencia directa a otro responsable, siempre que sea técnicamente factible; cuando el tratamiento es automatizado y se basa en su consentimiento.

Buk Tip: en Buk los colaboradores pueden descargar directamente sus liquidaciones de sueldos, certificados y contratos. Seguimos trabajando para tener más reportes exportables para usuarios y administradores!

6

Bloqueo

Permite suspender temporalmente el tratamiento de un dato mientras se resuelve una solicitud de rectificación, supresión u oposición.

Buk Tip: en Buk puedes ejecutar las rectificaciones y eliminaciones en tiempo real antes de que se cumplan los plazos de bloqueo. Te recomendamos mantener un registro de las bases de licitud bajo las que operas en Buk, para poder dar respuesta a las solicitudes recibidas. En general nuestros clientes trabajan bajo la licitud del contrato laboral, y la ejecución de tus obligaciones contractuales van por sobre el derecho de Bloqueo.

Plazos y forma en la práctica

- Plazo general de respuesta: 30 días corridos desde recibida la solicitud, prorrogables una sola vez por otros 30 días en casos justificados.
- Plazo para bloqueo temporal: 2 días hábiles.
- Las solicitudes se presentan por escrito (correo, formulario u otro medio equivalente) y la respuesta debe darse por el mismo medio, salvo que el titular pida otro.
- Rectificación, supresión y oposición son siempre gratuitas. El derecho a acceso debe serlo al menos una vez al trimestre.
- Si la empresa rechaza la solicitud o no responde a tiempo, el colaborador puede reclamar directamente ante la Agencia de Protección de Datos Personales.

Datos personales vs. datos sensibles: qué significa en Buk

No todos los datos que administras en Buk tienen el mismo nivel de exigencia. La Ley 21.719 distingue entre datos personales "comunes" y datos sensibles, estos últimos con protección reforzada porque su mal uso puede generar discriminación o un daño grave a la persona. Además, considera categorías específicas:

Categoría	Ejemplos en Buk	Nivel de exigencia
Datos personales comunes	Nombre, RUT, correo, teléfono, cargo, fecha de ingreso, remuneración	Consentimiento o base de licitud general (ej. contrato de trabajo)
Datos sensibles	Licencias médicas, afiliación sindical, huella dactilar y reconocimiento facial en control de asistencia, cargas familiares (menores)	Consentimiento explícito y medidas de seguridad reforzadas
Categorías especiales	Datos de niñas y niños y adolescentes, datos con fines históricos, estadísticos, científico y de investigación, datos de geolocalización y datos para obligaciones financieras, bancarias o comerciales	Depende de cada categoría

Buenas prácticas para el administrador de Buk en tu empresa: aplica para todos los módulos

1 Accesos y permisos

- Utiliza mecanismos robustos de autenticación, si no cuentas con SSO activa el MFA nativo de Buk y requisitos mínimos para el uso de contraseñas.
- Revisa periódicamente quién tiene acceso a qué módulos dentro de Buk (RRHH, jefaturas, finanzas) a través de las configuraciones de Perfiles y usuarios, asegurando que los datos sean accedidos solo por las personas realmente necesarias.
- Aplica el principio de "mínimo acceso necesario": no todos los perfiles necesitan ver toda la información.
- Da de baja los usuarios de personas que dejan de trabajar en tu empresa de forma oportuna.

2 Calidad y minimización de datos

- Revisa qué campos y formularios usas dentro de Buk y pregúntate si realmente necesitas cada dato solicitado.
- Mantén actualizada la información de tus colaboradores; datos desactualizados también son un riesgo.
- Evita duplicar información sensible en planillas externas cuando ya está disponible en la plataforma.

3 Transparencia con tus colaboradores

- Informa a tus colaboradores qué datos se recopilan a través de Buk y para qué se usan.
- Explica de forma simple cómo pueden ejercer sus derechos (acceso, rectificación, eliminación, oposición).
- Si realizas evaluaciones, encuestas o procesos de reclutamiento, incluye un aviso de privacidad breve.

4 Retención y eliminación de datos

- Define cuánto tiempo necesitas conservar cada tipo de dato (por ejemplo, información de ex colaboradores).
- Elimina o anonimiza datos que ya no tengan una finalidad vigente, en línea con tu política interna.
- Ten claridad sobre los plazos legales de conservación de documentos laborales antes de eliminar cualquier registro, y documenta la base de licitud si es que requieres almacenarlos por más tiempo del exigido.
- Antes de eliminar o anonimizar el dato de un ex-colaborador, asegúrate que no tenga un flujo de workflows o automatizaciones vigentes en la plataforma.

5 Frente a un posible incidente de seguridad

- Define internamente quién debe ser notificado de inmediato si sospechas de un acceso indebido a datos.
- Documenta el incidente: qué pasó, qué datos se vieron afectados y qué medidas se tomaron.
- Recuerda que, si el incidente involucra datos administrados en Buk, nuestro equipo de soporte está para ayudarte a coordinar la respuesta.

6 Contratos y proveedores

- Revisa que tu contrato de servicio con Buk (y con otros proveedores que traten datos de tus colaboradores) contemple cláusulas de protección de datos. Contamos con un Acuerdo de Tratamiento de Datos (DPA) que puedes firmar. Comunícate con tu Customer Happiness para más detalles.
- Si compartes datos con otros proveedores (por ejemplo, seguros complementarios), confirma que también cumplan con la normativa.

Control de asistencia con biometría: qué exige la ley

El Módulo de Control de Asistencia de Buk permite distintos métodos de marcaje, y algunos de ellos usan datos biométricos, como la huella dactilar o el reconocimiento facial. Estos datos son sensibles bajo la Ley 21.719 y, además, el uso de biometría para marcar asistencia está regulado directamente por la Resolución Exenta N° 38 de la Dirección del Trabajo (mayo de 2024), que regula los sistemas de registro y control de asistencia. Por lo tanto, ten en consideración lo siguiente:

1 Lo que la Resolución 38 exige a tu empresa

- Ofrecer siempre al menos dos alternativas de marcaje distintas, y al menos una de ellas debe ser no biométrica (tarjeta, PIN, aplicación móvil, código QR, entre otras).
- El colaborador tiene derecho a elegir la alternativa no biométrica, sin que esto le genere ninguna sanción ni consecuencia laboral.
- El sistema utilizado debe estar dentro de los autorizados por la Dirección del Trabajo, con registro de entradas, salidas y pausas en tiempo real, y trazabilidad completa ante cualquier modificación.

2 Lo que agrega la Ley 21.719

- La huella dactilar, el reconocimiento facial y cualquier patrón biométrico se consideran datos sensibles, por lo que requieren consentimiento explícito, libre e informado del colaborador para poder tratarse.
- Como la ley presume que el consentimiento no fue libremente otorgado cuando la recolección del dato no es estrictamente necesaria, tu empresa debe poder demostrar que el marcaje biométrico es opcional y no una condición para trabajar.
- El artículo 154 ter del Código del Trabajo obliga a mantener en reserva la información y los datos privados del trabajador a los que accedas con ocasión de la relación laboral, lo que incluye estos datos biométricos.

3 Qué te recomendamos configurar en Buk

- Activa siempre, junto al marcaje biométrico, un método alternativo no biométrico (como la App Colaborador) para quienes prefieran no entregar su huella o su rostro.
- Documenta el consentimiento, a través del contrato o un anexo, de cada colaborador que opte por el método biométrico, y deja registrado que se le ofreció la alternativa no biométrica.
- Si tienes equipos de marcaje propios, o integraciones con otros proveedores para recolectar el marcaje, asegúrate que estos también cumplan con los requisitos de seguridad que establece la ley.

Buk Tip: para el módulo de Control de Asistencia contamos con alternativas no biométricas para el marcaje. Considera, además, que los datos biométricos son cifrados tanto en tránsito como en reposo, y no son accesibles por administradores ni usuarios, sólo son utilizados de manera interna para validación, asegurando así los mínimos privilegios desde el diseño de la solución.

¿Y qué hace Buk por mí?

Como tu software de RRHH, en Buk actuamos como el Encargado del Tratamiento de tus datos. Nuestra prioridad es proveer una infraestructura robusta, certificada y segura, para que tú, como Responsable, puedas cumplir con la Ley 21.719 sin fricciones técnicas.

Entendemos que la seguridad es un proceso continuo, y por eso trabajamos bajo estos pilares:

- **Infraestructura de clase mundial:** todo el procesamiento ocurre en entornos altamente seguros, cifrados (AES-256 en tránsito y reposo) y respaldados por certificaciones internacionales como ISO 27001 y auditorías SOC 2 tipo 2.
- **Seguridad desde el diseño:** nuestra arquitectura permite la segregación de funciones y controles granulares de acceso, garantizando que los datos sean vistos únicamente por quienes deben hacerlo, siguiendo el principio de "menor privilegio".
- **Disponibilidad garantizada:** ejecutamos backups diarios y mantenemos planes de continuidad operativa y recuperación ante desastres (DRP/BCP), asegurando que tu información esté siempre disponible.
- **Transparencia total:** en nuestro Buk Trust Center (<https://trust.buk.cl>) tienes acceso directo a nuestra documentación de seguridad y políticas, lo cual facilita enormemente tus propias evaluaciones de riesgo y auditorías internas.

Checklist rápido para tu empresa:



- ☐ Tengo visibilidad de donde están los datos personales en mi empresa y he documentado la base de licitud de cada tratamiento de datos.
- ☐ He validado que los datos que solicito son los estrictamente necesarios
- ☐ Revisé que el control de acceso de la plataforma sea robusto.
- ☐ Revisé quién tiene acceso a cada módulo de Buk y ajusté permisos innecesarios.
- ☐ Actualicé o creé un aviso de privacidad para colaboradores y postulantes.
- ☐ Definí un procedimiento simple para responder solicitudes de acceso/rectificación/eliminación.
- ☐ Revisé los plazos de retención de datos de ex colaboradores, postulantes y otros titulares almacenados en la plataforma.
- ☐ Designé a alguien responsable de protección de datos dentro de mi empresa.
- ☐ Revisé las cláusulas de protección de datos y las medidas de seguridad en mis contratos con proveedores.
- ☐ Capacité a mi equipo de RRHH y a los cargos claves en estas buenas prácticas.
- ☐ Verifiqué que el marcaje biométrico tenga una alternativa no biométrica activa y disponible.
- ☐ Documenté el consentimiento de colaboradores que usan huella o reconocimiento facial.
- ☐ Cuento con un protocolo de actuación ante incidentes, teniendo claro a quienes acudir y a quién tengo que informar en caso de identificar una posible brecha de datos.