NUEVA REGULACIÓN PROTECCIÓN DE DATOS PERSONALES

De qué estamos hablando

Derecho a la protección de datos personales

Datos de identificación	•Nombre, apellidos, estado civil, firma autógrafa y electrónica, lugar y fecha de nacimiento, nacionalidad, fotografía, edad, entre otros.
Datos de contacto	•Cargo, domicilio de trabajo, correo electrónico y teléfono institucional, fecha de ingreso y salida del empleo, salario, entre otros.
Datos laborales	•Trayectoria académica, títulos, cédula profesional, certificados, reconocimientos, entre otros.
Datos sobre características físicas	•Color de piel, del iris o del cabello; señas particulares o cicatrices, estatura, peso, complexión, tipo de sangre, entre Otros.
Datos académicos	•Trayectoria académica, títulos, cédula profesional, certificados, reconocimientos, entre otros.
Datos patrimoniales	•Propiedades, bienes muebles e inmuebles, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, números de tarjeta de crédito, cedula de identidad, entre otros.
Datos biométricos	•Forma del iris, huella dactilar, forma de la palma de la mano, patrones de la voz u otras características únicas.

Acceder

Rectificar

Cancelar

Oponer

Lealtad, legalidad y transparencia

El tratamiento de datos personales debe ser lícito, leal, y efectuado de manera transparente.

Limitación de finalidad

Los datos personales deben ser tratados para fines específicos, explícitos y legítimos, que deben ser declarados al momento de su recogida, y su tratamiento posterior debe ser compatible con dicha finalidad.

Minimización

El tratamiento de datos personales debe ser adecuado, relevante y limitado a la necesidad o al propósito para el cual están siendo tratados.

Exactitud

El tratamiento de datos personales debe ser exacto y completo, y deben adoptarse medidas para asegurar que permanezcan actualizados.

Limitación de conservación

Los datos personales deben ser almacenados solamente por el período de tiempo necesario para los fines por los que los datos fueron tratados.

Integridad y confidencialidad

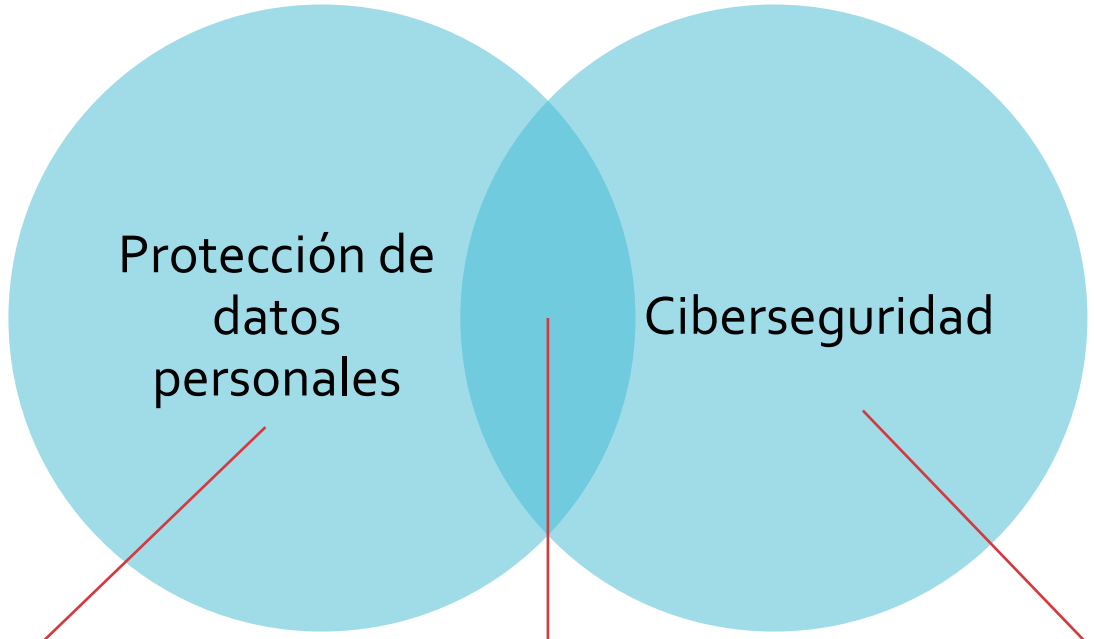
Deben adoptarse medidas apropiadas para garantizar la seguridad de los datos y sistemas de tratamiento de información, y para proteger los datos personales contra la pérdida, acceso no autorizado, destrucción, uso, modificación o difusión.

Responsabilidad

Quienes hagan tratamiento de datos personales deben rendir cuentas del cumplimiento con los principios antes señalados y de sus obligaciones, facilitando el ejercicio de derechos por parte de los titulares de datos personales y cumpliendo con los mismos.

Ojo:

No es ciberseguridad



Contratos, documentación y políticas de privacidad
Ejercicio de derechos
Habeas data
Responsabilidad administrativa y civil

Seguridad de activos de información (Incluyendo datos personales)

Seguridad de infraestructura
Protocolos de operación
Responsabilidad penal

Qué está pasando y lo que se viene en PDP

El GDPR y el Boletín 11144-07

Lo que está pasando: Europa impuso un estándar

- Cambio más sustantivo en 20 años
- Regulación estricta con alcance mucho mas allá de la UE
- Impacto global

Estándar muy elevado

1. **Privacidad por defecto**: empresas deben invertir arquitectura de decisiones para favorecer PDP. Ej: se prohíben casillas automarcadas de publicidad.
2. **Privacidad por diseño**: empresas tienen que diseñar procesos y proyectos en base a lógica garantista de PDP. Ej: los procesos deben revisar cuáles son los datos personales estrictamente necesarios para su operación.
3. **Evaluación de impacto**: es una exigencia previa al desarrollo de nuevos negocios que exige evaluar el tipo de datos y tratamientos necesarios y su cumplimiento con el RGPD, cuando existe un riesgo para las personas.
4. **Consentimiento**: empresas están obligadas a fijar los términos y condiciones de tratamiento de datos en términos claros y legibles. El consentimiento debe ser unívoco y distinto del asentimiento referido a otros bienes o servicios.
5. **Delegado de protección de datos personales**: empresas deben designar un responsable del cumplimiento del GDPR en la misma institución.
6. **Derecho de cancelación**: personas pueden exigir a los responsables del tratamiento de datos que eliminen toda su información personal que obren en dichas empresas.
7. **Multas**: empresas pueden ser multadas hasta con un 4% de su facturación anual mundial o 20 millones de euros por las infracciones más graves (depende de cuál es el monto más alto).

Efecto extraterritorial

- Art 3 GDPR: Aplicación extraterritorial GDPR
- Todas la empresas reaccionaron adecuando y exigiendo adecuación a sus proveedores
- Para las empresas chilenas, el RGPD puede ser aplicable:
  - De forma directa principalmente en dos casos:
    - 1. Cuando porque el responsable o el encargado del tratamiento tiene establecimiento en la UE (art. 3.1).
    - 2. Cuando ofrecen bienes y servicios a personas en la Unión (con o sin pago asociado) (art. 3.2.a.).
  - De forma indirecta: prestando bienes o servicios a cualquier jugador internacional, europeo o no.

Lo que se viene

Lo que se viene: Boletín 11144-07

- Salto cuántico: Ley se actualiza pasando de 1999 a la vanguardia en Latinoamérica
- Se sigue estándar GDPR
- Va a ser ley

Lo que se viene: Boletín 11144-07

- Las empresas tendrán que **demostrar** que tienen una **base de licitud** para tratar los datos personales que obran en su poder. Por ejemplo, deberán acreditar que tienen el consentimiento de sus clientes para tratar datos.
- Las empresas deberán **revisar el tipo de autorización para tratar datos personales** que han entregado a proveedores y empresas de suministro.
- Las empresas deberán invertir en **medidas de seguridad**, especialmente en materia informática, para resguardar los datos personales que tengan en su poder. Además, deberán **notificar las fallas de seguridad** que las afecten.
- Las empresas deberán **modificar sus procedimientos** para autorizar el acceso a datos personales sólo a aquellos trabajadores estrictamente necesarios para el proceso productivo.
- Las empresas deberán modificar sus formularios y sitios web para **comunicar los derechos de las personas y permitir el ejercicio de los mismos** ante éstas.
- Las empresas deberán **garantizar la portabilidad** de los datos personales de sus clientes.
- Las empresas deberán **implementar un modelo de prevención de infracciones** que será revisado por la autoridad de control.

Lo que se viene: estricto régimen de sanciones

- Hasta 5.000 UTM ($250 millones.)
- Suspensión de las operaciones y actividades de tratamiento de datos que realiza el responsable de datos, hasta por un término de 30 días