REUSCH

Plan estratégico de datos personales

Ley N.º 21.719 · del titular del dato a la autoridad

Cómo leer este mapa

1. **Titular:** entrega datos y ejerce derechos
2. **Responsable del dato (empresa):** decide y cumple
3. **Mandatario:** trata datos por encargo
4. **Receptor extranjero:** recibe datos
5. **Agencia:** fiscaliza y sanciona
6. **Tribunales:** reclamo judicial y acción civil

Círculos = orden de lectura

6 Tribunales
ART. 43

Corte de Apelaciones: reclamación judicial.

Multa a beneficio fiscal

5 Agencia (APDP)
ARTS. 30-32

Autoridad de control: fiscaliza y sanciona.

→ **Registro Nacional de Sanciones y Cumplimiento**
ART. 39
Registro de las sanciones.

Consecuencias
- Multa a beneficio fiscal
- Acción civil de responsabilidad
- Reclamación judicial ante la Corte de Apelaciones (art. 43)

Acción civil de responsabilidad

Reclamo ante la Agencia (arts. 11 y 41)

Fiscaliza y sanciona

1 Titular del dato
DATOS PERSONALES

Persona natural dueña del dato. Otorga consentimiento y ejerce derechos.

Datos personales

Otorga consentimiento y ejerce derechos

Derechos ARSOP
ARTS. 4-11

- **A** Acceso
- **R** Rectificación
- **S** Supresión
- **O** Oposición
- **P** Portabilidad

2 RESPONSABLE DEL DATO (EMPRESA)

Responsable de dato
ARTS. 14-15 TER

Decide fines y medios del tratamiento del dato personal.

Delegado (DPD)
ARTS. 49-50

Asesora y supervisa.

Principios del tratamiento
- Licitud y lealtad
- Finalidad
- Proporcionalidad
- Calidad
- Responsabilidad
- Seguridad
- Transparencia e información
- Confidencialidad

Compliance en tratamiento
- Política de Datos Personales (art. 14 ter)
- Registro de Actividades de Tratamiento (RAT)
- Evaluación de Impacto en Protección de Datos, EIPD (art. 15 ter)
- Manual de Prevención de Infracciones (art. 49 y ss.)

Privacy by Design & by Default
Protección desde el diseño y por defecto (art. 14 quater).

Encarga por contrato

Data Processing Agreement (DPA)

Contrato

3 Mandatario
ART. 15 BIS

Trata datos por cuenta del responsable.
Ejemplos: cloud, ERP, call center.
Encargo por contrato: Data Processing Agreement (DPA).

4 Receptor extranjero
Transferencia internacional
(arts. 27-29)

Licitud

País con nivel adecuado (ej. Europa): lícita.

País sin nivel adecuado (ej. EE. UU.): requiere contrato con cláusulas modelo, o modelos de cumplimiento o certificación entre responsable y receptor extranjero.

Principio rector *"Recoger la menor cantidad de datos posible, protegerlos desde el principio y no exponerlos salvo que el usuario lo decida expresamente."*

APLICA A TODO EL MAPA

Hoja de ruta de implementación

Seis meses de trabajo, en cuatro etapas

Mes 1
Gobernanza y diagnóstico

- Capacitación inicial Ley de Protección de datos personales
- Diagnóstico de brechas
- Checklist de nivel de madurez actual
- Contratos y proveedores
- Catálogo de políticas y procedimientos

Meses 2-3
Inventario y documentos

- Seguridad de datos y controles tecnológicos
- Matriz de riesgos
- Definición de roles Ley 21.719
- Determinar roles del Delegado de Protección de Datos

Meses 4-5
Controles y terceros

- Protocolos ARSOP
- Levantar el RAT
- Seguridad y evaluaciones de impacto
- Procesos de gestión de incidentes
- Capacitación de cumplimientos

Mes 6 en adelante
Modelo y mejora continua

- Acta del directorio
- Designar delegado o líder
- Canal de denuncia
- Auditoría interna
- Certificación ante la Agencia

Créditos: Sergio Escobar. Auditor líder e instructor ISO 27001, ISO 20000 e ISO 22301. Auditor interno ISO 9001. Cursos ISO 31000 y Ley de protección de datos.