

Data Protection Officer “DPO”: Chile y Colombia

ECIJA

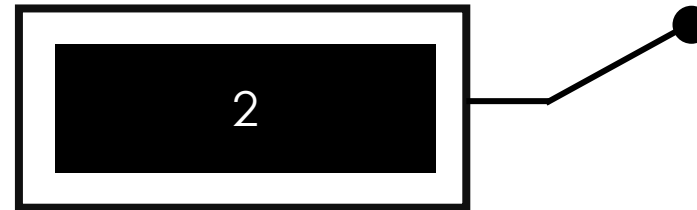
Conceptos fundamentales del ecosistema de datos



Data Protection Officer (DPO) o Delegado de Protección de Datos: Profesional que supervisa el cumplimiento de la normativa de protección de datos, asesora a la organización, promueve buenas prácticas y actúa como punto de contacto con la autoridad y los titulares, ejerciendo sus funciones con independencia.



Responsable del tratamiento: Persona o entidad que define los fines y medios del tratamiento de datos personales y asume la responsabilidad de su cumplimiento normativo.



Encargado del tratamiento: Persona o entidad que trata datos personales por cuenta del responsable, siguiendo sus instrucciones y sin decidir la finalidad del tratamiento.



Data Protection Officer en Chile



¿Existe regulación respecto el DPO Y que normativa regula la protección de datos?

- El nombramiento del DPO será obligatorio cuando el responsable del tratamiento adopte voluntariamente un modelo de prevención de infracciones.
- Se regula en el artículo 50 de la Ley N° 21.719, que modifica la Ley N° 19.628. Además, se encuentra en tramitación un reglamento sobre los modelos de prevención de infracciones.

¿Se determina algún proceso formal para su designación?

- El DPO debe ser designado por la máxima autoridad de la organización, y su contacto debe estar disponible para los titulares de datos.
- Puede desempeñar sus funciones como parte de la organización o mediante un contrato de servicios, pero siempre con autonomía en el ejercicio de sus funciones.
- Las empresas de un mismo grupo empresarial podrán designar un único DPO, si comparten estándares y políticas de protección de datos.

¿Cuáles son sus principales obligaciones?

- Principales obligaciones del DPO:
- Informar y asesorar sobre la normativa.
 - Supervisar el cumplimiento de la ley y de las políticas internas.
 - Promover la política de protección de datos dentro de la organización.
 - Capacitar al personal en tratamiento de datos personales.
 - Atender consultas de titulares y actuar como punto de contacto con la autoridad.

¿Debe contar con algún requisito para ejercer su cargo?

- Debe contar con idoneidad, capacidad y conocimientos especializados en protección de datos.
- Debe tener experiencia en la materia y habilidades profesionales para ejercer el cargo.
- Debe actuar con plena independencia, evitando conflictos de interés.
- En micro, pequeñas y medianas empresas, el dueño o la máxima autoridad puede asumir el rol de DPO

Data Protection Officer en Colombia



¿Existe regulación respecto al DPO Y que normativa regula la protección de datos?

- No existe obligación de designar un DPO. Sin embargo, la SIC recomienda su adopción mediante guías de buenas prácticas.
- Se regula principalmente por la Ley 1581 de 2012 y el Decreto 1074 de 2015. Esta normativa exige designar una persona o área responsable de protección de datos, y la SIC recomienda la figura del DPO como buena práctica para demostrar cumplimiento.

¿Se determina algún proceso formal para su designación?

- La SIC entrega recomendaciones para la designación del DPO. El responsable puede designarlo sin que el encargado deba hacerlo necesariamente, y si el DPO es compartido o externalizado, se recomienda definir claramente sus funciones y punto de contacto en el contrato.

¿Cuáles son sus principales obligaciones?

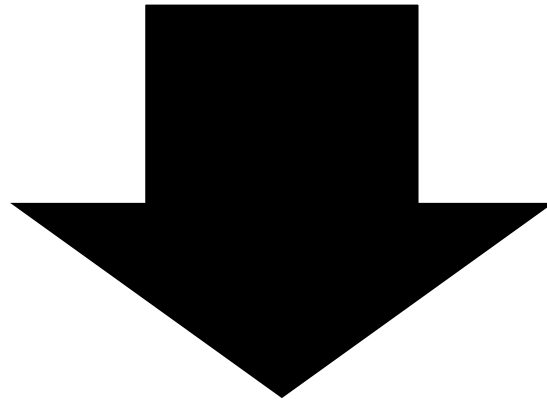
Principales obligaciones del DPO:

- Supervisar y asesorar sobre el cumplimiento de la normativa de protección de datos.
- Analizar las actividades de tratamiento y verificar su conformidad legal.
- Informar y recomendar medidas a la organización.
- Gestionar riesgos, controles y capacitaciones internas.
- Relacionarse con la SIC en materias de registros y trámites.

¿Debe contar con algún requisito para ejercer su cargo?

- La ley no establece requisitos obligatorios.
- Se recomienda conocimiento especializado en protección de datos, acorde al volumen y sensibilidad de los datos tratados.
- Conocimiento del sector o rubro de la organización y su normativa aplicable.
- Idealmente, nociones de estándares o regulación internacional.

DPO: Riesgos de no designarlo y beneficios de incorporarlo



Riesgos de no designar un DPO:
Mayor exposición a incumplimientos normativos, sanciones, gestión ineficiente de incidentes de seguridad y debilidades en la protección de datos, lo que puede afectar la confianza de clientes y autoridades.



Beneficios de incorporar un DPO:
Permite fortalecer el cumplimiento normativo, mejorar la gestión de riesgos y la gobernanza de datos, además de actuar como punto de contacto con autoridades y titulares, promoviendo buenas prácticas dentro de la organización.



ECIJA

www.ecija.com

The law firm of **the future**, today

Updates @   