

Data Protection Officer “DPO”: Chile y Argentina

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 Argentina



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

- No existe una regulación obligatoria sobre el DPO. Sin embargo, la Agencia de Acceso a la Información Pública (AAIP) ha promovido y recomendado su implementación mediante resoluciones administrativas para organismos de la Administración Pública Nacional.
- Mediante la Resolución AAIP 145/2025 (30 de julio de 2025), se creó el "Programa de fortalecimiento de Protección de Datos Personales en la Administración Pública Nacional", que busca implementar una red de DPOs en organismos públicos, integrada por responsables políticos y técnicos, con el objetivo de consolidarla en un plazo de 3 años.

¿Se determina algún proceso formal para su designación?

- En el sector privado, no existe un proceso obligatorio de registro o notificación ante la autoridad, por lo que su designación depende de la autonomía de la organización. Sin embargo, se recomienda formalizar el nombramiento en políticas internas o documentos que le otorguen jerarquía y respaldo jurídico.
- En el sector público, el proceso es más estricto, requiriendo notificación formal a la Red de Delegados de la AAIP.
- En ambos casos, se recomienda publicar los datos de contacto del DPO en las políticas de privacidad para asegurar transparencia y acceso de los titulares de datos.

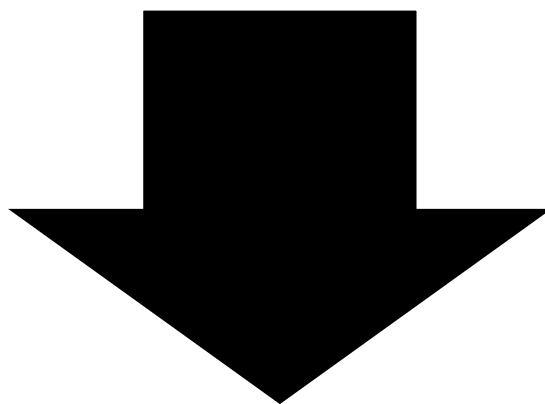
¿Cuáles son sus principales obligaciones?

- No existe una enumeración legal taxativa de sus funciones, tanto el sector público como privado.
- Sus obligaciones se definen en base a lineamientos internacionales, la Red Iberoamericana de Protección de Datos y guías de la AAIP:
 - Supervisar de forma independiente el cumplimiento de la normativa vigente.
 - Actuar como nexo técnico con la autoridad de control.
 - Coordinar evaluaciones de impacto en protección de datos.
 - Asesorar en la implementación de privacidad por diseño.
 - Gestionar y responder ante incidentes de seguridad.
 - Garantizar el ejercicio de derechos de los titulares (acceso, rectificación, supresión y oposición).

¿Debe contar con algún requisito para ejercer su cargo?

- No existen requisitos normativos obligatorios para el cargo.
- Se recomienda contar con conocimientos especializados en derecho y protección de datos.
- Debe tener comprensión técnica en seguridad de la información.
- No es obligatoria una certificación, pero la AAIP valora la idoneidad demostrable.
- Debe existir ausencia de conflicto de intereses.
- Requiere independencia funcional y reporte directo a la alta dirección.
- La organización debe garantizar recursos y tiempo suficientes para un ejercicio efectivo del rol.

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 @  **in** 