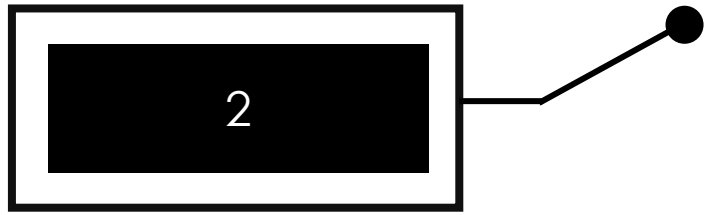
Data Protection Officer “DPO”: Chile y Puerto Rico

2026

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.

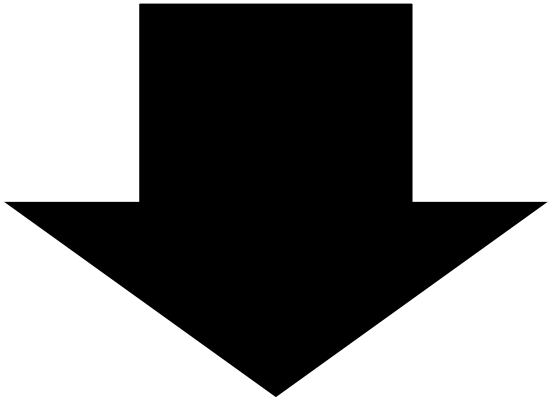
¿Debe contar con algún requisito para ejercer su cargo?

- 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 Puerto Rico

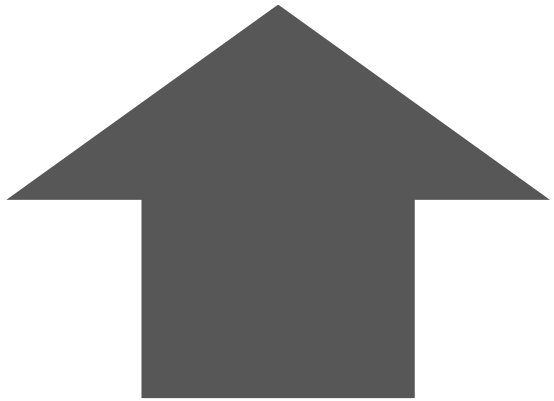
¿Existe regulación respecto el DPO y que normativa regula la protección de datos?	¿Se determina algún proceso formal para su designación?	¿Cuáles son sus principales obligaciones?	¿Debe contar con algún requisito para ejercer su cargo?
• Puerto Rico no posee una ley integral de protección de datos personales. Sin perjuicio de ello, existen diversas normas sobre privacidad, seguridad de la información y notificación de incidentes, entre ellas la Ley Núm. 11-2005 sobre seguridad de bancos de información, la Ley Núm. 39-2012 sobre políticas de privacidad en sitios web, y los Reglamentos Núm. 8568 y 7376 del DACO. • Así, Puerto Rico no cuenta con una disposición general que haga obligatoria la figura del DPO para todas las empresas privadas, ni existe un procedimiento formal establecido para su designación.	• No existe regulación que establezca un proceso formal para la designación de un DPO.	• Aunque no existe una obligación legal expresa, la designación de un DPO o responsable de privacidad es considerada una buena práctica internacional, especialmente para organizaciones que manejan grandes volúmenes de datos personales, información sensible, financiera, de salud o relativa a menores de edad.	• Dependiendo de la industria o del tipo de información tratada, pueden existir requisitos sectoriales indirectos, especialmente bajo normativa federal de Estados Unidos, como HIPAA (*Health Insurance Portability and Accountability Act*), GLBA (*Gramm-Leach-Bliley Act*) o estándares de ciberseguridad y cumplimiento contractual.

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

The law firm of the future, today

www.ecija.com

Updates @