Columnas & Opinión

Revista Pensamiento Penal
Sección Medios digitales y delitos informáticos
Vol. 2, núm. 3 – 2025, págs. 116–120
ISSN: 1853 – 4554

El delegado de protección de datos (DPO)

Por Carlos Damián Becerra[1]

La figura del delegado de protección de datos («DPO», por sus siglas en inglés) surge a partir de la incorporación del principio de *accountability* o responsabilidad proactiva en el Reglamento General de Protección de Datos («RGPD») de la Unión Europea. Este rol fue creado para facilitar el cumplimiento de las obligaciones en materia de protección de datos, rendir cuentas y actuar como intermediario entre las organizaciones, los titulares de los datos y las autoridades de control. El RGPD dispone que «al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos» (considerando 97 del Reglamento [UE] 2016/679). Realizar auditorías y dar respuesta a los ejercicios de derechos e incidentes de seguridad resulta esencial para un *data governance* efectivo

*delegado de protección de datos – reglamento general de protección de datos – protección de datos personales – accountability – data governance*

* * * * * *

a. La designación de un delegado de protección de datos

La designación de un delegado de protección de datos (en adelante «DPO», por sus siglas en inglés) será necesario cuando la figura del DPO debe ser designada principalmente en tres circunstancias clave. En primer lugar, cuando el tratamiento de datos personales sea realizado por una autoridad o un organismo público, excepto en los casos en que actúen los tribunales en el ejercicio de sus funciones judiciales.

En segundo término, resulta necesario contar con un DPO cuando la actividad principal del responsable o encargado del tratamiento implique la supervisión continua y sistemática de un gran número de personas interesadas, debido a la naturaleza, alcance y objetivos de dicho tratamiento.

Finalmente, la designación es obligatoria cuando el procesamiento se focaliza a gran escala en categorías especiales de datos, también conocidos como datos sensibles, o en información relativa a antecedentes

[1] Licenciado en administración. Abogado. Especialista en conducción de organizaciones militares terrestres. Especialista en estrategia operacional y planeamiento militar conjunto. Alumno en el posgrado de especialización en inteligencia estratégica (Centro de Altos Estudios Nacionales, «C.A.L.E.N»). Doctorando en derecho en la Universidad Nacional de Lomas de Zamora. Experto en protección de datos de la Universidad SXXI. Correo electrónico: abogarelderecho@gmail.com

judiciales o infracciones penales, conforme a lo especificado en los artículos correspondientes de la normativa vigente.

Estas condiciones responden a la necesidad de que las organizaciones con alta exposición y responsabilidad en el manejo de datos personales cuenten con un profesional capacitado para garantizar el cumplimiento normativo, asesorar sobre las obligaciones legales y actuar como enlace con las autoridades de supervisión. Lo expuesto precedentemente es según el artículo 37 del Reglamento General de Protección de Datos (en adelante, «RGPD») de la Unión Europea[2].

b. *Grupos empresariales u organismos públicos*

«Un grupo empresarial podrá nombrar un único DPO siempre que sea fácilmente accesible desde cada establecimiento»[3]

El RGPD establece que «cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único DPO para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño»[4]

c. *Funciones de un delegado de protección de datos*

(a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones que les incumben en virtud del Reglamento y de otras disposiciones de protección de datos aplicables;

(b) supervisar el cumplimiento de lo dispuesto en el reglamento, en otras disposiciones de protección de datos aplicables y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concientización y formación del personal que participa en las operaciones de tratamiento y las auditorías correspondientes;

(c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 3.

(d) cooperar con la autoridad de control;

(e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto[5].

En conclusión, las funciones asignadas al DPO, tal como establece el artículo 39 del RGPD, lo posicionan como un actor esencial para la gobernanza ética y legal del tratamiento de datos personales. No obstante, la efectividad de esta figura dependerá decisivamente de la autonomía, recursos, competencia y apoyo organizacional con que se le dote, así como de la madurez institucional respecto a la protección de datos en cada entorno específico.

---

[2] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos o «RGPD»). Regula el tratamiento de datos personales realizado por personas, organizaciones o empresas dentro de la Unión Europea

[3] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (art. 37).

[4] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (art. 37).

[5] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (art. 39).

d. Responsabilidad penal del delegado de protección de datos

Los DPO no son personalmente responsables en caso de incumplimiento del RGPD. El RGPD deja claro que es el responsable o el encargado del tratamiento es quien está obligado a garantizar y ser capaz de demostrar que el tratamiento se realiza de conformidad con sus disposiciones. Agencia Española de Protección de Datos (AEPD).

e. El delegado de protección de datos en Argentina

La resolución 40/2018 de la agencia de acceso a la información pública («AAIP»), al aprobar el documento *política modelo de protección de datos personales para organismos públicos*, recomienda a los organismos que implementen la figura del DPO. Expresamente, recomienda que para ello designen un agente de la planta permanente como delegado de protección de datos personales, que también se encargue de lo relacionado con el control de cumplimiento de la mencionada política[6].

Dicha resolución; representa un avance normativo importante al recomendar la instauración de la figura del DPO en los organismos públicos argentinos, sugiriendo que sea un agente de planta permanente quien asuma esta responsabilidad. Desde una perspectiva comprometida con los derechos humanos, esta iniciativa es positiva porque reconoce la necesidad de resguardar datos personales en el sector público, un ámbito donde la información sensible de los ciudadanos está fuertemente expuesta y cuya protección es esencial para garantizar el derecho a la privacidad y a la intimidad.

Sin embargo, la recomendación oficial también refleja desafíos profundos que atraviesan la implementación práctica de esta figura en Argentina. La designación «recomendada» y no obligatoria, junto con el hecho de que hasta fechas recientes solo un organismo público (el Registro Nacional de las Personas, y desde 2024 también la Agencia de Recaudación y Control Aduanero) cuenta con un DPO formal, evidencia la lentitud en la adopción de medidas concretas para garantizar este derecho fundamental.

Puede observarse un riesgo real de que la creación del DPO sea percibida como un formalismo administrativo más que como un compromiso genuino con la protección efectiva de las personas. Si el delegado carece de plena autonomía, soporte institucional y recursos suficientes, su capacidad para supervisar de manera independiente y rigurosa las prácticas de tratamiento de datos puede verse comprometida. Esto podría derivar en una protección débil frente a filtraciones, mal uso o negligencia, afectando derechos humanos esenciales.

En clave crítica, la consolidación de la figura del DPO debe estar acompañada de un fuerte impulso para promover la independencia institucional, la profesionalización y la transparencia. Se trata no solo de cumplir con una pauta técnica o normativa, sino de fortalecer el estado de derecho y la confianza ciudadana frente al manejo de información personal. El reconocimiento explícito de que el DPO actúa como interlocutor entre la autoridad de control y la organización, así como como garante del cumplimiento normativo, debe traducirse en garantías efectivas para que esta función no sea apenas formal sino realmente influyente en la protección de los derechos de las personas.

Por último, desde una mirada comprometida con los derechos humanos, la protección de datos personales en el sector público no puede limitarse a cumplir en letra con un documento modelo. Se debe avanzar hacia una cultura institucional que valore la privacidad como un derecho transversal, con capacitación continua, procedimientos claros y mecanismos

[6] Agencia de Acceso a la Información Pública (AAIP). Resolución 40/2018. *Política modelo de protección de datos personales para organismos públicos*, 4 de julio de 2018

efectivos de control y sanción ante incumplimientos. Solo así la Resolución 40/2018 podrá trascender su carácter declarativo y convertirse en una herramienta real para defender el derecho a la intimidad y prevenir abusos en el tratamiento de datos en el ámbito estatal argentino.

¿Qué tan realista es la implementación del DPO en el ámbito público argentino?

La implementación del DPO en el sector público argentino es un objetivo asumido en normativas y recomendaciones nacionales, como la Resolución 40/2018 de la AAIP. Sin embargo, la realidad muestra que la adopción efectiva de esta figura ha sido lenta y dispar. Hasta fechas muy recientes, eran prácticamente inexistentes las designaciones formales de DPO en organismos públicos, salvo excepciones puntuales como ARCA, que en 2024 se convirtió en el primer organismo del país en realizar una designación formal bajo este rol.

Los diagnósticos oficiales y de especialistas indican que muchos organismos carecen aún de políticas internas, manuales de procedimiento, planes de protección de datos y capacitación sistemática. La falta de estandarización y la necesidad de adaptar las recomendaciones nacionales a la realidad y necesidades de cada organismo o jurisdicción complican su implementación.

¿Existe riesgo de designaciones simbólicas, sin respaldo técnico ni autonomía?

Existe un riesgo real de que la designación del DPO en el sector público argentino se convierta en un trámite más formal que sustancial. Las recomendaciones y experiencias en talleres y capacitaciones han alertado sobre la posibilidad de que los organismos designen DPO sin brindarles suficiente autonomía, presupuesto ni capacitación técnica. Estos DPO podrían carecer de la capacidad real de actuar con independencia o de implementar cambios efectivos en la gestión de los datos personales, reduciendo su figura a un mero cumplimiento superficial de la normativa.

Las causas principales son

(1) Falta de personal especializado y presupuesto acotado para funciones de protección de datos;

(2) riesgo de designaciones recayendo en empleados sin la formación adecuada ni respaldo institucional; y

(3) posibilidad de acumulación de funciones o conflictos de interés al asignar el rol a funcionarios con otras responsabilidades ajenas a protección de datos.

¿Qué desafíos plantea esta figura en términos de independencia institucional?

Uno de los retos críticos al implementar la figura del DPO es garantizar su independencia funcional dentro de estructuras estatales a menudo jerárquicas y politizadas

(1) *Jerarquía administrativa*. El DPO podría verse sometido a presiones de superiores o cargos políticos, lo que podría limitar su capacidad de supervisar o denunciar irregularidades.

(2) *Recursos insuficientes*. Sin presupuesto y personal propio, el DPO dependería operacionalmente de las áreas que debe supervisar, afectando su autonomía.

(3) *Conflicto de intereses*. Cuando el DPO es un empleado interno que desempeña otras tareas o carece de estabilidad laboral, es más vulnerable a condicionamientos de la gestión política o administrativa.

(4) *Falta de respaldo legal en la práctica*. Aunque la normativa prevé independencia, su efectividad requiere voluntad política, controles externos y procesos transparentes de selección, formación y remoción.

Dimensiones clave de la independencia que deben reforzarse

(1) Autonomía funcional y presupuestaria.

(2) Estabilidad en el cargo y protección frente a represalias.

(3) Acceso directo a las máximas autoridades del organismo.

(4) Formación continua y certificación técnica.

f. Bibliografía

Agencia de Acceso a la Información Pública (AAIP). (2018, 4 de julio). *Resolución 40/2018. Política modelo de protección de datos personales para organismos públicos*. https://www.marval.com/publicacion/guia-de-fiscalizacion-en-materia-de-datos-personales-13919

Agencia de Acceso a la Información Pública (AAIP). (2019, 22 de febrero). *Resolución 34/2019. Modificaciones de la Disposición 60*.

Agencia de Acceso a la Información Pública (AAIP). (2022, 1 de diciembre). *Resolución 240/2022. Modificación de las disposiciones de la Dirección Nacional de Protección de Datos Personales*.

Agencia de Acceso a la Información Pública (AAIP). (2022, 5 de diciembre). *Resolución 244/2022. Sanciones. Topes máximos*.

Agencia de Acceso a la Información Pública (AAIP). (2022, 15 de diciembre). *Resolución 255/2022. Mejores prácticas en la aplicación de la Ley 25.326*.

Agencia Española de Protección de Datos (AEPD). (s.f.). *¿Cuál es la responsabilidad de un delegado de protección de datos?* https://www.aepd.es/es/preguntas-frecuentes/4-responsable-encargado-y-dpd/1-delegado-de-proteccion-de-datos/FAQ-0414-cual-es-la-responsabilidad-de-un-dpd

Argentina. (2000, 30 de octubre). *Ley 25.326. Protección de datos personales*.

Argentina. (2001, 29 de noviembre). *Decreto 1558/2001. Reglamentación de la Ley 25.326*.

Unión Europea. (2016, 27 de abril). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos)*. *Diario Oficial de la Unión Europea*, L 119, 1–88.