CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Posición de CEDPO sobre el Delegado de Protección de Datos (DPO) en el Reglamento General de Protección de Datos (RGPD)

15 de febrero de 2017

1. **Criterios de designación**

- "*Actividades principales*" debe interpretarse de acuerdo con la descripción del objeto social de la organización y los ingresos de la cuenta de pérdidas y ganancias.
- "*Gran escala*" debe entenderse según un enfoque basado en el riesgo (en lugar de utilizar únicamente criterios como el número de empleados o el "volumen" de datos personales procesado en un cierto período de tiempo).
- "*Observación de interesados*" debe excluir las actividades de supervisión de TI que cualquier organización debe realizar en la actualidad para los fines de (i) ciber(seguridad); (ii) proteger los sistemas y activos de la organización (incluyendo la propiedad intelectual e industrial y la información confidencial, así como los datos personales almacenados o tratados de otra forma por la organización); y (iii) cumplir con las leyes e instrucciones regulatorias (por ejemplo, obligaciones de protección de datos, acciones de lucha contra el fraude y blanqueo de capitales).

2. Perfil profesional

- A la vista de las tareas que se confían al/a la DPO, se requieren cualidades de distinta naturaleza, incluyendo conocimientos jurídicos, técnicos, de gestión de programas y de gestión de riesgos, así como habilidades de comunicación. El/la DPO debe velar por que sus funciones se lleven a cabo por él/ella mismo/a y/o por su equipo, formado por profesionales de diferentes perfiles, incluyendo pero no limitado a personas con titulación en Derecho o informática. La organización que nombra a un/a DPO debe facilitar al/ a la DPO recursos que reúnan estos diferentes perfiles.
- El RGPD exige que "*[E]l delegado de protección de datos será designado atendiendo a (…) sus conocimientos especializados del Derecho* (..)". La función del/de la DPO debe estar abierta a cualquier persona, cualquiera que sea su formación profesional o perfil curricular, y este requisito puede ser satisfecho incluso por profesionales que no cuenten con un título en Derecho. El texto no debe interpretarse de manera restrictiva; de lo contrario el riesgo es que los responsables y encargados considerarán fundamentalmente contratar abogados/as como DPOs.

3. DPO interno / externo

- El tamaño y las actividades de cada organización, así como su condición privada / pública determinarán si la decisión apropiada es un/a DPO interno/a o externo/a.
- Hay casos en los que podría tener sentido compartir el/la mismo/a DPO externo, como en el caso de pequeñas organizaciones y organizaciones que se ocupan de actividades de tratamiento de datos similares.
- Los/as DPOs externos/as pueden incluir personas jurídicas, aunque la organización cliente puede esperar una cierta estabilidad, en la medida en que sea compatible con las leyes locales, con respecto a la(s) persona(s) física(s) que acabe(n) finalmente asumiendo las tareas de DPO subcontratadas.
- La elección entre un/a DPO interno/a o externo/a no debe quedar influenciada por la protección laboral de los/las DPOs internos/as.

4. Independencia y conflicto de interés

- De nuevo, el tamaño y las actividades de cada organización deben determinar la estructura de DPO más adecuada. Si se trata de un/a DPO interno/a pero a tiempo parcial, así como si se trata de un/a DPO externo/a, tendrían que existir salvaguardas específicas para detectar y adoptar soluciones alternativas si surge un conflicto de intereses.

- La independencia del DPO no se debe interpretar para convertir al DPO en una (i) "mini-autoridad de protección de datos"; (ii) el/la CEO de la organización; o (iii) el representante de los interesado/as. La independencia del/de la DPO debe garantizarse con un/a DPO que tenga integridad y lealtad. De la misma manera, su relación con la organización debe estar de la "*potestas*" apropiada (lo que requiere un puesto patrocinado por los órganos de decisión de la organización, una línea de reporte funcional y recursos apropiados). El/la DPO debe tener una línea de reporte directo al Consejo de Administración –u órgano equivalente- de la organización o a un miembro de este, en relación a sus responsabilidades de DPO.
- Los deberes de confidencialidad del/de la DPO respecto a la organización que lo/la designó deben clarificarse para garantizar (i) que la lealtad del/ de la DPO respecto de su empleador (si es interno/a) o de su cliente (si es externo/a) no quede comprometida; y (ii) su adecuada integración en la organización como un/a "asesor/a de confianza".
- Los riesgos de conflicto de intereses pueden surgir si el puesto de DPO se sitúa en los departamentos de Seguridad, TI, RR.HH. u otros departamentos que tomen decisiones sobre las actividades de tratamiento de datos.

5. Posición

- El art. 38.3 estipula que el/la DPO informará directamente al más alto nivel jerárquico del responsable o del encargado. Esto requiere reforzar la autonomía y relevancia de los/las DPOs y requiere que la organización del responsable o del encargado vincule a los/las DPOs al más alto nivel jerárquico (como el Consejo de Administración o un miembro de este). Por ejemplo, la estructura organizativa debe garantizar que:
    - El/la DPO tenga acceso directo a la alta dirección y sin filtros, esto es, sin nivel intermedio entre el/la DPO y la alta dirección. Esto ayudará a garantizar que los/las DPOs no tengan conflictos de intereses respecto a su función como DPO y por lo tanto gocen de suficiente protección en el desempeño de sus tareas.
    - El respectivo Consejo o miembro del Consejo actúe como supervisor funcional y administrativo del/de la DPO, con responsabilidades respecto de las cuestiones relativas al personal y presupuesto del/ de la DPO.
    - La línea de reporte del/de la DPO a la alta dirección pueda ser claramente identificada (por ejemplo en un organigrama).

6. Ubicación

- La ubicación física específica de DPOs de un Grupo empresarial o DPOs de una organización que cuente con varios establecimientos parece irrelevante hoy en día. Su accesibilidad, una involucración en el negocio apropiada y una buena "red" local (por ejemplo, contando con profesionales de privacidad locales que sirvan de enlace), serían los elementos clave a tener en cuenta para asegurar una protección efectiva.
- La accesibilidad del/de la DPO no depende necesariamente solamente de sus propias habilidades, sino de la combinación de sus habilidades y las de su "red" local, por ejemplo, los mencionados enlaces locales de privacidad, para asegurar el conocimiento local jurídico y de lengua apropiados, cuando sea necesario. El Grupo de Trabajo recomienda que, para garantizar la accesibilidad, "*la comunicación tenga lugar en la lengua o lenguas utilizadas por las autoridades de control y los interesados*". Esta recomendación puede plantear problemas prácticos si no aporta mayor precisión. El RGPR no puede esperar que cualquier DPO de Grupo empresarial hable las 24 lenguas de la UE o de cada establecimiento de la UE de su Grupo. Por lo tanto, sugerimos que se añada que no se requiere que el/la propia/a DPO hable los idiomas de todos los países donde el responsable/encargado está establecido pero

que, en la práctica, esta necesidad puede ser satisfecha a través de traducciones de documentos y de los enlaces locales que asistan al/a la DPO. El RGPR es otra pieza de cómo se construye el mercado interior de la UE y no debería imponer ninguna restricción a la libertad de circulación de los profesionales y servicios de los DPOs dentro de la UE. El requisito del idioma no debe ser un obstáculo para la construcción de la UE.

7. Responsabilidad

- El/la DPO no debería tener una responsabilidad individual en el RGPR por tratamientos de datos: la organización es la responsable de cualquier incumplimiento. La organización puede decidir tomar acciones, de acuerdo con la ley local, contra un/a DPO negligente, tal y como sería el caso respecto de cualquier otro/a empleado/a o contratista que pueda ser considerado responsable en última instancia de los daños y perjuicios (por ejemplo, multas, prohibiciones de procesamiento, etc.) sufridos por la organización.

8. Tareas

- Registro de las actividades de tratamiento. El/la DPO asesora sobre la estructura del registro de las actividades de tratamiento, así como las reglas aplicables a su mantenimiento. Posteriormente, el/la DPO verifica periódicamente que el registro esté completo y sea preciso (deber de supervisión) y facilita orientaciones al responsable del tratamiento (a los respectivos departamentos) para corregir lo que es incorrecto.
- El RGPR prevé que la llevanza del registro de las actividades de tratamiento corresponde al responsable del tratamiento o a su representante (artículo 30). El DPO puede entonces encargarse de mantener el registro como representante del responsable. Esto no sería un caso de conflicto de intereses.
- Evaluaciones de impacto relativas a la protección de datos (DPIA, en su acrónimo en inglés): las DPIAs se realizan por el responsable de tratamiento. El/la DPO asesora al responsable de tratamiento respecto de la obligación o la oportunidad de llevar a cabo una DPIA. Posteriormente, el/la DPO emite su opinión sobre la pertinencia del análisis de riesgo realizado. Una vez que los riesgos se han mitigado, el/la DPO emite un dictamen sobre las medidas de mitigación para analizar la posibilidad de mitigar los potenciales riesgos remanentes.
- Una de las tareas del/ de la DPO que se podría agregar como una recomendación, y que sería una buena práctica de responsabilidad activa (*accountability*), sería la elaboración de un informe anual dirigido al más alto nivel jerárquico.

9. Formación

- Los/as DPO *deben* tener la oportunidad de mantenerse actualizados/as respecto a los desarrollos en materia de protección de datos en el sentido más amplio del término, incluidas actualizaciones legislativas, nuevas tecnologías, cuestiones internacionales, técnicas de auditoría ... El nivel de conocimientos de los/las DPO debe incrementarse constantemente, mediante su participación en cursos de formación de protección de datos y otras formas de desarrollo profesional, como su participación en foros de protección de datos, talleres de trabajo, etc. El Grupo de Trabajo del Artículo 29 debería dejar claro que este tipo de desarrollo profesional continuo por parte de los/as DPOs es, en realidad, un requisito implícito de carácter obligatorio de conformidad con los arts. 37.5 y 38.2. Además, para cumplir con el espíritu del requisito de *accountability* del art. 5.2, los/las DPO deben poder acreditar su desarrollo profesional continuo.

10. Publicación de los datos de contacto del DPO

- Las organizaciones deben poder proporcionar datos de contacto genéricos, tales como dpo@company.com. La organización debe poder decidir el nivel de información a proporcionar para garantizar una comunicación fluida con las partes interesadas externas (incluyendo pero no limitado a los/as interesados/as) así como el respeto por la privacidad del/de la DPO: Podemos sugerir la siguiente redacción:

  "El a*rtículo 37.7 no requiere que los datos de contacto que se publiquen incluyan el nombre del / de la DPO. El responsable de tratamiento y el/la DPO son quienes deben decidir lo que es necesario i útil como a las circunstancias particulares de que se trate.*"

Acerca de CEDPO:

CEDPO se fundó en septiembre de 2011 por organizaciones europeas de protección de datos, esto es, **AFCDP** (*Association Française des Correspondants à la Protection des Données à Caractère Personnel*), de Francia, **APEP** (*Asociación Profesional Española de Privacidad*), de España, **GDD** (*Gesellschaft für Datenschutz und Datensicherheit*), de Alemania, y **NGFG** (*Nederlands Genootschaap van Functionarissen voor de Gegevensbescherming*), de los Países Bajos. A la Confederación de unieron pronto **ADPO** (Association of Data Protection Officers), de Irlanda, **ARGE DATEN**, de Austria y **SABI** (*Stowarzyszenie Administratorów Bezpieczeństwa Informacji*), de Polonia.

CEDPO tiene por objeto promocionar el rol del /de la Delegado de Protección de Datos, facilitar asesoramiento respecto de una protección equilibrada, practicable y efectiva data y contribuir a una mejor armonización de las leyes y prácticas en materia de protección de datos en la UE/EEE.

Datos de contacto

Email: info@cedpo.eu / Sitio web: www.cedpo.eu