EL ROL DEL DPO EXTERNO: FUNCIONES Y LIMITACIONES

Sabadell, 17 de febrero de 2026

1. Finalidad y alcance

Estas directrices establecen cómo debe relacionarse **el RESPONSABLE DEL TRATAMIENTO** con **BETA LEGAL ASSESSORS, S.L.** como **Delegado de Protección de Datos (DPO) externo**, con el fin de:

- Asegurar una **gobernanza clara** de privacidad.
- Garantizar la **independencia** del DPO y la eficacia del modelo de cumplimiento.
- Evitar expectativas incorrectas sobre **responsabilidades** y **toma de decisiones**.
- Definir un modo de trabajo homogéneo en proyectos, proveedores, brechas, derechos y documentación.

Se aplican a todos los tratamientos de datos personales del RESPONSABLE DEL TRATAMIENTO, tanto cuando actúe como responsable/corresponsable como cuando actúe como encargado del tratamiento.

2. Rol del DPO: qué es y qué no es

2.1. Naturaleza del rol

El DPO asume una función especializada e independiente cuyo objetivo es **informar, asesorar y supervisar** el cumplimiento en protección de datos, actuando, por tanto, como:

- **Asesor** de la organización (criterios y recomendaciones).
- **Supervisor** del cumplimiento y del sistema de control.
- **Punto de contacto** para personas interesadas y autoridad de control.
- **Impulsor** de privacidad desde el diseño y por defecto en procesos y proyectos.

2.2. Reparto esencial de responsabilidad

La **responsabilidad última** del cumplimiento y de las decisiones sobre los fines y medios del tratamiento es del RESPONSABLE DEL TRATAMIENTO. El DPO es una figura de garantía y control interno, no un sustituto del responsable.

Qué puede hacer el DPO

- Formular **recomendaciones técnicas y jurídicas** y documentarlas.
- Solicitar evidencias y promover un **plan de mejora**.

- Elevar riesgos a Dirección cuando sea necesario.
- Actuar como canal de consulta y contacto.

Qué no puede hacer el DPO

- **Decidir** fines y medios del tratamiento.
- **Aprobar** formalmente tratamientos, proyectos o proveedores como "decisor final".
- Asumir la **responsabilidad** del cumplimiento de la empresa.
- Convertirse en "propietario" de los procesos operativos (IT/RRHH/Marketing, etc.).

3. Posición del DPO en la organización: independencia, acceso y garantías

3.1. Independencia y ausencia de instrucciones

Para que el DPO sea eficaz en su labor, el **RESPONSABLE DEL TRATAMIENTO** debe garantizar que el DPO:

- No recibe instrucciones sobre el contenido de sus análisis o recomendaciones.
- Puede desarrollar su función sin presiones o condicionantes indebidos.
- Puede emitir su criterio, aunque sea crítico con un proyecto o práctica.

Puede

- Emitir informes y recomendaciones **sin aprobación previa**.
- Solicitar información y reunirse con equipos internos.
- Escalar asuntos a la más alta Dirección.

No puede

- Ser dirigido para "concluir" en un sentido predeterminado.
- Condicionar su criterio a objetivos comerciales u operativos.

3.2. Acceso a alta dirección

Debe existir un canal efectivo para que el DPO pueda dirigirse a la **máxima instancia de decisión** cuando lo requiera un asunto, riesgo o incumplimiento relevante.

Puede

- Mantener interlocución directa con Dirección o Comité de Cumplimiento.
- Solicitar decisiones formales cuando existan riesgos relevantes.

No puede

- Quedar limitado a mandos intermedios cuando el riesgo requiere decisión ejecutiva.

3.3. No penalización por el desempeño del rol

El DPO no debe ser penalizado de ningún modo por el contenido de sus recomendaciones o por ejercer su función de supervisión.

Puede

- Señalar incumplimientos o carencias sin temor a represalias.

No puede

- Ser "apartado" o presionado por emitir recomendaciones "incómodas" o que choche, de alguna manera, con el objetivo del negocio.

4. Recursos, información y accesos mínimos necesarios

4.1. Recursos

Para que el DPO pueda desempeñar su rol, el **RESPONSABLE DEL TRATAMIENTO** debe facilitar:

- Tiempo y disponibilidad de interlocutores.
- Acceso a documentación, sistemas (cuando proceda) y evidencias.
- Medios para operar (canales, herramientas, soporte).

4.2. Acceso a información

El DPO debe poder acceder a:

- Inventario/registro de tratamientos (o información equivalente).
- Contratos con encargados/proveedores y anexos de protección de datos.
- Descripción de sistemas, flujos de datos, ubicaciones y subencargados.
- Procedimientos y evidencias (derechos, brechas, formación, seguridad, retención).
- Evaluaciones de riesgo y DPIA cuando aplique.

Puede

- Requerir evidencias y documentación razonables y proporcionales.
- Acceder a datos personales **si es estrictamente necesario** para su función y con controles adecuados.

No puede

- Exigir accesos indiscriminados o desproporcionados a datos/sistemas sin necesidad.
- Sustituir a IT/Seguridad/RRHH en su operativa diaria.

5. Funciones del DPO: alcance operativo (qué hace y cómo)

5.1. Informar y asesorar

Incluye:

- Bases legitimadoras, transparencia, conservación, comunicaciones y transferencias.
- Diseño de procesos (*privacy by design/by default*).
- Revisión de cláusulas informativas, formularios, textos, contratos y anexos.
- Asesoramiento en nuevas tecnologías (IA, analítica avanzada, biometría, videovigilancia, rastreadores, etc.).

Puede

- Proponer medidas, alternativas y salvaguardas.
- Recomendar cambios o condiciones para un despliegue responsable.

No puede

- Autorizar el tratamiento como "visto bueno obligatorio".
- Imponer decisiones de negocio.

5.2. Supervisar y monitorizar el cumplimiento

Incluye:

- Revisiones planificadas (auditorías internas, muestreos, controles).
- Seguimiento de planes de acción y priorización.
- Recomendación de políticas y procedimientos.

Puede

- Auditar evidencias y emitir informes sobre hallazgos con prioridades.
- Proponer métricas y revisiones periódicas.

No puede

- "Certificar" un cumplimiento absoluto.

- Asumir la ejecución completa del plan de acción (eso corresponde a áreas responsables).

5.3. DPIA / Evaluación de impacto (cuando proceda)

Incluye:

- Ayudar a determinar cuándo corresponde.
- Asesorar metodología y medidas.
- Revisar y emitir recomendaciones sobre conclusiones.

Puede

- Guiar y revisar una DPIA.
- Recomendar medidas de mitigación y controles.

No puede

- Ser el "propietario" o quien elabora la DPIA ni el responsable de su aprobación final.
- Sustituir a las áreas de negocio/IT en la descripción real del tratamiento y medidas.

5.4. Brechas de seguridad

Incluye:

- Ser incluido desde el inicio en el circuito de incidentes.
- Asesorar sobre riesgo, notificación, comunicación y medidas.

Puede

- Analizar impacto, recomendar notificación/comunicación y contenidos.
- Revisar borradores y mensajes a interesados.

No puede

- Realizar contención técnica, forense o remediación (función de IT/Seguridad).
- Decidir unilateralmente la notificación: la decisión final es de la empresa.

5.5. Derechos de los interesados y reclamaciones

Incluye:

- Diseñar y revisar el proceso.

- Apoyar en casos complejos.
- Analizar reclamaciones y recomendar mejoras.

Puede

- Coordinar criterios y revisar respuestas complejas.
- Recomendar medidas de prevención ante reclamaciones repetidas.

No puede

- Firmar o emitir en nombre de la empresa la respuesta final sin conocimiento del Responsable del Tratamiento.
- Obstaculizar el acceso de un interesado a la autoridad de control.

5.6. Punto de contacto con la autoridad y con interesados

Puede

- Actuar como canal de contacto, facilitar interlocución y coherencia.
- Recibir consultas externas y canalizarlas a la organización.

No puede

- Sustituir la voluntad corporativa ni "reconocer hechos" sin coordinación interna.
- Asumir la representación procesal contenciosa cuando comprometa su independencia (debe separarse del rol de defensa).

6. Límites del DPO y "líneas rojas" (lo que no se le debe pedir)

1. **No se le puede convertir en responsable del cumplimiento** ("que el DPO se encargue de todo").
2. **No se le puede asignar un rol decisor** sobre fines/medios del tratamiento.
3. **No se le puede situar en funciones operativas incompatibles** y luego pedirle que se audite a sí mismo.
4. **No se le puede exigir un resultado** ("cero riesgo", "cero sanción").
5. **No se le puede impedir el acceso** a información necesaria para supervisar.

7. Conflictos de interés: prevención y gestión

7.1. Norma general

Hay conflicto cuando el DPO ocupa una posición que le permite **determinar fines y medios** del tratamiento, o cuando debe evaluar decisiones propias.

7.2. Puestos típicamente de riesgo (orientativo)

Suelen ser incompatibles o de alto riesgo:

- Alta dirección (CEO/COO/CFO u homólogos).
- Dirección/Responsabilidad operativa de IT/Seguridad con control de decisiones sobre el tratamiento.
- Dirección de RRHH cuando determina tratamientos de empleados.
- Dirección de Marketing/Ventas cuando diseña perfiles, segmentaciones y tratamientos masivos.
- Compliance operativo cuando define y ejecuta controles y luego se evalúa.

7.3. Medidas de mitigación

- Matriz de incompatibilidades.
- Procedimiento de recusación (en proyectos donde haya intervenido operativamente).
- Separación de canales si presta otros servicios (p. ej., legal general), con **expedientes y circuitos separados**.
- Registro interno de conflictos identificados y cómo se mitigaron.

Puede

- Poner de manifiesto un conflicto de intereses y solicitar medidas.
- Abstenerse/recomendar sustitución puntual en una revisión.

No puede

- Mantener simultáneamente un rol decisor y el rol de supervisión sobre el mismo tratamiento.

8. Modelo de relación: protocolos por escenarios

8.1. Proyectos nuevos y cambios relevantes

Involucración temprana obligatoria interna cuando existan tratamientos relevantes o de riesgo:

- Nuevas herramientas o proveedores con acceso a datos.
- Tratamientos a gran escala, perfiles, IA, vigilancia, biometría, geolocalización.
- Integraciones, migraciones, data lakes, analítica avanzada.

Flujo recomendado

1. Brief (finalidad, categorías, colectivos, proveedores, países, medidas).

2. Análisis de base jurídica, transparencia, minimización, retención.
3. Recomendaciones y plan de mitigación.
4. Decisión sobre DPIA.
5. Cierre documental antes de producción.

8.2. Proveedores (encargados/subencargados)

Antes de contratar:

- Due diligence de privacidad y seguridad.
- Definición de roles.
- Contrato y anexo de tratamiento.
- Transferencias y garantías (si aplica).

8.3. Brechas

Activación inmediata. Contenido mínimo: qué, cuándo, sistemas, datos, volumen, medidas, contención, evaluación preliminar.

8.4. Derechos

Circuito estándar con registro, verificación, búsqueda, evaluación, respuesta y evidencias.

9. Publicidad y accesibilidad del DPO (canales y comunicación externa)

La empresa debe asegurar que los interesados puedan contactar con el DPO de forma sencilla (correo/canal publicado en políticas y avisos de privacidad cuando corresponda) y que internamente exista un circuito para canalizar esas consultas con rapidez.

10. Checklist mínimo de gobernanza del DPO

- Interlocutor interno (privacy coordinator).
- Canal de contacto dedicado (interno y externo).
- Procedimiento a seguir ante los proyectos (privacy by design).
- Procedimiento de brechas con participación del DPO.
- Procedimiento de derechos y registro de solicitudes.
- Proceso de alta de proveedores con revisión de privacidad.
- Matriz de conflictos de interés y recusación.
- Registro de recomendaciones y decisiones (trazabilidad).

FAQS (preguntas frecuentes)

1) ¿El DPO es responsable del cumplimiento?

No. El DPO asesora y supervisa; la responsabilidad y decisión final del cumplimiento es de la empresa

2) ¿Las recomendaciones del DPO son obligatorias?

No son órdenes. Deben considerarse seriamente. Si la empresa decide no seguirlas, debe documentar la decisión y su razonamiento, definiendo medidas alternativas si procede.

3) ¿Puede el DPO aprobar un tratamiento/proyecto/proveedor?

No como aprobador final. Puede recomendar condiciones y advertir riesgos. La decisión final corresponde a la empresa.

4) ¿Debe consultarse al DPO al inicio de un proyecto?

Sí, especialmente si hay datos a escala, nuevas tecnologías, perfiles, monitorización, biometría, IA, tratamientos sensibles o decisiones automatizadas. La consulta tardía suele generar reprocesos y riesgo.

5) ¿Quién hace la DPIA?

La empresa. El DPO asesora, guía, revisa y recomienda, pero no es el propietario ni el aprobador final.

6) ¿Puede el DPO tener acceso a datos personales?

Sí, si es necesario para sus funciones, de forma proporcional y con controles (minimización, confidencialidad, trazabilidad).

7) ¿El DPO decide si se notifica una brecha?

El DPO asesora sobre riesgo y criterios de notificación. La decisión final y la ejecución corresponden a la empresa.

8) ¿El DPO puede responder derechos en nombre de la empresa?

Puede apoyar y revisar. La respuesta formal debe seguir el circuito corporativo del responsable y contar con su autorización, salvo que se acuerde expresamente un soporte operativo específico.

9) ¿Qué puestos suelen ser incompatibles con el DPO?

Roles que determinen fines y medios del tratamiento (p. ej., dirección operativa de IT/Seguridad, RRHH, Marketing, alta dirección) o que obliguen al DPO a evaluarse a sí mismo.

10) ¿Qué hacemos si detectamos un posible conflicto de interés?

Se documenta, se aplica separación funcional o recusación, y se asigna la revisión a un perfil independiente cuando proceda.

11) ¿El DPO puede actuar como abogado del Responsable del Tratamiento en un procedimiento judicial relacionado con protección de datos?

Debe evitarse cuando comprometa la independencia. La defensa procesal debe separarse del rol del DPO.

12) ¿Qué se necesita para que el DPO sea eficaz?

Interlocutor interno, acceso a documentación y responsables, participación temprana en proyectos, comunicación inmediata de incidentes y compromiso con la ejecución de medidas.