Privacidad, biometría y función del DPO

Evaluación de impacto, proporcionalidad del reconocimiento facial y propuesta de supervisión independiente.

ÍNDICE

1. Obligatoriedad e independencia del DPO 3

2. Evaluación de Impacto en Protección de Datos (EIPD) 4

3. Papel del DPO en la Evaluación de Impacto 8

4. Relación entre los riesgos de seguridad y la protección de datos 9

5. Propuesta de servicio de DPO externo 9

6. Comunicación con la AEPD 12

Bibliografía y referencias normativas 12

1. Obligatoriedad e independencia del DPO

PYME Sanitaria Mediterránea | Informe para Dirección

1.1. Comprobación de obligatoriedad

Supuesto legal	¿Aplica?	Justificación
Art. 37.1.a RGPD: organismo público	No	El hospital es privado.
Art. 37.1.b RGPD: observación sistemática a gran escala	No acreditado	No consta que esta sea su actividad principal.
Art. 37.1.c RGPD: datos especiales a gran escala	Sí	Trata continuamente datos de salud de unos 85.000 pacientes al año.
Art. 34.1.l LOPDGDD: centros sanitarios	Sí	El hospital está obligado a mantener historias clínicas.
Otros sectores del art. 34 LOPDGDD	No	No desarrolla actividades de seguros, seguridad privada, juego, telecomunicaciones, información crediticia ni distribución de energía.

Resultado: DPO obligatorio. Basta con cumplir uno de estos supuestos. En Mediterránea concurren el tratamiento sanitario a gran escala y la obligación específica de los centros sanitarios.

1.2. Situación actual e independencia

La documentación interna indica que el responsable de IT lleva aproximadamente dos años gestionando asuntos de protección de datos. El correo de RR. HH. del 4 de abril de 2026 confirma que recibe consultas sobre derechos de los trabajadores y que el contacto de privacidad publicado en la web llega a su bandeja. No consta su nombramiento formal como DPO.

Esta situación debe regularizarse. IT participó en la propuesta de reconocimiento facial y podría tener que supervisar decisiones en las que intervino. Si el responsable de IT decide cómo se tratan los datos, no debería actuar también como DPO, porque existiría un conflicto de intereses (art. 38.6 RGPD). Gerencia debe comprobar sus funciones y garantizar que el DPO pueda trabajar con independencia.

1.3. Elección de DPO interno o externo

Criterio	Interno	Externo
Recursos	Requiere personal y dedicación suficientes.	Servicio contratado según necesidades.
Independencia	Exige separar funciones de IT.	Facilita la supervisión independiente.

Criterio	Interno	Externo
Especialización	Requiere experiencia en privacidad sanitaria.	Permite contratar experiencia específica.
Coste	Estimación de coste anual: 54.000 €/año.	Coste variable según alcance y dedicación.

Recomendación: contratar un DPO externo especializado en sanidad. El precio y la dedicación concretos se justificarán en la propuesta de servicio.

El DPO deberá asesorar, supervisar el cumplimiento, revisar las EIPD y actuar como contacto con la AEPD (art. 39 RGPD). Tendrá acceso directo a Gerencia, recursos suficientes y autonomía para emitir sus recomendaciones, sin recibir instrucciones sobre su criterio (art. 38 RGPD).

Decisión para Dirección: comprobar si existe un nombramiento válido y, de no existir, designar formalmente un DPO independiente. La designación deberá comunicarse a la AEPD en diez días (art. 34.3 LOPDGDD).

2. Evaluación de Impacto en Protección de Datos (EIPD)

Entidad: PYME Sanitaria Mediterránea · Centro 1, Valencia.
Tratamiento evaluado: reconocimiento facial para controlar el acceso del personal a quirófanos y zonas de hospitalización.
Responsable del tratamiento: PYME Sanitaria Mediterránea.
Estado: contratación iniciada; implantación y pruebas con datos biométricos no acreditadas.

2.1. Descripción del tratamiento

El 11 de marzo de 2026, el jefe de Quirófanos propuso implantar reconocimiento facial para reforzar el control de presencia del personal en zonas quirúrgicas y de hospitalización. Dirección autorizó iniciar la contratación y solicitar presupuestos a dos proveedores. No consta una consulta previa a asesoría jurídica ni una evaluación de impacto.

La propuesta consiste en utilizar características faciales del personal para comprobar su identidad antes de permitirle acceder a zonas restringidas. Sin embargo, todavía no se ha definido cómo funcionará el sistema ni qué información conservará.

Elemento	Información disponible
Finalidad	Restringir el acceso a quirófanos y hospitalización al personal autorizado.
Personas afectadas	Trabajadores y otros profesionales que necesiten acceder a estas áreas.
Datos y origen	Imágenes faciales y posibles plantillas biométricas obtenidas directamente del personal; registros de acceso si el sistema los genera.
Base jurídica	No determinada. Debe acreditarse una base del art. 6 RGPD y una excepción válida del art. 9.2.
Proveedores	Dos candidatos pendientes de presupuestar. No consta adjudicación ni

Elemento	Información disponible
	definición de sus responsabilidades.
Acceso y destinatarios	Sin definir. Debe comprobarse si el proveedor accedería a los datos y, en su caso, formalizar el contrato del art. 28 RGPD.
Conservación y transferencias	No constan plazos, ubicación de almacenamiento ni posibles transferencias internacionales.
Tecnología	Reconocimiento facial propuesto; pendiente de determinar si será identificación 1:N o verificación 1:1.

¿Por qué es necesaria una EIPD?

La propuesta utilizaría datos biométricos para identificar al personal. Por la sensibilidad de estos datos y los efectos que podría tener sobre los trabajadores, debe realizarse una EIPD antes de comenzar (art. 35.1 RGPD). La AEPD también exige justificar por qué es necesario utilizar biometría y no otra solución menos invasiva.

No consta que el proyecto incluya decisiones automatizadas con efectos jurídicos, vigilancia de espacios públicos a gran escala ni tratamiento biométrico de pacientes. No se atribuyen al proyecto características que el expediente no acredita.

2.2. Evaluación de necesidad y proporcionalidad

El objetivo del hospital es legítimo: proteger las zonas asistenciales y evitar accesos no autorizados. La cuestión es si necesita reconocimiento facial para conseguirlo.

El expediente no documenta accesos indebidos anteriores, fallos de identificación ni pruebas de que los controles existentes sean insuficientes. Tampoco explica por qué se ha elegido biometría frente a otras soluciones.

Alternativa	Valoración para el Centro 1
Tarjeta individual y PIN	Permite identificar al personal autorizado sin captar datos biométricos.
Permisos por función	Limita los accesos según el puesto y permite retirar autorizaciones cuando cambian las funciones.
Control adicional en áreas críticas	Puede reforzar determinados accesos sin extender la biometría a todo el personal.
Reconocimiento facial	Introduce datos especialmente protegidos sin una necesidad demostrada.

Para justificar la biometría, Dirección Médica e IT tendrían que documentar los problemas concretos del sistema actual, explicar por qué las alternativas no resultan suficientes y acreditar la base jurídica del tratamiento.

El **art. 6 RGPD** exige una base legal para tratar los datos personales. Además, al utilizar información biométrica para identificar de manera unívoca a los trabajadores, debe cumplirse alguna de las

condiciones del **art. 9.2 RGPD**. La finalidad de seguridad no basta por sí sola para cumplir ambos requisitos. El consentimiento tampoco constituye una solución adecuada sin demostrar que sería realmente libre en el contexto laboral.

Resultado: con la información disponible, el reconocimiento facial no supera la evaluación de necesidad y proporcionalidad del **art. 35.7.b RGPD**. Recomendamos priorizar un sistema no biométrico que también permita entradas rápidas en situaciones de urgencia.

2.3. Identificación y evaluación de riesgos para los derechos y libertades

Esta evaluación analiza las consecuencias para los trabajadores, no únicamente los posibles daños a los sistemas del hospital.

Se utiliza una escala cualitativa de probabilidad e impacto: **baja (B), media (M) y alta (A)**. Para evitar interpretaciones distintas, el nivel resultante sigue esta regla: B×B = bajo; B×M y M×B = bajo; M×M = medio; cualquier combinación con impacto alto y probabilidad media o alta = alto. B×A y A×B se consideran medios; A×M y A×A, altos.

Las probabilidades son estimaciones preventivas, no estadísticas de incidentes ocurridos. Se valoran a partir de la tecnología propuesta, el entorno hospitalario y la información que falta por definir.

Riesgo para los trabajadores	Prob.	Impacto	Nivel
R1. Acceso no autorizado: exposición de imágenes o plantillas faciales, con posible utilización indebida de la identidad.	M	A	Alto
R2. Modificación no autorizada: alteración de autorizaciones que provoque una denegación injustificada de acceso al puesto.	M	A	Alto
R3. Pérdida o destrucción: desaparición de registros necesarios para acreditar o recuperar autorizaciones de entrada.	M	M	Medio
R4. Reidentificación: utilización de características faciales para reconocer al trabajador en otros sistemas o contextos.	M	A	Alto
R5. Discriminación o sesgos: errores de reconocimiento que afecten de forma desigual a determinados empleados.	M	A	Alto
R6. Pérdida de control: uso de los registros para seguir movimientos o actividades del personal con otra finalidad.	M	A	Alto

Justificación del impacto. R1 y R4 pueden afectar gravemente a la privacidad porque las características biométricas no pueden sustituirse con facilidad como una contraseña. R2 y R5 podrían dificultar el acceso del personal sanitario a su puesto; su impacto aumentaría si interfirieran en una urgencia asistencial. R6 supone el riesgo de utilizar información de seguridad para vigilar al personal sin una justificación adecuada.

R3 se clasifica inicialmente como medio porque la pérdida de un registro no implica necesariamente exposición de datos ni imposibilidad de trabajar. Si el diseño impidiera acceder a quirófanos durante una urgencia, habría que elevar su impacto.

A estos seis escenarios se añade una cuestión previa: **no se ha acreditado la licitud ni la necesidad del tratamiento biométrico**. Esta deficiencia no desaparece aunque el sistema tenga buenas medidas de seguridad.

2.4. Medidas previstas para hacer frente a los riesgos

Las medidas responden a los riesgos identificados y se adaptan a los accesos de quirófanos y hospitalización del Centro 1.

Riesgo	Medida concreta	Responsable y plazo	Riesgo residual
R1	No captar imágenes faciales mientras se evalúa el proyecto. Si se reconsidera, comprobar el cifrado y quién tendría acceso a los datos para reducir el riesgo de exposición.	IT y Compras. **Antes de contratar.**	Alto; sin medidas acreditadas.
R2	Dar permisos según el puesto y disponer de otra forma de entrada. Así se evitarían bloqueos injustificados y retrasos ante una urgencia.	IT y Dirección Médica. **Antes de implantar.**	Alto; sin pruebas.
R3	Preparar la recuperación de los registros y una apertura excepcional documentada. Así se reducirían los retrasos si falla el sistema.	IT y responsable de Quirófanos. **Antes de implantar.**	Medio; sin pruebas.
R4	Pedir al proveedor que explique si guarda, exporta o reutiliza las plantillas faciales. Prohibir otros usos para reducir el riesgo de reidentificación.	IT y Compras. **Antes de contratar.**	Alto; sin verificar.
R5	Comprobar los errores de reconocimiento y ofrecer una revisión humana y entrada alternativa. Así se reducirían las exclusiones injustificadas.	IT, RR. HH. y Dirección Médica. **Antes de implantar.**	Alto; sin verificar.
R6	Limitar los registros al control de accesos, definir quién puede consultarlos y cuánto tiempo se conservan. Revisar su uso para evitar el seguimiento indebido del personal.	RR. HH. y Gerencia. **Antes de implantar.**	Alto; sin verificar.

Valoración residual. Las medidas propuestas podrían reducir los riesgos, pero todavía no se ha demostrado que funcionen ni que estén implantadas. Por eso se mantienen los niveles iniciales: altos en R1, R2, R4, R5 y R6, y medio en R3. Aunque mejorase la seguridad, seguiría siendo necesario justificar legalmente el uso de la biometría.

La opción recomendada es **descartar el reconocimiento facial actual y comprobar una alternativa con tarjeta, PIN y permisos por función**. Con ello se evitarían los riesgos propios de captar datos faciales, aunque el nuevo sistema también necesitaría controles y pruebas.

Consulta a los trabajadores (art. 35.9 RGPD). No consta en el expediente una consulta a los trabajadores o sus representantes. Dado que recomendamos no seguir con el tratamiento biométrico, no se propone realizar una consulta para justificar su puesta en marcha. Si Dirección reconsidera el proyecto, deberá valorar y documentar esa consulta cuando proceda.

2.5. Dictamen del DPO y conclusión: ¿requiere consulta previa?

Dictamen propuesto: desfavorable. Se recomienda no implantar el reconocimiento facial.

El hospital necesita controlar los accesos a sus zonas asistenciales, pero no ha demostrado que deba utilizar datos biométricos para hacerlo. Tampoco ha acreditado una base jurídica suficiente y las medidas de seguridad propuestas todavía no están verificadas.

Decisiones recomendadas a Dirección:

1. Detener la contratación del reconocimiento facial y no realizar pruebas con datos faciales del personal.
2. Pedir a Dirección Médica e IT que identifiquen los problemas reales de acceso a quirófanos y hospitalización.
3. Priorizar tarjetas individuales, PIN y permisos según el puesto, con una vía de entrada rápida para urgencias.
4. Comprobar el funcionamiento de la alternativa y documentar la retirada de permisos cuando cambien las funciones del personal.

¿Hay que consultar previamente a la AEPD?

No se recomienda utilizar la consulta previa para desbloquear el proyecto actual. Primero habría que demostrar que la biometría es necesaria y que su uso está permitido.

El **art. 36 RGPD** exige consultar a la AEPD antes de iniciar un tratamiento cuando, tras valorar las medidas posibles, permanece un riesgo alto que no puede reducirse suficientemente. Esta consulta no sustituye los requisitos legales del proyecto.

Aprobación y revisión. La recomendación deberá ser revisada por el DPO cuando se formalice su designación. Corresponde a Gerencia decidir sobre el proyecto y dejar constancia de su decisión. Si más adelante se plantea otra solución biométrica, habrá que revisar la EIPD antes de iniciar el tratamiento de datos personales.

Conclusión para Dirección: recomendamos reforzar los accesos a quirófanos y hospitalización con una alternativa no biométrica. Así se protege la actividad asistencial sin recoger datos faciales cuya necesidad no se ha demostrado.

3. Papel del DPO en la Evaluación de Impacto

La Evaluación de Impacto del reconocimiento facial es responsabilidad de PYME Sanitaria Mediterránea. El DPO asesora, revisa los riesgos y supervisa las medidas propuestas, pero no dirige la implantación ni decide si se aprueba el proyecto (arts. 35.2 y 39.1.c RGPD).

Para este proyecto, las responsabilidades se distribuyen así:

Responsable	Función
Gerencia	Aprueba o descarta el proyecto y facilita los recursos necesarios.

Responsable	Función
Dirección Médica e IT	Justifican las necesidades de acceso a quirófanos y hospitalización, estudian alternativas y aportan información técnica.
RR. HH. y asesoría jurídica	Analizan los efectos sobre los trabajadores y las condiciones legales del tratamiento.
DPO	Asesora durante la evaluación, revisa los riesgos para los trabajadores, emite su dictamen y supervisa que se atiendan sus recomendaciones.

Aplicación al hospital. Se recomienda no implantar el reconocimiento facial porque no se ha demostrado que sea necesario ni que tenga una base jurídica suficiente. Una vez designado, el DPO revisará esta recomendación. Gerencia deberá valorar sus conclusiones y dejar constancia de la decisión.

Si el hospital estudia otra solución que implique tratar datos personales, el DPO deberá participar desde el inicio. Si resulta necesaria una consulta previa a la AEPD, actuará como punto de contacto, conforme a los artículos 36 y 39.1.e del RGPD.

4. Relación entre los riesgos de seguridad y la protección de datos

El análisis de seguridad del Centro 1 identificó riesgos relacionados con el robo de credenciales (R10) y la asignación incorrecta de permisos (R11). Para reducirlos se propusieron medidas como la autenticación reforzada, la revisión periódica de accesos y la retirada de permisos cuando cambian las funciones del personal.

Estas medidas protegen los sistemas clínicos, pero el proyecto de reconocimiento facial exige valorar también sus consecuencias para los trabajadores.

Por ejemplo, un sistema biométrico podría impedir que una persona no autorizada accediera a quirófanos. Sin embargo, aunque funcionara correctamente y no sufriera ningún incidente de seguridad, seguiría afectando a la privacidad del personal si recogiera características faciales sin una necesidad justificada.

Esta es la diferencia fundamental: **el análisis de seguridad estudia los posibles daños a los sistemas y a la actividad del hospital; la EIPD estudia los posibles daños a los derechos y libertades de las personas**.

Para Dirección, ambas evaluaciones son necesarias y se complementan: una medida puede mejorar la seguridad del hospital y, al mismo tiempo, resultar excesiva para sus trabajadores. Por eso, la elección del sistema de acceso debe considerar tanto su eficacia como su impacto sobre la privacidad.

5. Propuesta de servicio de DPO externo

Cliente: PYME Sanitaria Mediterránea · Valencia
Servicio propuesto: Delegado de Protección de Datos (DPO) externo
Duración inicial: 12 meses
Honorarios: 1.800 € mensuales más IVA

Objeto de la propuesta

Se propone contratar un DPO externo especializado en el sector sanitario para asesorar a Dirección, supervisar el cumplimiento de la normativa de protección de datos y actuar como punto de contacto con la Agencia Española de Protección de Datos (AEPD).

El hospital trata información sanitaria de aproximadamente 85.000 pacientes al año y cuenta con 220 trabajadores. Su actividad exige un control permanente de la protección de datos y la designación de un DPO, conforme a los artículos 37.1.c del RGPD y 34.1.l de la LOPDGDD.

La documentación revisada muestra asuntos que requieren atención: no consta un nombramiento formal de DPO, existen solicitudes de derechos cuya gestión debe comprobarse y hay información pendiente de completar en el Registro de Actividades de Tratamiento (RAT). Además, el proyecto de reconocimiento facial se planteó sin una evaluación previa de su impacto sobre los trabajadores.

Alcance del servicio

Servicio	Actuaciones previstas
Asesoramiento y supervisión	Resolver consultas de Dirección y los departamentos; revisar el RAT, las políticas y el cumplimiento del RGPD y la LOPDGDD.
Derechos de las personas	Supervisar la atención de solicitudes de pacientes y trabajadores, incluidos exempleados, y comprobar sus plazos de respuesta.
Evaluaciones de impacto	Asesorar y supervisar las EIPD antes de aprobar tratamientos de alto riesgo y emitir recomendaciones por escrito.
Proveedores	Revisar las garantías y los contratos de protección de datos de proveedores de sistemas clínicos, laboratorio y gestión de citas.
Brechas de seguridad	Asesorar sobre la evaluación y notificación de incidentes, supervisar las medidas correctoras y cooperar con la AEPD.
Formación y seguimiento	Impartir dos sesiones anuales, revisar el cumplimiento y presentar informes periódicos a Gerencia.

Estas actuaciones cubren las funciones del artículo 39 del RGPD. El DPO supervisará y asesorará; la responsabilidad de implantar las medidas y decidir sobre los tratamientos seguirá correspondiendo al hospital.

Modelo de prestación

Se propone una dedicación ordinaria de **24 horas mensuales**, con atención principalmente remota, una visita presencial trimestral al Centro 1 y reuniones de seguimiento con los responsables de las áreas implicadas.

- **Consultas ordinarias:** respuesta inicial en un máximo de dos días laborables.
- **Incidentes urgentes:** canal de aviso disponible las 24 horas, con respuesta inicial en un máximo de dos horas desde su recepción.

- **Seguimiento:** reunión mensual e informe trimestral a Gerencia con incidencias, medidas pendientes, responsables y plazos.

Durante el primer mes se comprobará la situación del DPO, se revisarán los datos pendientes del RAT, la solicitud del exempleado y los procedimientos de respuesta a brechas. En los meses siguientes se revisarán los contratos con proveedores, las evaluaciones de impacto y los procedimientos de derechos. También se impartirán las dos sesiones de formación previstas. Cada trimestre, Gerencia recibirá un informe sobre las tareas realizadas, los asuntos pendientes y sus responsables.

Honorarios y justificación

Se propone una cuota de **1.800 € mensuales más IVA**, equivalente a **21.600 € anuales sin IVA**.

El importe se calcula sobre una dedicación estimada de 24 horas al mes y un coste medio de 75 €/hora. Incluye consultas, revisión documental, reuniones, informes y disponibilidad para la atención inicial de incidentes urgentes.

La dedicación responde al volumen y la sensibilidad de los datos tratados por el hospital, la actividad de sus sistemas clínicos, los proveedores que intervienen y la necesidad de supervisar tanto tratamientos existentes como nuevos proyectos.

El presupuesto se revisará al finalizar el tercer mes, comparando las horas utilizadas, las consultas recibidas y los asuntos pendientes. Cualquier ampliación deberá contar con aprobación de Dirección.

No se incluyen investigaciones forenses, implantaciones técnicas, auditorías extraordinarias ni representación jurídica en procedimientos sancionadores. Estos servicios requerirán un presupuesto independiente.

Condiciones principales del contrato

El contrato de prestación de servicios recogerá:

1. **Objeto y funciones:** designación del DPO, servicios incluidos, dedicación, tiempos de respuesta y entregables.
2. **Independencia:** acceso directo a Gerencia, recursos suficientes y libertad para emitir recomendaciones sin instrucciones sobre su criterio, conforme al artículo 38 del RGPD.
3. **Confidencialidad:** protección de la información sanitaria, laboral y empresarial conocida durante el servicio.
4. **Responsabilidades:** el hospital conserva las decisiones y la implantación de medidas; el DPO asesora, supervisa y documenta sus recomendaciones.
5. **Relación con la AEPD:** identificación del DPO como punto de contacto y procedimiento de colaboración ante requerimientos o consultas.
6. **Duración y condiciones económicas:** contrato inicial de doce meses, cuota mensual, servicios adicionales, renovación, preaviso de 30 días y causas de resolución.

Antes de contratar se comprobará la experiencia del profesional en protección de datos sanitarios, que pueda atender las necesidades del hospital y que no tenga conflictos de intereses. También se revisarán las garantías profesionales que ofrezca, incluida, en su caso, la cobertura de su seguro de responsabilidad civil.

Decisión solicitada a Dirección

Se recomienda aprobar la contratación de un DPO externo especializado en sanidad, con un presupuesto anual de **21.600 € más IVA**, sujeto a la validación del alcance y de las condiciones contractuales.

Una vez designado, el hospital deberá comunicar el nombramiento a la AEPD dentro de los diez días previstos en el artículo 34.3 de la LOPDGDD y facilitar al DPO acceso directo a Gerencia y a la información necesaria para ejercer sus funciones.

6. Comunicación con la AEPD

El Delegado de Protección de Datos (DPO) será el punto de contacto del hospital con la Agencia Española de Protección de Datos (AEPD), conforme al artículo 39.1.e del RGPD.

Ante una inspección o requerimiento, el DPO coordinará la respuesta con Gerencia, IT, RR. HH. y los responsables asistenciales. El hospital deberá facilitar la documentación solicitada, explicar las medidas aplicadas y responder dentro del plazo indicado por la AEPD.

Para ello, deberán mantenerse actualizados y accesibles el Registro de Actividades de Tratamiento (art. 30 RGPD), las evaluaciones de impacto, los contratos con proveedores que actúen como encargados (art. 28), los registros de solicitudes de derechos y la documentación de brechas de seguridad.

Plazos y actuaciones clave:

- **Brechas de datos personales:** notificación a la AEPD en un máximo de 72 horas desde que el hospital tenga conocimiento, salvo que sea improbable que exista riesgo para las personas (art. 33 RGPD). Si existe alto riesgo, también deberá informarse a los afectados sin dilación indebida (art. 34).
- **Solicitudes de derechos:** respuesta en un mes, con posibilidad de ampliación en los supuestos previstos por el artículo 12.3 RGPD.
- **Consulta previa:** si una futura evaluación identifica un riesgo alto que no puede reducirse suficientemente, el hospital deberá consultar a la AEPD antes de iniciar el tratamiento (art. 36 RGPD).

En el caso del reconocimiento facial, **no se recomienda iniciar una consulta previa para justificar su implantación**, ya que primero debe acreditarse que el tratamiento es necesario y legal.

Recomendación a Dirección: formalizar el nombramiento del DPO, establecer un canal único para las comunicaciones con la AEPD y garantizar que cada área aporte sus registros y evidencias cuando se soliciten. La responsabilidad de cumplir y responder ante la autoridad sigue correspondiendo al hospital.

Bibliografía y referencias normativas

- Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD)*. Artículos 5, 6, 9, 12, 28, 30, 33–39. https://eur-lex.europa.eu/eli/reg/2016/679/oj

- Jefatura del Estado. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)*. Artículo 34. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673
- Agencia Española de Protección de Datos. (2023). *Guía sobre tratamientos de control de presencia mediante sistemas biométricos.* https://www.aepd.es/documento/guia-control-presencia-biometrico-nov-2023.pdf
- Agencia Española de Protección de Datos. (s. f.). Realización de evaluaciones de impacto de protección de datos. https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/realizacion-de-evaluaciones-de

- Agencia Española de Protección de Datos. (2021). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. https://www.aepd.es/documento/guia-evaluaciones-de-impacto-rgpd.pdf
- Grupo de Trabajo del Artículo 29. (2017). Directrices sobre los delegados de protección de datos (WP243 rev.01). https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf