# Guía práctica de cumplimiento RGPD/LOPDGDD

## Gabinete de medicina estética, responsable persona física (Andalucía)

> Documento de trabajo interno. No es la cláusula que entregas al paciente ni el RAT que enseñas a la AEPD: es tu mapa para montar el cumplimiento y no dejarte nada. Fecha de referencia: julio 2026. Marco: RGPD (Reglamento UE 2016/679), LOPDGDD (LO 3/2018), Ley 41/2002 de autonomía del paciente.

---

## 1. Lo primero que tienes que entender: dos capas, no una

Los datos de salud son **categoría especial** (art. 9.1 RGPD). Su tratamiento está **prohibido** salvo excepción del art. 9.2. Para tratarlos con licitud necesitas **dos bases a la vez**, no una:

1. Una base de licitud general del **art. 6**.
2. Una excepción que levante la prohibición del **art. 9.2**.

Aquí es donde casi todo el mundo se equivoca: cree que la base para tratar la historia clínica es el consentimiento del paciente. **No lo es.**

**Tu combinación correcta para la asistencia sanitaria es:**

- **Art. 6.1.b RGPD**, ejecución del contrato de prestación del servicio médico del que el paciente es parte.
- **Art. 9.2.h RGPD**, tratamiento necesario para diagnóstico médico, prestación de asistencia o tratamiento sanitario, realizado por un profesional sujeto a **obligación de secreto** (art. 9.3). Este es el encaje nuclear de la historia clínica.
- **Refuerzo en Derecho español:** art. 9.2 LOPDGDD (permite tratar datos de salud cuando lo ampara una ley) y **Disposición Adicional 17ª LOPDGDD** (tratamientos amparados en la Ley 41/2002 y demás legislación sanitaria).

**Por qué esto importa en la práctica:** si basaras la asistencia en el consentimiento, el paciente podría retirarlo y dejarte sin base para conservar su historia clínica, que la ley te obliga a guardar. Por eso la AEPD es explícita: **no necesitas el consentimiento del paciente para recoger y tratar sus datos con fines asistenciales**. La base es 6.1.b + 9.2.h.

### Dónde SÍ necesitas consentimiento explícito (art. 9.2.a)

El consentimiento vuelve a ser la base, pero solo para lo que **no es asistencia**:

- Publicar fotos en redes, web, publicidad, “antes y después”, testimonios.
- Enviar comunicaciones comerciales.
- Uso de imágenes con fines docentes o científicos.
- Cesiones a terceros no amparadas por ley.

Ahí el consentimiento debe ser **libre, específico, informado, inequívoco, explícito y revocable**. Y separado por finalidad (lo desarrollas en el documento 04).

### Tres cosas que no puedes confundir

- **Consentimiento informado clínico ≠ consentimiento RGPD.** El consentimiento informado de la Ley 41/2002 (aceptar el acto médico y sus riesgos) es una figura distinta del consentimiento de protección de datos. No los fusiones en un mismo papel ni pretendas que uno sustituya al otro.
- **El papel que firma el paciente al darse de alta como paciente no es un "consentimiento de datos".** Es una **cláusula informativa** (deber de información del art. 13 RGPD). Documento 03.
- **Consentir una foto "con fin médico" no habilita a publicarla.** Son finalidades distintas y bases distintas. Documento 04.

---

## 2. Historia clínica: contenido, conservación y custodia (Ley 41/2002)

### Qué tiene que contener (art. 15)

La HC incorpora toda la información trascendental para conocer de forma veraz y actualizada el estado de salud. En tu consulta ambulatoria, como mínimo:

- Identificación del paciente y del profesional.
- Anamnesis y exploración física.
- Antecedentes, alergias, medicación habitual.
- Evolución y hojas de seguimiento de cada proceso.
- Órdenes y hoja de tratamiento: **producto, lote, dosis y zona** en toxina/relleno (dato crítico ante reclamación o farmacovigilancia).
- Consentimientos informados de cada procedimiento (arts. 8-10).
- Informes de pruebas complementarias si las hubiera.
- Fotografías clínicas con finalidad asistencial (forman parte de la HC).
- Informe o evolutivo de alta de cada proceso.

La HC debe ser **única por paciente** dentro del centro (art. 15.4) e integrar todos sus procesos. Nada de una carpeta por tratamiento sin conexión entre ellas.

### Cuánto tiempo la conservas (art. 17), este es tu plazo real

- **Mínimo estatal: 5 años** desde la fecha del alta **de cada proceso asistencial**. Ojo: se cuenta desde el cierre de cada proceso, no desde la última visita global del paciente.
- **Andalucía no fija plazo propio.** No hay normativa autonómica andaluza de conservación de HC, así que **aplica el mínimo estatal de 5 años**. (Contraste: Cataluña 15/20 años, Navarra 20; a ti no te aplican.)

- **Excepciones que te obligan a guardar más allá de 5 años (art. 17.2):** razones judiciales (mientras exista o pueda existir reclamación), epidemiológicas, de investigación o de organización del SNS.
- **Criterio recomendado para estética:** la litigiosidad por resultados es alta. Conserva la HC **más allá del mínimo**, orientándote por el plazo de prescripción de posibles acciones de responsabilidad, y **justifica ese plazo ampliado en el RAT**. Fija tu plazo, escríbelo y cúmplelo.
- **Tienes que informar del plazo al paciente** (art. 13.2.a RGPD) y hacerlo **constar en el RAT** (art. 30.1.f). No informarlo es de los incumplimientos más habituales.

### Derechos del paciente sobre su HC (arts. 18 y 19)

- **Acceso** a su documentación y a obtener copia (art. 18.1), coordinado con el derecho de acceso RGPD (art. 15).
- **Límites:** no perjudica la confidencialidad de terceros y **no ampara el acceso a tus anotaciones subjetivas** (art. 18.3), que puedes reservar.
- **Pacientes fallecidos** (art. 18.4): acceso por personas vinculadas salvo prohibición del fallecido, nunca en perjuicio de terceros ni de las anotaciones subjetivas.
- Además, aplican rectificación, supresión (limitada por tu obligación de conservación clínica), oposición, portabilidad y limitación.

### Custodia (art. 19 Ley 41/2002 + art. 32 RGPD)

Tú, como centro, respondes de la gestión y custodia de las HC y garantizas su conservación, seguridad y confidencialidad. Deber de custodia y de secreto reforzado.

---

## 3. RAT: obligatorio siempre, sin excepción posible (art. 30 RGPD)

La exención del art. 30.5 (menos de 250 empleados) **no te sirve**: decae en cuanto tratas categorías especiales de datos, y tú tratas salud. Por tanto **el RAT es obligatorio siempre**, seas persona física con una sola sede o no.

Cada actividad de tratamiento debe recoger (art. 30.1): responsable y contacto; fines; categorías de interesados y de datos; categorías de destinatarios; transferencias internacionales; plazos de conservación; descripción general de las medidas de seguridad.

Formato libre (Word/Excel). Documento **interno**, a disposición de la AEPD si lo requiere. La plantilla ya montada con tus actividades (Pacientes/Asistencia, Facturación, Marketing y RRSS, Videovigilancia) está en el documento 02. Puedes generar un RAT base con la herramienta **FACILITA RGPD** de la AEPD.

---

## 4. EIPD: no es automática para ti, pero el análisis de riesgos sí (art. 35)

**Regla:** para una consulta estética individual de escala reducida, la EIPD (evaluación de impacto) **no es obligatoria de forma automática**. Sí lo es si el tratamiento alcanza "gran escala" o cumple **≥2 criterios de riesgo** de la lista de la AEPD.

- La "gran escala" se valora por número de interesados, volumen y variedad de datos, duración y extensión geográfica. Una consulta individual con un número limitado de pacientes **no es gran escala**, la propia AEPD pone como ejemplo al médico o dentista que no trata datos de forma masiva.
- **Cuándo SÍ se te dispararía la EIPD:** volumen alto de pacientes o varias sedes; biometría (reconocimiento facial); IA o perfilado de pacientes; app de telemedicina; almacenamiento masivo de historiales en la nube combinado con otras fuentes.

**Lo que sí debes hacer siempre, aunque no toque EIPD:** un **análisis de riesgos** proporcionado (arts. 24 y 32). Déjalo por escrito aunque la conclusión sea que no hace falta EIPD. Mínimo:

1. Inventario de tratamientos y flujos: quién accede, dónde se almacena, quién es encargado.
2. Amenazas: acceso indebido, pérdida, envío erróneo, exfiltración.
3. Valoración probabilidad × impacto sobre los derechos del paciente.
4. Medidas de mitigación (cifrado, control de acceso, copias, contratos de encargado) y riesgo residual.
5. Documentar y revisar periódicamente.

Metodología: Guía AEPD "Gestión del riesgo y evaluación de impacto" (`02D_Guia_gestion_riesgo_y_EIPD.pdf`).

---

## 5. DPD: probablemente NO, a revisar si contratas enfermería (art. 37 RGPD / art. 34 LOPDGDD)

**Regla general (art. 34.1.o LOPDGDD):** los centros sanitarios obligados a mantener historias clínicas deben nombrar DPD. **Pero hay una excepción expresa:** se exceptúan los profesionales de la salud que, aun estando obligados al mantenimiento de las HC, **ejerzan su actividad a título individual**.

**Tu caso, punto por punto:**

- Ejerces a título individual, sin apenas estructura → **DPD no obligatorio**.
- **Una auxiliar administrativa en recepción no dispara la obligación.**
- **Cuidado aquí:** si contratas **personal sanitario auxiliar** (típicamente **una enfermera/DUE** que asiste a pacientes) puede discutirse que dejes de ejercer "a título individual" a estos efectos y que, con ello, **decaiga la excepción y el DPD pase a ser obligatorio**. El encaje exacto de la excepción del **art. 34.1.o LOPDGDD** no

es unívoco: **conviene confirmarlo con un especialista o con la AEPD** antes de darlo por cerrado. Es el punto que más se pasa por alto al crecer.

- Si designas DPD (obligatorio o voluntario), tienes que **comunicarlo a la AEPD en 10 días** (art. 34.3 LOPDGDD) y publicar sus datos de contacto.

**Recomendación operativa:** decide la plantilla antes de contratar. Si va a haber enfermería, lo prudente es **presupuestar y valorar** desde ya la designación de un **DPD externo** (y confirmar el encaje de la excepción del art. 34.1.o con un especialista o la AEPD) , en vez de dejarlo para después.

---

## 6. Seguridad y deber de secreto (art. 32 RGPD + art. 5 LOPDGDD)

Datos de salud = alto riesgo → medidas reforzadas. El RGPD no da catálogo cerrado; la referencia técnica útil es el **Esquema Nacional de Seguridad (ENS, RD 311/2022)**, obligatorio en el sector público, pero excelente marco para el privado sanitario.

**Medidas que debes tener montadas:**

- **Cifrado** de datos de salud en reposo (disco, base de datos) y en tránsito. Para un centro sanitario la AEPD lo considera prácticamente obligatorio. **Nunca datos de salud en claro en portátiles o móviles.**
- **Control de acceso individualizado:** usuario y contraseña robusta **+ doble factor (2FA/MFA)** en correo, software de gestión y accesos cloud. Acceso por necesidad (need-to-know).
- **Registro de accesos (logs) y trazabilidad:** quién entra a qué HC y cuándo, con alertas ante accesos anómalos. Esto mitiga la brecha más típica del sector: el acceso indebido del propio personal.
- **Copias de seguridad** automáticas, cifradas y **con restauración probada** (hacer backup no basta; hay que verificar que restaura). Regla 3-2-1.
- **Seudonimización y minimización** donde puedas; separa datos identificativos de datos clínicos en los usos secundarios.
- **Soportes y papel:** destrucción segura, borrado seguro de dispositivos, política de puesto de trabajo (pantalla bloqueada, mesa limpia).
- **Actualizaciones, antivirus, firewall** y plan de continuidad.

**Deber de secreto (reforzado):**

- **Art. 5 LOPDGDD:** deber de confidencialidad, complementario al secreto profesional, que **subsiste aun terminada la relación** con el paciente o con el empleado.
- **Art. 9.3 RGPD + art. 16.6 Ley 41/2002:** todo el que accede a datos de salud queda sujeto al deber de secreto.
- **Todo el personal** (sanitario y administrativo, y en su caso becarios o subcontratados) debe firmar un **compromiso de confidencialidad por escrito** (documento 06) y

recibir formación. Violar el secreto puede ser infracción RGPD **y delito** (art. 199 Código Penal).

## 7. Encargados de tratamiento: contrato con todo el que toque datos por ti (art. 28)

Firma **contrato de encargado (art. 28.3)** con **todo tercero que acceda o trate datos de pacientes por tu cuenta**. Sin ese contrato, cada acceso o cesión es una **comunicación ilícita**. La plantilla reutilizable está en el documento 05.

**Con quién firmar:**

| Proveedor | ¿Encargado? | Nota |
|---|---|---|
| Software de HC / gestión de citas en la nube | **Sí (crítico)** | Aloja datos de salud. Verifica ubicación de servidores (EEE) y transferencias internacionales; exige cifrado y medidas del art. 32. |
| Hosting web / correo profesional | Sí, si accede a datos | Sobre todo si el formulario web recoge datos de pacientes. |
| Gestoría / asesoría fiscal-laboral | **Sí** | Trata facturación de pacientes y datos de empleados. |
| Laboratorio de análisis / anatomía patológica | **Matizado** | Por tu cuenta → encargado. Con fines propios → responsable independiente. Analízalo caso a caso. |
| Empresa de destrucción documental | **Sí** | Destrucción certificada de HC en papel o soportes. |
| Agencia de marketing / community manager / plataforma de email | **Sí** | Si gestiona datos de pacientes o publica sus imágenes. |
| Mantenimiento informático con acceso a sistemas | Sí | Acceso potencial a datos de salud. |
| Pasarela de pago / TPV | Normalmente responsable propio | Verifícalo según el servicio. |

**Requisitos mínimos del contrato (art. 28.3):** objeto, duración, naturaleza y finalidad; tipo de datos y categorías de interesados; confidencialidad; tratar solo según tus instrucciones; medidas de seguridad; régimen de **subencargados** (autorización previa); asistencia en derechos y brechas; **devolución o supresión** al finalizar; sometimiento a auditoría.

## 8. Fotografías: separa siempre finalidad asistencial de promocional

**Dos regímenes distintos, no los mezcles nunca:**

1. **Foto clínica con fin asistencial o documental** (seguimiento, evolución): es **documentación asistencial** y **forma parte de la HC**, base **art. 6.1.b + 9.2.h**. **No se pide autorización para poder tratar al paciente: se le informa.** No es opcional ni revocable como si fuera marketing (la HC hay que conservarla) , y lleva medidas reforzadas.
2. **Redes, web, publicidad, "antes y después", testimonios, docencia:** no lo cubre la asistencia. Necesitas **consentimiento explícito, específico, informado, separado y por escrito** (art. 9.2.a) **+** consentimiento por derecho a la propia imagen (**LO 1/1982**). Debe decir: finalidad concreta (qué red o soporte), alcance, duración, revocabilidad y si se anonimiza o no.

**Reglas aprendidas de sanciones reales:**

- **Granularidad por finalidad:** consentir fotos "con fines médicos" **no** habilita a publicarlas. Hay precedente AEPD de sanción a clínica estética por "antes y después" en redes sin consentimiento específico (arts. 6 y 9 RGPD).
- **Revocabilidad real:** si el paciente revoca, retira las imágenes.
- **Anonimización insuficiente:** recortar la cara puede no anonimizar (tatuajes, marcas, contexto). Si es identificable, sigue siendo dato personal.
- **El consentimiento no puede ser condición** para recibir el tratamiento.
- **Menores:** consentimiento de los titulares de la patria potestad.
- Conserva **prueba** del consentimiento y de su versión informada.

Publicar imágenes sin consentimiento específico es de lo más sancionado del sector, con daño reputacional añadido.

---

## 9. Brechas de seguridad: el reloj de 72 horas (arts. 33 y 34)

- **Notificación a la AEPD (art. 33): 72 horas máximo** desde que **tienes constancia** de la brecha (cuentan fines de semana y festivos). Solo te libras si es **improbable** que suponga riesgo para derechos y libertades. Si te pasas del plazo, tienes que justificar la demora.
- **Comunicación al paciente afectado (art. 34):** cuando sea **probable un alto riesgo** para sus derechos (exponer datos de salud lo es), comunícaselo sin dilación y en lenguaje claro. Excepciones (art. 34.3): datos cifrados/ininteligibles, medidas posteriores que eliminan el alto riesgo, o esfuerzo desproporcionado (→ comunicación pública).
- **Registro interno de brechas (art. 33.5):** documenta **toda** brecha aunque no la notifiques (hechos, efectos, medidas). La AEPD lo exige en inspección.

- **Contenido de la notificación:** naturaleza; categorías y número aproximado de afectados y de registros; contacto del DPD o punto de contacto; consecuencias probables; medidas adoptadas y propuestas.
- Brechas típicas en salud: **acceso indebido del propio personal** a HC, **envío a destinatario erróneo** (email/WhatsApp), destrucción incorrecta de papel, pérdida de dispositivos.

Herramientas AEPD: guía de brechas (`02D_Guia_notificacion_brechas_seguridad.pdf`), notificación por la sede electrónica y "Asesora Brecha" para decidir si notificar.

---

## 10. Checklist de cumplimiento del día 0

Antes de ver al primer paciente, ten esto en marcha:

**Documentación base** - [ ] RAT redactado con las 4 actividades (documento 02) y plazo de conservación de HC decidido y escrito. - [ ] Cláusula informativa del art. 13 lista para consulta y web, capa 1 + capa 2 (documento 03). - [ ] Formularios de consentimiento explícito para marketing e imagen, separados y granulares (documento 04). - [ ] Análisis de riesgos por escrito (aunque concluya que no hace falta EIPD).

**Historia clínica** - [ ] Sistema que garantice HC única por paciente e integración de procesos. - [ ] Registro de producto, lote, dosis y zona en cada procedimiento. - [ ] Plazo de conservación configurado (≥5 años desde el alta de cada proceso, ampliado por litigiosidad).

**Seguridad** - [ ] Cifrado en reposo y en tránsito activado; nada de salud en claro en portátiles/móviles. - [ ] 2FA en correo, software de gestión y accesos cloud. - [ ] Logs de acceso a HC activados. - [ ] Copias de seguridad automáticas, cifradas y con **restauración probada**. - [ ] Política de puesto: bloqueo de pantalla, mesa limpia, destrucción segura de papel.

**Terceros y personal** - [ ] Contrato de encargado (art. 28) firmado con software de HC, gestoría, hosting/correo, destrucción documental, marketing e IT (documento 05). - [ ] Ubicación de servidores del software cloud verificada (EEE / transferencias internacionales). - [ ] Compromiso de confidencialidad firmado por todo el personal (documento 06).

**Estructura y decisiones** - [ ] Decidido si habrá enfermería/DUE → si sí, **valorar la designación de DPD** (confirmar el encaje del art. 34.1.o con especialista/AEPD) y, en su caso, comunicarlo a la AEPD en 10 días. - [ ] Procedimiento de brechas definido: quién detecta, quién decide, plazo de 72 h, registro interno. - [ ] Procedimiento de ejercicio de derechos (acceso, copia de HC, rectificación, etc.) definido.

---

### Documentos oficiales AEPD descargados (referencia)

En `H:\IA-projects\U48 Andalucia\09_Formularios_Oficiales\` (prefijo `02D_`):

| Archivo | Uso |
|---|---|
| 02D_Guia_profesionales_sector_sanitario.pdf | Marco sectorial completo. |
| 02D_Guia_deber_informar_clausula_informativa.pdf | Base del documento 03. |
| 02D_Modelo_clausula_informativa_clientes.docx | Modelo AEPD de cláusula. |
| 02D_Guia_gestion_riesgo_y_EIPD.pdf | Metodología del análisis de riesgos (§4). |
| 02D_Lista_tratamientos_requieren_EIPD_art35-4.pdf | Criterios que disparan EIPD. |
| 02D_Guia_notificacion_brechas_seguridad.pdf | Procedimiento de brechas (§9). |
| 02D_Guia_proteccion_datos_por_defecto.pdf | Privacidad desde el diseño y por defecto. |
| 02D_Formulario_derecho_acceso.pdf | Modelo para ejercicio de derechos. |

**Herramientas online AEPD:** FACILITA RGPD (RAT y cláusulas para bajo riesgo), Gestiona RGPD (riesgo más alto), Asesora Brecha (decisión de notificar).