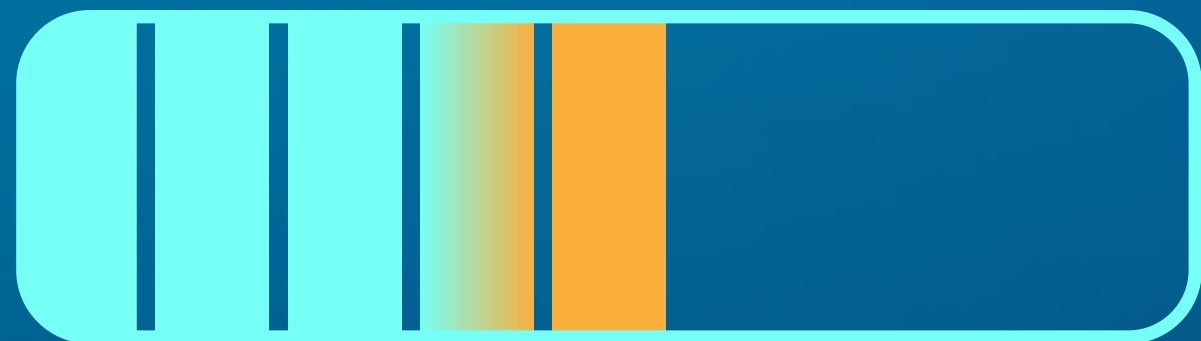


Tu negocio está protegido **en parte**

Estás obligado por ley, y mañana
puede costarte caro.



**Estás en una posición sólida,
pero aún quedas expuesto
a multas de hasta 30.000€ ↘**

Eso demuestra compromiso, responsabilidad y una visión de futuro. Pero ojo: un buen cumplimiento no significa cumplimiento total. Aún puedes estar dejando grietas abiertas que, con una inspección o una reclamación, podrían escalar y convertirse en sanciones innecesarias.

La protección de datos no es una foto estática: es un vídeo en movimiento. La nueva normativa exige ser proactivo por tu parte. Puede que no trates datos sensibles ahora.

Pero, ¿y si mañana sí?

Has realizado una evaluación RGPD y los resultados muestran **que ya tienes implementadas muchas medidas clave.**

- Sanciones por omisiones puntuales (entre 600 y 30.000 €).
- Requerimientos de la AEPD que te obliguen a actuar contrarreloj.
- Desconfianza por parte de clientes o proveedores si detectan fallos.
- Riesgos reputacionales si no puedes demostrar que cumples al 100%

¿A qué te estás exponiendo?

Casos reales: esto ya le ha pasado a otros.



Clínica estética

3.000 € por enviar comunicaciones sin consentimiento.

Academia online

Requerimiento de la AEPD por no responder a tiempo una solicitud de supresión.

Estudio de arquitectura

1.200 € por no firmar contrato con el proveedor de hosting..

Tienda local

2.000 € cámara de videovigilancia sin cartel informativo.

Consulta privada

900 € por no actualizar la política de privacidad tras un cambio de actividad.

Tu puntuación indica que vas por el buen camino, pero... ➤

Aún hay detalles que pueden marcar la diferencia entre una empresa que “casi cumple” y otra que puede dormir tranquila.

Revisando tu evaluación, vemos que quedan algunas medidas clave por cerrar:

Faltan pequeños ajustes en documentación o textos legales.

No todos los procesos están documentados ni revisados.

Puede que tu equipo no tenga formación actualizada.

Hay contratos, protocolos o registros que no están al día.

1. Documentación y bases legales de cumplimiento

- Documento de seguridad adaptado.
- Registro de actividades completo y revisado.
- Política de privacidad y cookies actualizadas según tu actividad.
- Aviso legal completo en web y comunicaciones.
- Contratos con proveedores de datos firmados y archivados.

¿Qué vas a solucionar con esto?

- ✓ Tendrás todo en regla para demostrar que tratas los datos de forma legal y transparente ante cualquier inspección
- ✓ Evitarás errores y sanciones por 'detalles técnicos'.
- ✓ Refuerzas la confianza de tus clientes y proveedores

¿Qué vas a evitar?

- ✗ Multas menores de hasta 3.000 € por errores fácilmente evitables.
- ✗ Problemas en convocatorias públicas o con clientes exigentes.
- ✗ Inspecciones en las que no puedes justificar nada por escrito.

2. Protocolos y procedimientos activo

- Procedimiento documentado de respuesta a solicitudes ARSULIPO
- Plan de actuación ante incidentes de seguridad.
- Control y seguimiento del acceso a los datos.

- ✓ Reaccionar con rapidez y eficacia si alguien te pide sus datos, quiere borrarlos o reclama.
- ✓ Estás preparado si hay una filtración, error o pérdida de información.
- ✓ Controlas qué personas tienen acceso a qué datos, dentro y fuera de tu empresa.

- ✗ Requerimientos por no atender correctamente los derechos.
- ✗ Reclamaciones por incumplir plazos legales o no tener canales habilitados.
- ✗ Riesgos de fuga de información por accesos no controlados.

3. Obligaciones internas con tu equipo

- Formación básica en RGPD (obligatoria).
- Compromisos de confidencialidad firmados.
- Procedimientos internos claros.
- Supervisión periódica del cumplimiento.

- ✓ Todos en tu equipo sabrán cómo actuar y qué está permitido.
- ✓ Reduces los errores humanos, que son la causa más común de sanción.
- ✓ Demuestras que hay un compromiso real con la protección de datos en tu negocio.

- ✗ Multas de hasta 30.000 € por falta de formación o acuerdos de confidencialidad.
- ✗ Sanciones por filtraciones accidentales o mal uso de los datos.
- ✗ Inseguridad ante auditorías o inspecciones.

¿Por qué es **urgente** **avanzar al siguiente nivel?**

Porque la diferencia entre estar
"medio bien" y "totalmente en orden"
puede costarte miles de euros.

Y porque no basta con haber
empezado: **el RGPD exige que puedas**
demostrarlo todo, por escrito y al día.

8

tips para evitar sanciones
(y que debes implementar
cuanto antes)



01. Informa siempre a clientes, proveedores y empleados

Toda persona cuyos datos recojas, trates o almacenes tiene derecho a saber con claridad quién los gestiona, con qué finalidad, qué derechos le asisten y cómo puede ejercerlos.

Esta información debe incluirse en cada formulario, contrato y comunicación, especialmente en los correos electrónicos, que deben incorporar un pie legal adaptado a la normativa vigente. **No cumplir con esta obligación básica supone una infracción directa del deber de transparencia exigido por el RGPD.**

02. Controla los accesos y firma contratos con terceros

Cada proveedor o colaborador externo que tenga acceso a los datos personales de tu empresa —como asesores, servicios informáticos, plataformas de software o gestorías— debe firmar un Contrato de Encargo del Tratamiento.

Este documento regula sus responsabilidades y garantiza que actúan conforme a la normativa. Además, internamente, debes limitar el acceso solo a aquellas personas que realmente necesitan tratar los datos para desempeñar sus funciones.

03. Establece protocolos para atender los derechos de las personas

Debes tener definidos y documentados los procedimientos para responder correctamente a las solicitudes de ejercicio de derechos: acceso, rectificación, supresión, oposición, limitación, portabilidad e información. Estas solicitudes deben ser gestionadas de forma estructurada, segura y dentro del plazo legal (normalmente 30 días).

Es esencial que tanto tú como tu equipo sepáis cómo proceder ante cualquier requerimiento de este tipo.

04. Detecta y comunica cualquier brecha de seguridad

Un incidente de seguridad puede ser tan sencillo como enviar un correo al destinatario equivocado o perder un dispositivo con datos. Si dicho incidente compromete los derechos de las personas, se considera una brecha de seguridad que debe ser notificada a la Agencia Española de Protección de Datos en un plazo máximo de 72 horas.

Por ello, es imprescindible contar con un protocolo interno de detección, valoración del impacto y notificación.

05. Forma a tu equipo y exige confidencialidad

Cada persona que forme parte de tu organización y tenga acceso a datos personales debe recibir formación básica sobre el RGPD. Además, debe firmar un compromiso de confidencialidad y estar preparada para actuar ante situaciones como brechas de seguridad, solicitudes de derechos o tratamiento indebido de datos.

La falta de formación es una de las principales causas de errores y sanciones en pequeñas y medianas empresas.

06. Informa correctamente si utilizas videovigilancia

Si tu negocio emplea sistemas de grabación mediante cámaras (ya sea en oficinas, zonas comunes o vehículos), debes informar de ello mediante cartelería visible y cláusulas informativas. También es necesario garantizar el uso responsable del sistema, limitar el acceso a las grabaciones y eliminar las imágenes dentro del plazo legal.

El uso de videovigilancia sin información adecuada es una causa frecuente de sanción por parte de la AEPD.

07. Revisa los textos legales de tu página web

Tu sitio web debe cumplir tanto con el RGPD como con la normativa de servicios de la sociedad de la información (LSSI CE). Esto implica tener un aviso legal actualizado, una política de privacidad adaptada a tu actividad, una política de cookies funcional con consentimiento válido y mecanismos de configuración, y cláusulas informativas visibles en todos los formularios.

Los errores en estas áreas son actualmente una de las principales fuentes de multas.

08. Mantén tu sistema de cumplimiento actualizado

El RGPD exige no solo implantar medidas, sino mantenerlas activas y actualizadas. Tu negocio evoluciona, y la normativa también. Por eso, al menos una vez al año, debes revisar toda la documentación, realizar un nuevo análisis de riesgos, comprobar que los procedimientos se siguen correctamente y elaborar un informe de cumplimiento.

Este enfoque continuo es el que te permitirá defender tu responsabilidad proactiva ante cualquier inspección o reclamación.

Póntelo Fácil: nosotros nos encargamos de que cumplas ↘

No necesitas volverte experto en protección de datos, pero sí asegurarte de que tu empresa cumple con todo lo obligatorio.

Aunque tu riesgo sea más bajo, las sanciones no lo son.

En ubimia[®] compliance llevamos más de 15 años ayudando a autónomos, pymes y negocios como el tuyo a adaptarse al RGPD de forma ágil, completa y sin dolores de cabeza. Analizamos tu caso, implantamos lo que necesitas, redactamos la documentación, formamos a tu equipo, y te defendemos si llega una inspección o una reclamación.

Con nuestro
acompañamiento:

Cumples con la ley,
sin agobios.

Evitas sanciones,
reclamaciones y susto.

Tienes tranquilidad
y respaldo legal
continuo.

Te centras en hacer
crecer tu negocio, no
en pelear con la
burocracia.

Solicita tu **consultoría gratuita** y empieza ya

Solo por haber hecho este test, **puedes solicitar ahora una sesión de consultoría de 30 minutos completamente gratuita** y sin compromiso, donde uno de nuestros especialistas evaluará tu situación y te dirá cómo ponerte al día de forma sencilla y eficaz.

 Tel. +34 911 01 34 96

 Agendar Cita

 compliance.ubimia.com

ubimia[®]
compliance

Más allá del cumplimiento. Competitividad global.