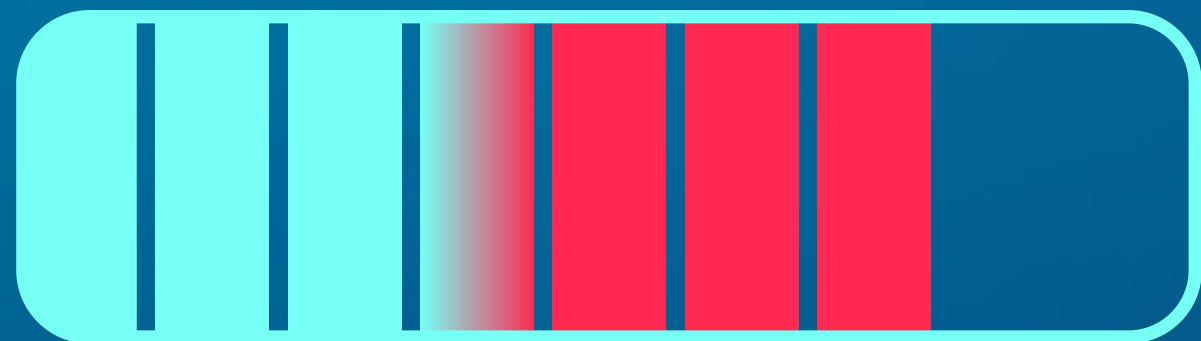


Tu negocio está en riesgo

Estás a medio camino,
pero no te salvas de sanciones



Estás en una zona de peligro:
lo que no has hecho
aún puede salirte caro. ↘

Has dado algunos pasos, sí, pero todavía tienes huecos importantes que dejan tu negocio expuesto a sanciones de hasta 60.000€, reclamaciones y pérdidas de confianza.

En Protección de Datos no vale el "casi". La normativa exige evidencias, protocolos y control continuo.

Tu evaluación de cumplimiento con el RGPD **muestra un nivel insuficiente y desequilibrado.**

- Multas desde 1.500 € hasta más de 60.000 €, incluso si eres autónomo o pyme.
- Reclamaciones de personas cuyos datos has tratado sin la información o base legal correcta.
- Inspecciones que pueden destapar documentación incompleta o mal aplicada.
- Pérdida de clientes o contratos por no demostrar el cumplimiento.
- Desconfianza interna si tu equipo no sabe cómo actuar ante un incidente

¿Qué riesgos sigues corriendo?

Casos reales: esto ya le ha pasado a otros.



Clínica veterinaria

9.000 € por no renovar contratos de tratamiento con proveedores.

Academia de formación

6.000 € por subir a la nube datos de alumnos sin medidas de seguridad ni base legal.

Asesoría Laboral

12.000 € por no poder acreditar formación del equipo.

E-commerce

7.000 € por mantener datos de clientes más tiempo del permitido.

Despacho de abogados

20.000 € por enviar emails con datos personales a destinatarios equivocados.

Estás mejor que muchos... pero eso no basta ↴

Tu puntuación indica que tienes algunas medidas en marcha, pero no están completas, actualizadas o bien ejecutadas.

Esto es lo que significa estar en riesgo medio: no estás en la casilla de salida, pero tampoco cerca de la meta.

Tu negocio todavía:

No tiene documentación completa ni actualizada.

No ha definido todos los protocolos exigidos por la ley.

No informa correctamente en todos los canales ni documentos.

No garantiza que todo el equipo esté formado y comprometido.

No controla de forma efectiva los accesos y cesiones de datos.

1. Documentación y bases legales de cumplimiento

- Registro de actividades de tratamiento (no vale el genérico).
- Política de privacidad y cookies bien configuradas en tu web.
- Aviso legal con datos del responsable.
- Cláusulas informativas en formularios, contratos y correos.
- Contratos de encargo del tratamiento con proveedores que gestionan datos.
- Análisis de riesgos adaptado a tu actividad.

¿Qué vas a solucionar con esto?

- ✓ Tendrás todo en regla para demostrar que tratas los datos de forma legal y transparente.
- ✓ Evitarás errores por desinformación o falta de documentación.
- ✓ Refuerzas la confianza de tus clientes y proveedores.

¿Qué vas a evitar?

- ✗ Sanciones de hasta 60.000€ por no informar correctamente.
- ✗ Problemas con proveedores que usan tus datos sin protección legal.
- ✗ Inspecciones en las que no puedes justificar nada por escrito.

2. Protocolos y procedimientos activo

- Un procedimiento claro para responder a derechos (acceso, rectificación, etc.).
- Un plan de actuación ante incidentes o brechas de seguridad.
- Controles de acceso a los datos (internos y externos).
- Mecanismos para acreditar el cumplimiento ante terceros.

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

- ✗ Sanciones de hasta 100.000 € por no atender derechos o gestionar mal una brecha de seguridad.
- ✗ 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 protección de datos (mínima y obligatoria).
- Compromisos de confidencialidad firmados.
- Instrucciones claras ante errores o incidencias.
- 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 errores internos que acaban filtrando o usando mal los datos.
- ✗ Riesgos legales por falta de control o seguimiento del cumplimiento.

¿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 ↘

Estás en el camino, pero necesitas apoyo para cerrar brechas. No se trata solo de evitar multas, sino de que tu negocio funcione con confianza y legalidad.

Pero también debes saber que no necesitas complicarte ni cargarte con todo.

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.