



CHECK LIST CUMPLIMIENTO NORMATIVO LOPDGDD



www.tusdatosasalvo.com

Patricia Gallego

Teléfono: 658.342.479

E-mail: patricia@tusdatosasalvo.es



Patricia Gallego Ferrari

Consultora de Protección de Datos

658 342 479

patricia@tusdatosasalvo.es

Imagina que puedes cumplir con la Protección de Datos de una manera sencilla, efectiva y sin que te quite mucho tiempo; aunque no sepas nada de leyes.

Hola!! Permíteme que me presente, me llamo Patricia Gallego y soy Consultora Experta en Protección de Datos, a lo que me dedico desde el 2009; y tras visitar cientos de empresas en estos años, he ido adaptando la norma a la realidad práctica de cada negocio.

Como emprendedores tenemos muchos frentes a los que atender y tenemos que estar pendientes de multitud de tareas, desde **TUS DATOS A SALVO** queremos ayudarte para que desarrolles un **Sistema de Recogida de Datos Global** y adaptado a tus necesidades que te dé la tranquilidad de estar haciéndolo bien, para que tú te puedas ocupar de la parte que más te gusta de tu negocio.

Queremos darte pautas prácticas, efectivas y adecuadas a tu empresa y a tu situación.

Beneficios de adecuar legalmente tu actividad:

¿Verdad que no te plantearías el abrir un negocio sin licencia de apertura? pues igual de importante es tener una web que capte clientes de manera legal. Estos son sólo algunos de los beneficios que vas a obtener al adecuar legalmente vuestra actividad:

1. Aseguras la continuidad de tu negocio evitando denuncias y sanciones; a la vez que obtienes una gran ventaja competitiva.
2. Mejoras tu reputación y la imagen que proyectáis, aumentando la confianza de tus clientes presentes y futuros.
3. Proteges el activo más valioso de tu empresa: vuestras bases de datos, convirtiendo tu negocio en confiable y recomendable.

Velar por la seguridad de los datos de tus clientes y/o trabajadores nunca ha sido tan sencillo.

www.tusdatosasalvo.com

Patricia Gallego

Teléfono:

658.342.479

E-mail: patricia@tusdatosasalvo.es

AUDITORIA INTERNA CUMPLIMIENTO NORMATIVO

1. CHECK LIST VERIFICACIÓN CUMPLIMIENTO

1. Deber de información

- Incluir las cláusulas de protección de datos: CLIENTES, PROVEEDORES, RESPUESTA A CANDIDATOS, EMAIL y FAX.
- Propone al cliente el otorgamiento del consentimiento por escrito para el tratamiento de sus datos personales.

2. Funciones y obligaciones del personal

El Responsable de Fichero deberá informar al personal sobre las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en las que pudiera incurrir en caso de incumplimiento. El **artículo 47** del reglamento de protección de datos dice que la formación a los trabajadores es OBLIGATORIA.

- Firma de la cláusula de confidencialidad de los empleados.
- Entrega de copia de las normas de seguridad.
- Formación de los empleados que manejan datos personales.
- No procede porque no hay empleados.

3. Acceso a los datos por cuenta de terceros

- Firmar los contratos de encargado de tratamiento.
- Firmar compromisos de confidencialidad.

4. Identificación y autenticación

- Establecer un mecanismo de identificación y autenticación para acceder a los equipos informáticos que contengan datos de carácter personal.
- En sistemas de autenticación basados en el uso de contraseñas, éstas serán actualizadas periódicamente y deberán almacenarse de forma ininteligible.
- Se limitará el número de intentos fallidos de acceso al sistema de información.

5. Control de acceso

- Restringir el acceso de los usuarios al sistema de información, de forma que dispongan únicamente de acceso autorizado a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- Los dispositivos de almacenamiento de documentación que contenga datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.

6. Gestión de soportes

- Inventariar los soportes utilizados en la entidad, identificando el tipo de información que contienen, almacenándolos en un lugar de acceso restringido al personal autorizado.
- Registrar la entrada y salida de soportes de forma que permita conocer el tipo de soporte, fecha y hora, emisor/destinatario, el número de soportes, tipo de información que contienen, forma de envío y el responsable del envío/entrega.
- Adoptar medidas que impidan cualquier recuperación de datos desde soportes desechados o reutilizados, así como cuando éstos vayan a salir fuera de las instalaciones como consecuencia de operaciones de mantenimiento.

7. Copias de respaldo y recuperación

- Realizar, al menos semanalmente, una copia de seguridad de la información que garantice la reconstrucción de los datos.
- Las copias de seguridad de los datos y de los procedimientos de recuperación de los mismos deberán conservarse en un lugar diferente de aquel en el que se encuentren los equipos informáticos que los tratan.

8. Registro de incidencias

- Cada vez que se produzca o detecte una incidencia deberán llevarse a cabo los registros y notificaciones pertinentes empleando los formularios creados para tal fin.

9. Registro de accesos

- Deberá llevarse a cabo un registro de cada acceso a la información de **nivel alto** contenida en los equipos informáticos, además de establecerse mecanismos que permitan identificar los accesos realizados en el caso de ficheros no automatizados que puedan ser accedidos por múltiples usuarios.

10. Telecomunicaciones

- La transmisión de datos a través de redes de telecomunicaciones deberá garantizar un nivel de seguridad equivalente a los accesos en modo local. Así mismo, la transmisión de datos de nivel alto se realizará cifrando dichos datos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

11. Ejercicio de derechos

- El responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado por el ejercicio de sus derechos.
- Dispone de hojas formularios en papel para el ejercicio de derechos de los afectados.

- En caso de obtener datos personales a través de la web, cómo se realiza el ejercicio de derechos de los afectados:
 - Indicando una dirección de email de contacto Indicando la dirección física de la entidad.
 - La web dispone de una opción específica para ello.
 - No se indica dónde o cómo ejercitar los derechos.

2. CUESTIONES PARTICULARES

DOCUMENTACIÓN EN PAPEL

- Los documentos en papel (Facturas, presupuestos, minutas, albaranes, peticiones, etc.) contienen la cláusula informativa sobre protección de datos RGPD.
- Dispone de consentimiento expreso para la obtención de imágenes o videos de personas, con independencia de su finalidad y destinadas a ser publicadas o difundidas en las propias instalaciones, web, redes sociales, o cualquier otro medio de difusión.

CURRICULUMS

- No se reciben Curriculums**
- Sí se reciben Curriculums**

a) Se informa y/o se solicita el consentimiento al candidato sobre el tratamiento y protección de sus datos personales

- Se informa
- Se solicita consentimiento

b) Cuanto tiempo conserva los curriculums recibidos. Número de meses:

EMPLEADOS (Indique S para SI, N para NO, X para NO SE)

- No hay empleados**
- Sí hay empleados**

a) Cláusulas

- Dispone de documento de Confidencialidad y Funciones y Obligaciones firmado con cada empleado que accede a datos personales.
- Tiene identificado el perfil de acceso a datos personales de cada empleado, tratamientos autorizados, soportes, etc.
- Ha formado a todos los trabajadores de la empresa que manejan datos personales cumpliendo con la política de formación del personal.

CORREO ELECTRÓNICO

- No se utiliza el correo**
- Sí se utiliza el correo**

- Dispone de leyenda informativa al pie de los envíos de emails adaptada al RGPD
- En los casos de envíos masivos o periódicos de emails por motivos publicitarios o suscripción a newsletters, estos incluyen texto apropiado sobre la protección de datos conforme RGPD

WEB

- No tiene página web propia**
- Sí tiene web**
 - La web es sólo informativa, no se obtienen datos personales
 - Dispone de formulario de contacto para consultas o solicitudes
 - Dispone de opción para suscribirse a Newsletter o servicios similares.
 - Se dispone de medio sencillo e inmediato para canalizar la baja del servicio del usuario.

VIDEO VIGILANCIA

- No tiene**
- Sí tiene**

a) Dispone de:

- Cartel de Informativo de zona videovigilada ubicado en cada zona, área, o espacio en que se encuentran las cámaras
- El cartel está adaptado a la nueva norma RGPD (3 espacios de información)
- Dispone de documento informativo a disposición de los usuarios que lo soliciten.
- Ha informado adecuadamente a los empleados sobre la instalación y usos de las videocámaras

ENCARGADOS DE TRATAMIENTO (asesoría, empresa de prevención, software, hosting...)

- No tiene**
- Sí tiene**
 - Dispone de contrato firmado de confidencialidad y protección de datos con TODOS sus encargados de tratamiento.
 - La gestión con algunos encargados se realiza a través de web o plataformas online.
 - El Encargado le ha aportado prueba de que cumple y aplica las normas establecidas en el RGPD

PRESTADORES DE SERVICIOS SIN ACCESO A DATOS (Mantenimiento informático, redes, servicios de limpieza, otros.)

- No tiene**
- Sí tiene**
 - Dispone de contrato firmado de confidencialidad con sus prestadores de servicios habituales.