

RESPONSABLE DE TRATAMIENTO

SOCIEDAD ANONIMA DE PROMOCION Y EQUIPAMIENTO DEL SUELO DE LORCA

A30054019

POL. IND. SAPRELORCA, PARC. EQUIPAMIENTO CTL BZ. 2. 30817 LORCA

DELEGADO DE PROTECCIÓN DE DATOS / AUDITOR EXTERNO

AUDITTA CONSULTORES DE SISTEMAS S.L.

B73488116

AVDA. JUAN CARLOS I, N.º 6, 1ºA. 30800 LORCA

OBJETIVOS DE LA EVALUACIÓN

- Verificar el cumplimiento de la normativa vigente en materia de protección de datos personales:
 - Reglamento UE 2016/679 General de Protección de Datos (RGPD)
 - Ley Orgánica 3/2018 de Protección de Datos Personales (LOPD)
 - Otras normas relacionadas (LSSI, etc.)
 - Otras instrucciones de la autoridad de control
- Evaluar buenas prácticas en materia de protección de datos.

VALIDEZ DEL INFORME

El presente informe tiene un plazo máximo de validez de un año.

PRINCIPIOS GENERALES

LICITUD, LEALTAD Y TRANSPARENCIA	Los datos deben tratarse de manera lícita, leal y transparente. Toda información relativa al tratamiento de datos debe ser accesible y fácil de entender. Con lenguaje claro y sencillo.
LIMITACIÓN DE LA FINALIDAD	Los datos deben recogerse y tratarse con fines determinados, explícitos y legítimos. No siendo posteriormente tratados para fines distintos o incompatibles.
MINIMIZACIÓN DE DATOS	Los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
EXACTITUD	Los datos deben ser exactos y, si fuera preciso, actualizados, debiendo adoptarse todas las medidas razonables para que se rectifiquen o supriman los datos inexactos.
LIMITACIÓN DEL PLAZO DE CONSERVACIÓN	La conservación de los datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o, al menos, desprovistos de elementos que permitan identificar a los interesados.
INTEGRIDAD Y CONFIDENCIALIDAD	Debe garantizarse la seguridad de los datos aplicando medidas de seguridad técnicas y organizativas para asegurar la confidencialidad, integridad y disponibilidad. Protegiéndolos frente acceso no autorizados de terceros, uso ilícito, pérdida, destrucción o daño.
RESPONSABILIDAD PROACTIVA	

Mediante el presente informe pretendemos poner en valor el Principio de Responsabilidad Proactiva según el cual el Responsable debe estar en condiciones de demostrar que el tratamiento de los datos personales se lleva a cabo en cumplimiento de la normativa vigente y los principios generales expuestos.

ALCANCE DE LA EVALUACIÓN

El presente informe se deriva de la evaluación y auditoría de cumplimiento de los principios de responsabilidad proactiva para el siguiente inventario de actividades de tratamiento llevadas a cabo por el responsable de los ficheros:

REGISTRO DE TRATAMIENTO	CATEGORÍAS DE DATOS	FINES DEL TRATAMIENTO	CATEGORÍAS DE INTERESADOS
USUARIOS WEB	DATOS IDENTIFICATIVOS	GESTIÓN DE LOS SERVICIOS Y COMUNICACIONES PRESTADOS A TRAVÉS DEL SITIO WEB Y REDES SOCIALES	USUARIOS WEB Y REDES SOCIALES.
VIDEOVIGILANCIA	IMAGEN / VOZ	SEGURIDAD DE LAS INSTALACIONES. CONTROL DE ACCESO. GESTIÓN Y CONTROL DE LA ACTIVIDAD EN LAS INSTALACIONES. GESTIÓN Y CONTROL LABORAL Y DE SERVICIOS PRESTADOS EN LAS INSTALACIONES.	USUARIOS, VISITANTES, COLABORADORES, TRABAJADORES.
RRHH	DATOS IDENTIFICATIVOS, DATOS SENSIBLES, DATOS DE CARACTERÍSTICAS PERSONALES, DATOS DE CIRCUNSTANCIAS SOCIALES, DATOS ECONÓMICOS Y DE SEGUROS, DATOS NO ECONÓMICOS DE NÓMINA, OTRA INFORMACIÓN LABORAL.	GESTIÓN DE RECURSOS HUMANOS. MANTENIMIENTO Y CONTROL DE OBLIGACIONES LABORALES. PREVENCIÓN DE RIESGOS LABORALES. GESTIÓN DE PERSONAL Y CANDIDATOS. CONTROL DE ACCESO / PRESENCIA. OTROS FINES.	TRABAJADORES, CANDIDATOS.
GESTIÓN	DATOS IDENTIFICATIVOS, DATOS DE CARACTERÍSTICAS PERSONALES, DATOS ECONÓMICOS, FINANCIEROS Y DE SEGUROS. OTROS DATOS.	GESTIÓN DE RELACIONES COMERCIALES CON CLIENTES Y PROVEEDORES. GESTION ADMINISTRATIVA. GESTIÓN ECONÓMICA DE LA ACTIVIDAD. MANTENIMIENTO Y CONTROL DE LAS OBLIGACIONES CONTABLES Y FISCALES. OTROS FINES.	CLIENTES, CLIENTES POTENCIALES, USUARIOS, PROVEEDORES.

**El inventario completo en virtud del artículo 30 RGPD está incluido en la documentación de seguridad del responsable de tratamiento. Este anterior es solamente un resumen limitado al presente informe.*

ANÁLISIS DE CUMPLIMIENTO

A continuación, se recogen los resultados de los aspectos evaluados para comprobar el grado de cumplimiento del responsable del tratamiento y su política de responsabilidad proactiva. Siendo la leyenda de las comprobaciones como sigue:

CONFORME	La cuestión evaluada es conforme a los parámetros y requisitos exigidos.
PENDIENTE	La cuestión evaluada tiene acciones pendientes en proceso de ejecución o decisiones pendientes de administrar.
NO CONFORME	La cuestión evaluada no es conforme a los requisitos exigibles o no se ajusta a las buenas prácticas planteadas por el delegado de protección de datos en su caso.
NO APLICA	La cuestión carece de evaluación por inexistencia o inaplicabilidad en su caso.

En las cuestiones que el auditor considere necesario podrán añadirse además observaciones o recomendaciones con el fin de que el responsable de tratamiento pueda valorarlas.

ASPECTOS JURÍDICOS.

¿Se mantienen actualizados y exactos los datos personales tratados? (art. 5 RGPD) (art. 4 LOPD)	CONFORME
¿Tiene la legitimación necesaria para el tratamiento de los datos personales? (art. 6 RGPD) (arts. 6, 7 y 8 LOPD)	CONFORME
En caso de basarnos en el consentimiento para el tratamiento de datos, ¿se puede demostrar que el afectado dio su consentimiento? (art. 7 RGPD) (arts. 6, 7 y 19 LOPD)	CONFORME
¿Ha incorporado las cláusulas de información y consentimiento en los canales donde se recojan datos personales (formularios de recogida de datos, e-mails, facturas, presupuestos, etc.)? (arts. 12, 13 y 14 RGPD) (art. 11 LOPD)	CONFORME
¿Ha firmado los correspondientes contratos con los terceros que acceden a datos para prestarle un servicio (encargados de tratamiento)? (art. 28 RGPD) (art. 28 LOPD)	CONFORME
En caso de enviar comunicaciones comerciales por correo electrónico, ¿tiene la autorización correspondiente de los destinatarios o puede ampararse en alguno de los casos de legitimación que establecidos? (arts. 5 y 6 RGPD) (arts. 4 y 23 LOPD)	CONFORME
¿Los empleados han firmado el compromiso de confidencialidad correspondiente? (arts. 5 y 32 RGPD) (art. 5 LOPD)	CONFORME

Si se realiza transferencia internacional de datos, ¿se realizan a países declarados de nivel de protección adecuado por la Comisión Europea? (arts. 44 a 50 RGPD) (arts. 40 a 43 LOPD)	NO APLICA
--	------------------

ASPECTOS ORGANIZATIVOS

¿Se ha proporcionado a los empleados información acerca de sus funciones y obligaciones en relación con los datos que tratan? ¿Se ha llevado a cabo algún tipo de concienciación o formación? (arts. 24 y 32 RGPD) (art. 28 LOPD)	CONFORME
¿Dispone del correspondiente Registro de Actividades de Tratamiento debidamente actualizado? (art. 30 RGPD) (art. 31 LOPD)	CONFORME
Ha valorado, según el tratamiento de datos, ¿si debe llevar a cabo una evaluación de impacto relativa a la protección de datos (EIPD)? (art. 35 RGPD) (art. 28 LOPD)	CONFORME
Ha valorado, según el tratamiento de datos, ¿si debe designar un delegado de protección de datos (DPD) en su empresa? (arts. 37 a 39 RGPD) (arts. 34 a 37 LOPD)	CONFORME

ASPECTOS TÉCNICOS

Ha implantado medidas de seguridad en sus sistemas para garantizar la integridad y confidencialidad de los datos personales? (art. 32 RGPD)	CONFORME
¿Se ha establecido un método de autenticación para cada uno de los usuarios del sistema de información de la empresa? (art. 32 RGPD)	CONFORME
¿Hay establecida una política de complejidad de las claves de acceso y caducidad de las mismas? (art. 32 RGPD)	CONFORME
¿Hay establecidos perfiles de usuario según los roles de cada uno de los empleados? (art. 32 RGPD)	CONFORME
¿Tiene activado el bloqueo de las estaciones de trabajo pasado cierto tiempo de inactividad? (art. 32 RGPD)	CONFORME
¿Realiza copias de seguridad periódicas de forma segura? (art. 32 RGPD)	CONFORME
¿Dispone de una copia de seguridad fuera de sus instalaciones? (art. 32 RGPD)	CONFORME
¿Tiene instalados en sus ordenadores sistemas de protección contra ataques externos (antivirus, firewall, etc.)? (art. 32 RGPD)	CONFORME
¿Tiene aplicadas medida de protección adicionales para los dispositivos portátiles que contienen datos personales? (art. 32 RGPD)	CONFORME

¿Ha realizado el correspondiente análisis de riesgos donde se valoren qué medidas de seguridad aplicar en función de las amenazas detectados? (arts. 32 Y 35 RGPD)	CONFORME
¿Se aplican las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratan los datos necesarios para cada una de las finalidades? (art. 25 RGPD)	CONFORME

DOCUMENTACIÓN EN PAPEL

¿Tiene establecido un criterio de archivo para la documentación en papel? (art. 32 RGPD)	CONFORME
¿Guarda bajo llave la documentación más sensible? (art. 32 RGPD)	CONFORME
¿Dispone de destructora/s de papel o contrato con empresa externa para dicha finalidad? (art. 32 RGPD)	CONFORME

PROTOCOLOS

¿Se ha establecido un protocolo y procedimiento de ejercicio de los derechos por parte de los interesados? (arts. 15 a 22 RGPD) (arts. 12 a 18 LOPD)	CONFORME
¿Disponen de los protocolos correspondientes para la gestión de las brechas de seguridad? (arts. 33 y 34 RGPD)	CONFORME

SITIO WEB

¿Ha incluido en su página el aviso legal correspondiente?	CONFORME
En caso de recogerse datos a través de la web, ¿ha incluido la política de privacidad?	CONFORME
En caso de disponer de una suscripción a un boletín electrónico, ¿obtiene el consentimiento para dicho envío de forma adecuada y sin casillas pre-marcadas?	NO APLICA
En caso de utilizar cookies en su página web, ¿ha incluido la política de cookies y el banner correspondiente de uso de las mismas?	CONFORME
En caso de gestionar una tienda online (ecommerce), ¿ha incluido las correspondientes condiciones generales de contratación?	NO APLICA
Si envía comunicaciones comerciales vía electrónica, ¿ofrece la posibilidad de darse de baja de dichas comunicaciones en cada uno de los envíos?	NO APLICA

**En la evaluación del sitio web se han tenido en cuenta normas aplicables de privacidad, sociedad de la información y comercio electrónico.*

VIDEOVIGILANCIA

¿Ha colocado el cartel informativo para informar sobre la captación de imágenes?	CONFORME
¿Indica claramente en los carteles donde ejercer los derechos de los afectados?	CONFORME

¿Tiene establecida una política de conservación de las imágenes que no supere los 30 días?	CONFORME
¿Se ha asegurado que las cámaras de video vigilancia no vulneren el derecho a la intimidad o no graben en zonas públicas?	CONFORME

**arts. 15 RGPD y arts. 22 y 89 LOPD*

OBSERVACIONES

Los datos personales que se tratan en los sistemas del responsable de tratamiento pertenecen a las siguientes categorías de interesados / afectados:

- Clientes
- Proveedores
- Trabajadores
- Otros interesados

En el caso de los trabajadores el tratamiento de datos se legitima en base a los artículos 6, 7, 9 y 10 RGPD existiendo tanto un justificante de la relación contractual (contrato de trabajo) como un justificante de información ampliada y obtención de consentimiento acerca de los distintos fines de tratamiento de datos de los trabajadores.

En el caso de los clientes y proveedores, el responsable de tratamiento ampara su base legal de manejo de los datos en el artículo 6 RGPD, dada la relación comercial y negocial existente y el interés mutuo de las partes; así como en el artículo 19 LOPD, dada la característica de ser datos personales de contacto de personas que prestan sus funciones y servicios en personas jurídicas.

Cualquier otra categoría de interesados así como actividad de tratamiento distinta a las anteriores se basará en alguna de las posibles legitimaciones siguientes: a) consentimiento informado del interesado; b) cumplimiento de compromisos contractuales; c) intereses legítimos del responsable; y d) cumplimiento de deberes y obligaciones legales.

En todo caso el responsable de tratamiento cuenta con los procedimientos correctos para cumplir con el deber de información y transparencia a los interesados.

El presente informe deriva de la toma de datos practicada por el Auditor así como la información facilitada por el Auditado, incluidas las valoraciones correspondientes según la línea temporal de los servicios prestados al Auditado.

En general el plan de protección de datos se desarrolla con normalidad, basándose en un ciclo de vida continuado por el que periódicamente se revisan los distintos puntos de control correspondientes. La propia naturaleza de la actividad del responsable es causa de que sobrevengan cambios organizativos, técnicos o legales; los cuales generan tareas que son debidamente atendidas una vez detectadas.

El compromiso del responsable con el plan de protección de datos y conciencia por la privacidad existe y es elevado.

CONCLUSIONES FINALES

El Responsable de Tratamiento observa y cumple la normativa vigente en materia de protección de datos: L.O. 3/2018 (LOPD), REGLAMENTO UE 2016/679 (RGPD), y otras disposiciones legales en la materia vigentes.

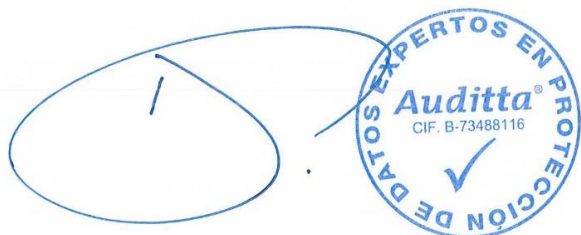
Auditta Consultores de Sistemas S.L. presta los servicios especializados en esta materia a favor del Responsable de Tratamiento: consultoría, asesoramiento y evaluación, RESULTANDO:

1. Se ha evaluado el estado de cumplimiento de la normativa vigente LOPD Y RLOPD.
2. Se han estudiado las obligaciones derivadas del RGPD y otras impuestas por el resto de las disposiciones vigentes en la materia (instrucciones de la autoridad de control)
3. Se han analizado los tratamientos de datos personales que se llevan a cabo en los sistemas de información (papel e informático) del Responsable de Tratamiento, y se han estudiado las bases de legitimación de estos.
4. Se han inventariado las actividades de tratamiento.
5. Se han analizado los riesgos existentes y registrado la evaluación de impacto pertinente.
6. Se ha establecido un sistema de gestión de derechos de los interesados.
7. Se ha establecido un sistema de control de intercambio de datos con terceras partes (corresponsables, encargados de tratamiento).
8. Se han definido el marco general de tratamiento de los datos, la política de privacidad y la política general de seguridad de los datos. Introduciéndose los oportunos textos legales necesarios en las diferentes áreas (comercial, personal, marketing, atención al cliente, etc.)
9. Se ha definido la figura del Delegado de Protección de Datos.
10. Se ha iniciado un protocolo de cumplimiento (ciclo de cumplimiento).

Todo ello ha permitido al Responsable de Tratamiento establecer un sistema de cumplimiento y gestión de la privacidad basado en un ciclo de vida continuado sobre el que se trabaja recurrentemente para garantizar la adopción de las disposiciones legales, la seguridad de la información y el ejercicio de los derechos de los interesados.

Mediante el presente hacemos constar la realidad de estos hechos, dando por cierto el compromiso, implementación y cumplimiento del Responsable de Tratamiento, habiendo obtenido un **RESULTADO FAVORABLE** en las acciones de evaluación practicadas.

A quien pueda legítimamente interesar,



Fdo.: AUDITTA CONSULTORES DE SISTEMAS S.L.

Recibí conforme,

Fdo.: SOCIEDAD ANONIMA DE PROMOCION Y EQUIPAMIENTO DEL SUELO DE LORCA