¿POR QUÉ ES NECESARIO INSTALAR UN GESTOR DE CONSENTIMIENTOS AVANZADO EN TU SITIO WEB?

En esta era digital, la protección de datos personales y la transparencia en el manejo de estos se han convertido en aspectos cruciales, no solo para el cumplimiento legal, sino también para fortalecer la confianza de sus usuarios. La Agencia Española de Protección de Datos (AEPD), junto con el Reglamento General de Protección de Datos (RGPD) de la UE y otras normativas relevantes como la LOPDGDD y la LSSI-CE, han establecido directrices claras que exigen una gestión más sofisticada de los consentimientos en las páginas web.

Todas estas normativas son fundamentales porque:

1. **Protegen los datos personales de los usuarios:** Estas leyes garantizan que la información personal de los usuarios, como nombres, direcciones de correo electrónico y hábitos de navegación, esté segura y se utilice de manera responsable.
2. **Establecen la transparencia en el uso de datos:** Obligan a las empresas a ser transparentes sobre cómo se recopilan, usan y comparten los datos de los usuarios.
3. **Empoderan a los usuarios:** Les dan a los usuarios el control sobre sus datos, permitiéndoles elegir qué información comparten y cómo se utiliza.

Aspectos clave de la nueva guía de la AEPD y otras Leyes

El **pasado 11 de enero del 2024** terminó el período transitorio de 6 meses que la Agencia Española de Protección de Datos estableció para que las páginas web se adaptasen a los nuevos criterios de la Guía sobre el uso de las cookies.

La nueva guía de la AEPD, junto con el RGPD, LOPDGDD y la Ley de Cookies, establece requisitos estrictos para la gestión de consentimientos en sitios web. Estas normativas son fundamentales para la protección de datos personales y la privacidad en línea, y su cumplimiento es esencial para evitar sanciones y mantener la confianza de los usuarios.

A continuación, exploramos los puntos clave y las implicaciones de estas normativas para los propietarios de sitios web.

- **Consentimiento claro y afirmativo:** El consentimiento para el uso de cookies debe ser explícito, no asumiendo el consentimiento por el mero hecho de navegar en el sitio web.
- **Configuración granular del consentimiento:** Posibilidad para los usuarios de dar su consentimiento de manera detallada, aceptando o rechazando diferentes tipos o categorías de cookies.
- **Información concisa, transparente e inteligible:** Proporcionar información clara y accesible sobre el uso de las cookies, incluyendo su definición, función, tipos, finalidades, y entidades que las gestionan.
- **Actualización del consentimiento:** Se recomienda renovar el consentimiento cada 24 meses, manteniendo las preferencias del usuario durante este período.
- **Cumplimiento con RGPD:** Asegurar que la gestión de consentimientos esté en conformidad con el RGPD, protegiendo los datos personales recogidos.
- **Monitorización regular y actualización de políticas de cookies:** Verificar regularmente la existencia de nuevas cookies y actualizar la política correspondiente.
- **Bloqueo previo al consentimiento:** Todos los elementos de seguimiento deben estar bloqueados hasta obtener el consentimiento explícito del usuario.
- **Opción de rechazo claramente visible y accesible:** Facilitar una opción para rechazar las cookies, presentada con la misma facilidad que la opción de aceptarlas.
- **Facilidad para cambiar preferencias:** Permitir a los usuarios cambiar su consentimiento sobre el uso de las cookies, fácilmente y en cualquier momento.

- **Consentimiento de menores de edad:** Incluir medidas específicas para obtener el consentimiento en el caso de usuarios menores de edad.
- **Evitar patrones engañosos:** No emplear tácticas que puedan inducir a los usuarios a aceptar cookies involuntariamente, usando un diseño adecuado en botones y opciones de consentimiento.
- **Documentación y registros de consentimiento:** Mantener registros adecuados del consentimiento otorgado, documentando cómo y cuándo se obtiene y facilitando la revocación de este.
- **Facilidad de integración y actualización:** La plataforma debe ser fácil de integrar y mantener actualizada con los cambios legislativos y las mejores prácticas.

¿Cuáles son las consecuencias de no cumplir las normativas?

El incumplimiento de las nuevas normativas de la AEPD sobre consentimiento en sitios web puede llevar a penalizaciones significativas.

El valor de las multas por incumplimiento de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) en relación con el uso de cookies y la gestión de consentimientos en sitios web puede variar ampliamente. Las sanciones se determinan en función de varios criterios, como la gravedad de la infracción, las medidas de seguridad previamente implementadas por la empresa, y el impacto causado por la infracción. Factores adicionales como el volumen y la sensibilidad de los datos implicados, el potencial daño a los individuos afectados, y la duración del incumplimiento también juegan un papel importante en la determinación de la multa. Estos criterios ayudan a establecer una sanción proporcional a cada caso específico, garantizando que las penalizaciones sean justas y acordes con la naturaleza del incumplimiento.

Para garantizar el cumplimiento de estas normativas y evitar posibles sanciones, es altamente recomendable realizar una auditoría completa de su página web. Esta auditoría debería centrarse en identificar y clasificar todas las cookies utilizadas, así como en revisar los métodos actuales de obtención de consentimiento.

Además, la implementación de un gestor de consentimientos avanzado se ha vuelto imprescindible. Un gestor de consentimientos eficaz no solo asegura que su sitio web esté en conformidad con las leyes actuales, sino que también mejora la experiencia del usuario, proporcionando transparencia y control sobre sus datos personales.

¿Qué es un gestor de consentimientos y por qué es vital para su sitio web?

Un gestor de consentimientos es una herramienta esencial para sitios web en la era de las regulaciones de privacidad de datos. Su función principal es obtener, gestionar y documentar el consentimiento de los usuarios para el uso de sus datos personales, incluyendo cookies y otros métodos de seguimiento. Esto es vital para cumplir con las normativas mencionadas, que exigen el consentimiento claro y específico de los usuarios para el tratamiento de sus datos. Un gestor de consentimientos adecuado asegura que su sitio web no solo cumpla con estas normativas, sino que también ofrezca transparencia y controle la privacidad de los usuarios, fortaleciendo su confianza y cumpliendo con los requisitos legales.

¿Cómo te ayudamos a cumplir?

En Dimension Compliance, les ofrecemos la implantación de la plataforma avanzada de gestión de consentimientos, Lex4Web, que está diseñada para cumplir con todas estas regulaciones. Nuestro objetivo es hacer que este proceso sea lo más sencillo y transparente posible, tanto para ustedes como para sus usuarios.

¿Qué incluye Lex4Web?

1. **Actualización dinámica:** Se adapta automáticamente a cambios en la legislación. Si un país actualiza sus leyes de protección de datos, la herramienta se ajusta automáticamente para cumplir con estas nuevas normas.
2. **Multianalítica**: Permite integrar varias herramientas de análisis web, como Google Analytics o Matomo, garantizando que se obtenga el consentimiento adecuado para su uso.
3. **Consentimientos para datos sensibles:** Facilita la obtención de consentimientos específicos para el tratamiento de datos categorizados como sensibles, como la información de salud.
4. **Recibo de consentimiento:** Genera comprobantes de consentimiento, proporcionando un registro del consentimiento del usuario que puede ser crucial durante las auditorías de cumplimiento. Esto supone una garantía para la empresa. Sin la generación automática de estos recibos, el desarrollo de dicho documento llega a ser un trabajo complicado y costoso, ya que exigirá mucho tiempo.
5. **Protección Infantil:** Asegura el cumplimiento de las leyes de protección infantil en línea, solicitando consentimientos apropiados para usuarios menores de edad.

6. **Control global de privacidad:** Respeta las preferencias de privacidad de los navegadores de los usuarios, como "No rastrear", y ajusta el seguimiento en consecuencia.
7. **Ejercicio de derechos:** Permite a los usuarios ejercer fácilmente sus derechos de privacidad, como el acceso, rectificación o eliminación de sus datos.
8. **Consentimiento para marketing:** Gestiona el consentimiento para comunicaciones de marketing y publicidad, permitiendo a los usuarios optar por recibir o no dichas comunicaciones.
9. **Multi Idioma:** Ofrece opciones en varios idiomas, facilitando que usuarios de diferentes regiones comprendan y gestionen sus preferencias de privacidad.
10. **Multi País:** Se adapta a la legislación específica de cada país, asegurando el cumplimiento legal, indistintamente de dónde se encuentre el usuario. *(Consultar lista de países)*

Cada una de estas funcionalidades está diseñada para hacer que la gestión del consentimiento sea más accesible, transparente y conforme a las leyes vigentes, mejorando la experiencia del usuario y asegurando el cumplimiento legal del sitio web.

Entendiendo las Cookies y los Trackers en los sitios Web

En el vasto mundo de Internet, cada sitio web que visitamos interactúa de alguna manera con nuestros datos. Esta interacción se realiza principalmente a través de "cookies" y "trackers".

Las cookies son pequeños archivos de texto que se almacenan en nuestro navegador. Son utilizadas por los sitios web para recordar información sobre nosotros, como nuestras preferencias de navegación, detalles de inicio de sesión, y para rastrear nuestro comportamiento en línea con fines de análisis o publicidad.

Por otro lado, los trackers son software que trabajan de forma oculta dentro de una aplicación para recopilar, almacenar y compartir información sobre los usuarios en Internet. De esta manera, estos operadores reportan datos, como el tiempo que el usuario pasa en dicha aplicación, los botones que se pulsan y toda la actividad que se registre.

Si bien estas herramientas son fundamentales para una experiencia de navegación moderna y personalizada, también plantean preocupaciones significativas sobre la privacidad y el uso de datos personales. Es aquí donde entran en juego las regulaciones y leyes de protección de datos, que buscan equilibrar los beneficios de estas tecnologías con el derecho a la privacidad y el control sobre la propia información personal.

Conoce las normativas vigentes

- El **Reglamento General de Protección de Datos (RGPD)** es una ley de la Unión Europea que establece cómo se deben recopilar, almacenar y utilizar los datos personales. Exige que los usuarios den su consentimiento de manera clara y explícita antes de que sus datos sean utilizados. Esto incluye detalles como su nombre, dirección de correo electrónico, ubicación, etc.

- La **Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)** es la ley española específica que amplía la del RGPD, proporcionando normas adicionales para asegurar que los derechos digitales de los usuarios estén protegidos.

- La **Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE)** regula las actividades en línea en España, incluyendo el marketing por correo electrónico y la publicidad en línea.

- La **Ley de Cookies en España**, que complementa las disposiciones del RGPD, regula específicamente el uso de cookies en páginas web, aplicaciones y servicios en línea. Ha evolucionado para adaptarse a las prácticas actuales y las preocupaciones de privacidad, especialmente en lo que respecta a cookies de terceros y cookies de seguimiento.

Más ejemplos de incumplimiento comunes en sitios web

Enunciado del caso	Explicación detallada	Cómo resolverlo para evitar una sanción
Consentimiento implícito	El sitio asume consentimiento cuando el usuario sigue navegando.	Implementar un sistema de consentimiento explícito.
Falta de opción de rechazo	No hay botón para rechazar cookies en el banner.	Añadir un botón claro de rechazo en el banner.
Información confusa	El banner de cookies usa lenguaje técnico difícil de entender.	Usar lenguaje claro y sencillo en el banner.
Consentimiento no granular	El sitio solo permite aceptar o rechazar todas las cookies juntas.	Permitir a los usuarios elegir tipos específicos de cookies.
Cookies preseleccionadas	Las cookies opcionales están preseleccionadas para el consentimiento.	Dejar todas las cookies opcionales sin seleccionar por defecto.
Falta de actualización de consentimiento	El consentimiento no se actualiza regularmente.	Establecer recordatorios para renovar consentimientos cada 24 meses.
Uso de patrones engañosos	Diseño del banner que induce a aceptar cookies inadvertidamente.	Asegurar un diseño equitativo de opciones en el banner.
Cookies no necesarias activas sin consentimiento	Cookies no esenciales activas antes de obtener consentimiento.	Bloquear todas las cookies no esenciales hasta obtener consentimiento.

Confirmación de rechazo con cookies y trackers activos	A pesar de que el usuario rechaza el uso de cookies y trackers, estos siguen activos en el sitio web, recopilando datos sin consentimiento.	Implementar controles técnicos que desactiven efectivamente todas las cookies y trackers no esenciales cuando un usuario rechace su uso. Realizar pruebas regulares para asegurar que el rechazo de consentimiento sea respetado y efectivo.
Ausencia de documentación de consentimiento	No se guardan registros del consentimiento otorgado.	Implementar un sistema para documentar y almacenar consentimientos.
No protección infantil	Falta de medidas específicas para el consentimiento de menores.	Integrar verificaciones de edad y consentimientos parentales.
Consentimiento no específico	Consentimiento general que no cubre todos los usos de datos.	Obtener consentimientos específicos para distintos usos de datos.
No informar sobre transferencias internacionales	Falta de información sobre transferencia de datos a terceros países.	Incluir información sobre transferencias internacionales en el banner.
Consentimiento no bien informado	Los usuarios no entienden completamente para qué dan consentimiento.	Proporcionar información detallada sobre el uso de los datos.
Falta de facilidad para revocar consentimiento	No es fácil para los usuarios cambiar o retirar su consentimiento.	Ofrecer una opción clara y accesible para cambiar preferencias.
Falta de opciones en múltiples idiomas	El sistema de consentimiento solo está disponible en un idioma.	Proporcionar opciones de consentimiento en varios idiomas.
No cumplimiento de legislaciones nacionales	El sistema no se adapta a las leyes específicas de cada país.	Ajustar el sistema a las normativas específicas de cada país.
Falta de consentimiento para perfiles	No se obtiene consentimiento específico para la creación de perfiles.	Solicitar consentimiento separado para actividades de perfilado.
Uso de cookies sin consentimiento	Cookies usadas antes de obtener consentimiento.	Configurar el sitio web para que no use cookies hasta obtener consentimiento.
Uso de terceras partes sin transparencia	Falta de claridad sobre el uso de cookies de terceros.	Informar explícitamente sobre el uso y finalidad de cookies de terceros.
Seguimiento de menores sin protección	Rastreo de menores de edad sin medidas de protección adecuadas.	Implementar verificaciones de edad y obtener consentimiento parental donde sea necesario.
Uso de patrones engañosos	Diseño de banners de consentimiento que inducen a aceptar cookies involuntariamente.	Diseñar banners de consentimiento de manera que todas las opciones sean igualmente visibles y accesibles.

Mapa de Google sin consentimiento	Si tienes una página web sencilla sin formulario de contacto, pero incluyes un mapa de Google para mostrar la ubicación de tu empresa, estás utilizando cookies de Google. Estas cookies recopilan información del usuario y son esenciales para el funcionamiento del mapa. Sin embargo, el uso de estas cookies requiere consentimiento explícito de los usuarios según el RGPD y la Ley de Cookies, ya que implican un tratamiento de datos personales.	Implementar un gestor de consentimientos en tu sitio web que informe a los usuarios sobre estas cookies y les permita aceptarlas o rechazarlas antes de activar el mapa.
Instalación de Google Analytics, o similares, sin consentimiento	Tu agencia de marketing sugiere usar Google Analytics para entender mejor a tus visitantes, pero no has informado ni obtenido el consentimiento de los usuarios.	Asegúrate de informar a los usuarios sobre el uso de Google Analytics y obtener su consentimiento antes de la instalación.
Uso de cookies de seguimiento sin aviso	Tu sitio web utiliza cookies para personalizar la publicidad, pero no has avisado a los usuarios ni les has dado la opción de rechazarlas.	Implementa un aviso claro sobre el uso de cookies y proporciona una opción para aceptarlas o rechazarlas.
Formularios pre-marcados para marketing	Los formularios de tu web vienen con opciones pre-marcadas para recibir marketing, lo cual no es un consentimiento explícito.	Asegúrate de que las casillas de marketing estén desmarcadas por defecto y requieran una acción clara del usuario para optar por ellas.
Falta de aviso legal en la web	Tu sitio no cuenta con un aviso legal que cumpla con la normativa vigente.	Incluye un aviso legal completo y accesible que cumpla con la Ley 34/2002 LSSI-CE1.
Ausencia de política de cookies clara	Las políticas de cookies de tu web son confusas o inexistentes.	Redacta una política de cookies clara y asegúrate de que sea fácilmente accesible para los usuarios.
No permitir la revocación del consentimiento	Los usuarios no pueden revocar fácilmente el consentimiento otorgado previamente.	Proporciona una opción clara y accesible para que los usuarios retiren su consentimiento en cualquier momento.
No cumplir con el derecho de acceso	Un usuario solicita acceso a sus datos personales y no se le proporciona esta información.	Cumple con las solicitudes de acceso a datos de manera oportuna y conforme a lo establecido por la ley.
No cumplir con el derecho al olvido	Un usuario solicita la eliminación de sus datos y no respondes a su petición.	Establece un proceso para atender y cumplir con las solicitudes de eliminación de datos de forma oportuna.

Falta de actualización de la política de privacidad	La política de privacidad de tu web está desactualizada y no refleja las prácticas actuales de recopilación de datos.	Revisa y actualiza tu política de privacidad regularmente para asegurar que cumple con la normativa vigente.
Ausencia de Delegado de Protección de Datos (DPO)	Tu empresa está obligada a tener un DPD y no lo has designado.	Designa un DPD y asegúrate de que sus datos de contacto estén disponibles para los usuarios.

Extractos más importantes de las leyes que orientan al uso de un gestor de consentimientos avanzado

Según la RGPD y la Directiva ePrivacy , lo que se requiere es:

Considerando (42) RGPD

Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento.

RGPD Artículo 7. Condiciones para el consentimiento

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.
2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.
4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Todo esto implica que se requiere poder demostrar que el interesado ha dado el consentimiento (de manera informada) a la (concreta) operación de tratamiento. No solo demostrar que se ha solicitado, en su lugar, lo que se pide es demostrar que el interesado ha otorgado el consentimiento, además de manera informada.

Directrices EDPB 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679

5.1 Demostrar el consentimiento

- 104. El artículo 7, apartado 1, del RGPD indica claramente la obligación explícita del responsable del tratamiento de demostrar el consentimiento del interesado. De conformidad con el artículo 7, apartado 1, le corresponde al responsable de demostrar dicho consentimiento.

- 105. El considerando 42 establece que: «Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento».

- 106. Los responsables del tratamiento tienen libertad para desarrollar métodos que permitan cumplir esta disposición adaptados a sus operaciones diarias. Al mismo tiempo, la obligación de demostrar que un responsable del tratamiento ha obtenido un consentimiento válido, no debe en sí misma provocar un tratamiento adicional de datos excesivo. Esto significa que los responsables deberían tener datos suficientes para mostrar un enlace al tratamiento (para mostrar que se obtuvo el consentimiento), pero no deberían recopilar más información de la necesaria.

- 107. Corresponde al responsable demostrar que obtuvo el consentimiento válido del interesado. El RGPD no prescribe cómo debe hacerse esto exactamente. No obstante, el responsable debe poder demostrar que, en un caso concreto, un interesado ha dado su consentimiento. La obligación de demostrar el consentimiento existirá mientras dure la actividad de tratamiento de los datos en cuestión. Una vez finalizada dicha actividad, la prueba del consentimiento no deberá conservarse más allá de lo estrictamente necesario para cumplir una obligación legal o para la formulación, el ejercicio o la defensa de reclamaciones, de conformidad con el artículo 17, apartado 3, letras b) y e).

- 108. Por ejemplo, el responsable debe mantener un registro de las declaraciones de consentimiento recibidas, de manera que pueda demostrar cómo se obtuvo el consentimiento y cuándo se obtuvo dicho consentimiento, y también deberá demostrarse la información que se facilitó al interesado en su momento. El responsable también deberá poder demostrar que se informó al interesado y que el flujo de trabajo del responsable cumplió todos los criterios pertinentes para un consentimiento válido. La lógica subyacente a esta obligación en el RGPD es que los responsables del tratamiento deben rendir cuentas con respecto a la obtención del consentimiento válido de los interesados y con respecto a los mecanismos de

consentimiento que han adoptado. Por ejemplo, en un contexto en línea, un responsable podría conservar información sobre la sesión en la que se expresó el consentimiento, junto con documentación sobre el flujo de trabajo del consentimiento cuando dicha sesión tuvo lugar, y una copia de la información que se presentó en ese momento al interesado. No sería suficiente referirse únicamente a una configuración correcta del sitio web en cuestión.

- 109. Ejemplo 21: Un hospital crea un programa de investigación científica, denominado proyecto X, para el que se requiere el historial clínico dental de pacientes reales. Los participantes se captan a través de llamadas telefónicas a pacientes que acuerdan voluntariamente formar parte de una lista de candidatos a los que se pueda contactar para este fin. El responsable del tratamiento busca el consentimiento explícito de los interesados para utilizar su historial clínico dental. El consentimiento se obtiene por teléfono mediante la grabación de una declaración verbal del interesado en la que confirma que está de acuerdo con que se utilicen sus datos para los fines del proyecto X.

- 110. El RGPD no establece un límite de duración para el consentimiento. La duración del consentimiento dependerá del contexto, del alcance del consentimiento original y de las expectativas del interesado. Si las operaciones de tratamiento cambian o evolucionan de manera considerable, el consentimiento original dejará de tener validez. En este caso, deberá obtenerse un nuevo consentimiento.

- 111. El CEPD recomienda como mejor práctica la renovación del consentimiento a intervalos apropiados. Facilitar toda la información de nuevo contribuye a garantizar que el interesado sigue estando bien informado sobre cómo se utilizan sus datos y sobre cómo ejercer sus derechos.

Por todo esto recomendamos, además de tener actualizados los tratamientos y los textos legales en la web (política de privacidad, política de cookies y aviso legal), implantar un gestor de consentimiento de cookies que mantenga un registro seguro de todos los consentimientos, obligados por ley, para que en el caso de ser requeridos poder demostrarlo.

Según las recomendaciones del Consejo Europeo de Protección de Datos (CEPD) sobre mecanismos para hacer efectiva la denegación o la retirada del consentimiento:

- La cookie para registrar la negativa del consumidor es necesaria para respetar su elección. Puede ser necesario registrar la decisión del usuario durante un período determinado, a fin de reducir la frecuencia de las solicitudes de consentimiento que recibe un usuario. El CEPD considera que el período de un año es adecuado para ello.

- El CEPD recomienda aclarar que el registro del "consentimiento negativo" basado en cookies no debe contener un identificador único, sino más bien información genérica, una bandera o un código, común a todos los usuarios que han rechazado el consentimiento. El CEPD recuerda que las cookies que registran la denegación del consentimiento pueden ser eliminadas por el usuario o debido a un cambio en la configuración técnica, en el plazo de un año. En tal caso, cuando el responsable del tratamiento ya no tenga acceso al registro de la denegación del consentimiento, el CEPD considera razonable solicitar al usuario una nueva solicitud de consentimiento.

Todas estas estipulaciones de la normativa condicionan a cualquier propietario de un sitio web, que disponga de cookies que no sean estrictamente las necesarias para su funcionamiento, a implantar un gestor de consentimiento de avanzado que cumpla las

funciones de registro de consentimiento según las indicaciones de las Autoridades de Control

¡Con Lex4Web todas estas situaciones quedan resueltas y evitarás sanciones!

Además

1. Es una plataforma diseñada por expertos en cumplimiento normativo.

2. Es una solución española que asegura que las empresas de nuestro país estarán siempre actualizadas con los últimos requerimientos de las normativas vinculadas.

3. Ofrecen un soporte más cercano y ágil, frente a soluciones de grandes corporaciones que deben seguir unos procedimientos muy estrictos de atención y soporte al usuario.

4. Trabajan continuamente en mejoras de la plataforma, con un diseño basado en la ciberseguridad y en el cumplimiento normativo.