Financiado por la Unión Europea
NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA, COMERCIO Y EMPRESA

GUÍA DE CUMPLIMIENTO NORMATIVO DE COMERCIO

Servicio de modernización y dinamización de la oferta comercial de Reinosa a través de la transformación digital.

Exp. 2023/3147

Actuación A3 - Formación para el sector comercial

REINOSA

LEGISLACIÓN COMERCIAL Y PROTECCIÓN DE DATOS

GUÍA PRÁCTICA

1. La nueva legislación en materia de protección de datos.

En los últimos años, la preocupación por la privacidad y la protección de los datos personales ha cobrado una relevancia sin precedentes. Con el crecimiento exponencial de la digitalización y la globalización de los negocios, el volumen de datos generados y compartidos ha aumentado de manera significativa. Esto ha llevado a que los legisladores de diversas partes del mundo revisen y actualicen sus marcos normativos para garantizar una *adecuada* protección de los datos personales. En este contexto, la nueva legislación en materia de protección de datos surge como una respuesta necesaria para salvaguardar la privacidad de los individuos y fortalecer la confianza en el entorno digital.

Una de las regulaciones más destacadas en este ámbito es el **Reglamento General de Protección de Datos (RGPD) de la Unión Europea,** que entró en vigor el 25 de mayo de 2018. Este reglamento ha establecido un nuevo estándar global para la protección de datos, imponiendo obligaciones rigurosas a las organizaciones que manejan información personal de ciudadanos europeos. El RGPD no solo afecta a las empresas situadas en la Unión Europea, sino también a aquellas fuera de sus fronteras que procesan datos de residentes en la UE, ampliando así su impacto a nivel global. La finalidad principal del RGPD es dar a los individuos un mayor control sobre sus datos personales y simplificar el entorno regulatorio para los negocios internacionales mediante la unificación de las regulaciones de privacidad dentro de la UE.

El RGPD introduce varios principios fundamentales que las organizaciones deben seguir para garantizar el cumplimiento. Entre estos principios se encuentran la **legalidad, equidad y transparencia en el procesamiento de datos, la limitación de propósito, la minimización de datos, la precisión, la limitación del almacenamiento y la integridad y confidencialidad**. Estos principios obligan a las empresas a recopilar solo los datos necesarios, a mantenerlos actualizados y a almacenarlos de manera segura, lo que minimiza los riesgos de violaciones de la privacidad.

En el ámbito del comercio, el cumplimiento normativo en materia de protección de datos se ha vuelto una prioridad crucial. Los comercios, tanto grandes como pequeños, manejan una gran cantidad de información personal, desde datos de contacto hasta historiales de compra y

preferencias de los clientes. Asegurar la protección de estos datos no solo es una obligación legal, sino también una práctica esencial para mantener la confianza de los clientes y evitar sanciones significativas.

Para los comercios, adaptarse a la nueva legislación en protección de datos implica implementar diversas medidas técnicas y organizativas. **Entre estas medidas se incluyen la realización de evaluaciones de impacto sobre la protección de datos, la designación de un delegado de protección de datos (DPO), la adopción de políticas de privacidad claras y comprensibles, y la formación continua del personal sobre las mejores prácticas en protección de datos.** Además, es fundamental establecer procedimientos efectivos para la gestión de incidencias de seguridad, como las brechas de datos, y garantizar que los derechos de los individuos, como el derecho de acceso y el derecho al olvido, se respeten y faciliten adecuadamente.

El cumplimiento normativo en materia de protección de datos no solo protege a los individuos, sino que también ofrece beneficios significativos a los negocios. Al adherirse a estas normativas, las empresas pueden reducir el riesgo de sanciones financieras y daños a su reputación derivados de posibles violaciones de datos. Asimismo, pueden mejorar la confianza y lealtad de sus clientes, quienes se sentirán más seguros al saber que su información personal está protegida.

En conclusión, la nueva legislación en materia de protección de datos representa un avance significativo hacia la creación de un entorno digital más seguro y confiable. Para los comercios, comprender y cumplir con estas normativas es esencial no solo para evitar sanciones legales, sino también para fortalecer la relación con sus clientes y adaptarse a un mercado cada vez más centrado en la privacidad y la seguridad de los datos.

2. Las claves de la nueva legislación para el comercio.

El RGPD introduce una serie de obligaciones y principios fundamentales que las empresas del sector minorista deben cumplir a la hora de recopilar, almacenar, utilizar y compartir datos personales de sus clientes. Entre los aspectos más relevantes se encuentran:

- **Principio de licitud, lealtad y transparencia:** los datos personales deben ser tratados de forma lícita, con lealtad y de manera transparente para el interesado.
- **Principio de limitación de finalidades:** los datos personales deben ser recogidos para finalidades determinadas, explícitas y legítimas, y no podrán ser tratados con posterioridad de modo incompatible con dichas finalidades.
- **Principio de minimización de datos:** los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Principio de exactitud:** los datos personales deben ser exactos y, en caso necesario, actualizados.
- **Principio de limitación del plazo de conservación:** los datos personales deben conservarse durante un período no superior al necesario para los fines para los que son tratados.
- **Principio de integridad y confidencialidad:** los datos personales deben ser tratados de forma que garantice su seguridad adecuada, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.
- **Principio de responsabilidad:** el responsable del tratamiento debe ser capaz de demostrar el cumplimiento de los principios anteriormente mencionados.

Cumplimiento del RGPD: Un reto y una oportunidad para el comercio minorista

El cumplimiento del RGPD representa un reto importante para las empresas del sector minorista, que deben adaptar sus prácticas de tratamiento de datos a las nuevas exigencias legales. Sin embargo, también representa una oportunidad para mejorar la confianza de los clientes, fortalecer la seguridad de la información y generar un valor diferencial en un mercado cada vez más competitivo.

Para cumplir con el RGPD, las empresas del sector minorista deben implementar una serie de medidas, como:

- **Designar un Delegado de Protección de Datos (DPO):** un profesional con conocimientos específicos en materia de protección de datos que será responsable de supervisar el cumplimiento del RGPD en la empresa.

- **Realizar una Evaluación de Impacto en la Protección de Datos (EIPD):** un análisis de los riesgos que el tratamiento de datos personales puede suponer para los derechos y libertades de las personas físicas.
- **Implementar medidas de seguridad técnicas y organizativas adecuadas:** para proteger los datos personales frente a accesos no autorizados, alteraciones, pérdida o destrucción.
- **Establecer mecanismos para el ejercicio de los derechos de los interesados:** acceso, rectificación, supresión, limitación del tratamiento, oposición al tratamiento y portabilidad de los datos.
- **Formar y concienciar a los empleados en materia de protección de datos.**

3. Certificados de protección de datos para el comercio.

En el actual entorno digital, donde la protección de datos personales es una prioridad tanto para consumidores como para reguladores, los certificados en materia de protección de datos se han convertido en herramientas esenciales para los comercios. Estos certificados no solo demuestran el compromiso de una empresa con la seguridad y privacidad de la información, sino que también ayudan a cumplir con las normativas legales y a ganar la confianza de los clientes. A continuación, se detallan los principales certificados en materia de protección de datos que son necesarios para el comercio.

ISO/IEC 27001

La ISO/IEC 27001 es una de las certificaciones más reconocidas a nivel mundial en la gestión de la seguridad de la información. Esta norma proporciona un marco para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). La certificación ISO/IEC 27001 asegura que una empresa ha adoptado las mejores prácticas para proteger la confidencialidad, integridad y disponibilidad de los datos.

Para los comercios, obtener esta certificación significa que han implementado medidas de seguridad robustas y procesos de gestión del riesgo que protegen la información sensible, incluyendo los datos

personales de los clientes. La certificación también implica la realización de auditorías periódicas para asegurar que el sistema de gestión de seguridad de la información se mantiene actualizado y efectivo.

ISO/IEC 27701

La ISO/IEC 27701 es una extensión de la ISO/IEC 27001, específicamente centrada en la gestión de la privacidad de la información. Este estándar proporciona directrices para establecer, implementar, mantener y mejorar un sistema de gestión de información de privacidad (PIMS). La certificación ISO/IEC 27701 ayuda a las organizaciones a cumplir con los requisitos de privacidad y protección de datos establecidos en regulaciones como el RGPD y la LGPD.

Para los comercios, esta certificación es particularmente valiosa porque demuestra que no solo se están protegiendo los datos, sino que también se están gestionando de acuerdo con los principios de privacidad. Esto incluye la recopilación, almacenamiento, uso y eliminación de datos personales de manera responsable y transparente.

Certificación PCI DSS

La Payment Card Industry Data Security Standard (PCI DSS) es una certificación esencial para cualquier comercio que procese, almacene o transmita información de tarjetas de crédito. Este estándar de seguridad es mantenido por el PCI Security Standards Council y tiene como objetivo proteger los datos del titular de la tarjeta y asegurar que las transacciones con tarjetas de crédito se realicen de manera segura.

Para los comercios, la certificación PCI DSS implica cumplir con una serie de requisitos de seguridad, como la instalación y mantenimiento de una configuración de firewall para proteger los datos del titular de la tarjeta, la encriptación de la transmisión de datos sensibles, y la implementación de medidas de control de acceso estrictas. Cumplir con el PCI DSS no solo protege a los clientes contra el fraude con tarjetas de crédito, sino que también evita sanciones financieras y pérdidas de reputación para el negocio.

Certificado de Conformidad con el RGPD

El **Reglamento General de Protección de Datos (RGPD) de la Unión Europea establece que las organizaciones pueden optar por obtener certificaciones de conformidad con el RGPD como un medio para demostrar su cumplimiento con las normativas de protección de datos**. Aunque el RGPD no especifica un estándar de certificación en particular, varias organizaciones y entidades certificadoras ofrecen

programas que ayudan a las empresas a alinearse con los requisitos del RGPD.

Obtener una certificación de conformidad con el RGPD puede ser beneficioso para los comercios, ya que proporciona una garantía adicional a los clientes de que su información personal se gestiona de acuerdo con los estándares de privacidad más estrictos. Además, estas certificaciones pueden facilitar la demostración de cumplimiento durante las auditorías y en caso de inspecciones por parte de las autoridades de protección de datos.

Certificación CSA STAR

La Certificación de Seguridad, Confianza y Aseguramiento de la CSA (Cloud Security Alliance) STAR (Security, Trust & Assurance Registry) es un programa específico para proveedores de servicios en la nube. Este programa combina los requisitos de la norma ISO/IEC 27001 con los criterios adicionales de la CSA para asegurar la protección de los datos en entornos de nube.

Para los comercios que utilizan servicios en la nube para gestionar datos de clientes, la certificación CSA STAR puede proporcionar una capa adicional de confianza en la seguridad y privacidad de los datos. Esta certificación demuestra que el proveedor de servicios en la nube ha implementado medidas de seguridad avanzadas y ha sido evaluado por una entidad independiente.

En resumen, **los certificados en materia de protección de datos son herramientas fundamentales para que los comercios aseguren la protección de la información personal de sus clientes y cumplan con las normativas legales**. La obtención de certificaciones como ISO/IEC 27001, ISO/IEC 27701, PCI DSS, conformidad con el RGPD y CSA STAR no solo mejora la seguridad de los datos, sino que también fortalece la confianza de los clientes y proporciona una ventaja competitiva en el mercado. Al invertir en estas certificaciones, los comercios pueden demostrar su compromiso con la privacidad y la protección de datos, asegurando un entorno digital más seguro y confiable para todos.