Vol. 1 Edición 12- Mayo 2023

IN SOLIDUM Social

Reflexionando sobre cinco años de RGPD: logros, desafíos y la relevancia de la protección de datos

WWW.INSOLIDUMABOGADOS.COM

Introducción

Por Mgtr. José Ramírez

La fecha del 25 de mayo marca un hito importante en el mundo de la privacidad y protección de datos, ya que conmemoramos el quinto aniversario de la entrada en vigor del Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Este marco legal, que establece nuevas normas para el manejo y procesamiento de los datos personales de los ciudadanos de la UE, ha tenido un impacto significativo en organizaciones en todo el mundo, cambiando la forma en que interactúan con los datos personales y cómo se protegen estos activos digitales valiosos.

Este reglamento es un ejemplo de lo que una legislación bien elaborada puede hacer para proteger los derechos de los ciudadanos y cómo puede influir en la forma en que las empresas operan en su día a día. Sin embargo, a pesar de su importancia, la plena comprensión y aplicación del RGPD sigue siendo un desafío para muchas organizaciones.

Este artículo se centra en proporcionar una visión general de las noticias y desarrollos más relevantes en relación con el RGPD en su quinto aniversario, aportando una perspectiva jurídica sobre su impacto en el panorama global de protección de datos.

A lo largo de este artículo, se presentará un análisis jurídico de los controles que el RGPD ejerce sobre la protección de datos de los usuarios en la comunidad europea.

Es fundamental comprender el alcance extraterritorial de la norma, ya que se aplica no solo a las organizaciones establecidas en la UE, sino también a aquellas fuera de la UE que procesan los datos personales de los ciudadanos de la UE. Además, se examinará la rigurosidad de las sanciones impuestas por incumplimientos del RGPD, que han llegado a alcanzar millones de euros para las grandes empresas multinacionales.

Además, este artículo también se centrará en los desafíos y consideraciones prácticas para el cumplimiento del RGPD. Se explorará cómo las empresas pueden adecuarse a las normas del RGPD y cuáles son las mejores prácticas recomendadas para mantenerse en conformidad.

Finalmente, se presentarán casos y sanciones ejemplares del RGPD, proporcionando un análisis jurídico de algunos de los fallos más destacados. Estos casos no solo sirven como advertencia sobre las posibles consecuencias del incumplimiento, sino que también brindan información útil sobre cómo se aplica el reglamento en diferentes contextos y situaciones.

Noticias y desarrollos relevantes

Este mes marca el quinto aniversario del Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Esta normativa, que entró en vigor el 25 de mayo de 2018, ha transformado el panorama de la privacidad y protección de datos en todo el mundo, introduciendo cambios significativos en la forma en que las organizaciones recopilan, procesan y almacenan los datos personales de los individuos (El Español, 2023).

El RGPD se ha convertido en el estándar de oro para la protección de datos, y sus principios y prácticas han sido adoptados por varias jurisdicciones fuera de la UE. En su quinto aniversario, es oportuno destacar las últimas noticias y desarrollos relacionados con esta influyente normativa.

Desde su implementación, el RGPD ha ejercido un fuerte control sobre cómo las empresas manejan los datos personales, con el objetivo de garantizar que se respeten los derechos y libertades fundamentales de las personas. En particular, el RGPD ha impuesto sanciones significativas a las empresas que no cumplen con sus requisitos. Cinco Días (2023) informa que las multas impuestas en el marco del RGPD han alcanzado los 1.000 millones de euros en todo el mundo. Entre los casos de mayor envergadura se encuentran las sanciones impuestas a grandes empresas tecnológicas como Meta, Google y Amazon.

El RGPD ha impulsado el cambio hacia una mayor transparencia y responsabilidad en el

tratamiento de los datos personales. Los titulares de los datos tienen ahora más control sobre sus propios datos y las empresas están obligadas a ser más transparentes en sus prácticas de tratamiento de datos (El Español, 2023).

Además, Business Insider (2023) informa que, a pesar del aumento de la conciencia y el cumplimiento, aún persisten desafíos significativos. Las empresas continúan enfrentándose a dificultades para interpretar y aplicar las complejas disposiciones del RGPD. La norma, aunque esencial para la protección de la privacidad, es amplia y requiere una interpretación y aplicación cuidadosas.

El RGPD también ha dado lugar a una serie de sentencias judiciales que han ayudado a esclarecer sus disposiciones. Entre ellas se encuentran las decisiones del Tribunal de Justicia de la Unión Europea en los casos "Schrems II" y "La Quadrature du Net", que han tenido un impacto significativo en las transferencias internacionales de datos y la vigilancia gubernamental, respectivamente.

En cuanto a los desarrollos recientes, Cinco Días (2023) informa sobre un informe de la Agencia de Derechos Fundamentales de la UE que señala que, a pesar de los esfuerzos para implementar el RGPD, aún existe una brecha entre la norma y su aplicación práctica. Según el informe, a pesar de los avances en la concienciación y el cumplimiento, los ciudadanos siguen encontrando dificultades para ejercer sus derechos en virtud del RGPD.

Análisis jurídico

El RGPD, con su enfoque de protección de datos personales centrado en los derechos del individuo, ha marcado un hito en la legislación mundial de privacidad. A cinco años de su entrada en vigencia, es evidente que la normativa ha creado un nuevo estándar para la protección de datos personales, que ha tenido un impacto global.

La territorialidad y la extraterritorialidad son dos principios fundamentales del RGPD. Aunque la normativa se aplica principalmente a las empresas y organizaciones establecidas en la UE, su alcance se extiende más allá de las fronteras de la Unión. El RGPD tiene un impacto significativo en las empresas fuera de la UE que ofrecen bienes o servicios a individuos en la UE, o que monitorean su comportamiento. Este principio de extraterritorialidad ha puesto de relieve la importancia de tener políticas y prácticas de protección de datos que cumplan con el RGPD, independientemente de la ubicación geográfica de la empresa.

Las sanciones impuestas en virtud del RGPD han demostrado ser una herramienta efectiva para garantizar el cumplimiento de la normativa. El RGPD ha establecido un régimen de sanciones estricto, con multas de hasta el 4% de la facturación global anual de la empresa, o 20 millones de euros, lo que sea mayor. Esta estructura de sanciones ha generado un cambio significativo en la forma en que las empresas manejan los datos personales y ha llevado a un aumento del cumplimiento del RGPD en todo el mundo.

El RGPD también ha influido en la formación de otras leyes de protección de datos alrededor del mundo. Por ejemplo, la Ley de Privacidad del Consumidor de California (CCPA) y la Ley General de Protección de Datos de Brasil (LGPD) se han inspirado en muchos aspectos del RGPD. La influencia del RGPD se extiende más allá de la protección de datos, impactando en otros aspectos de la gobernanza corporativa, incluyendo la ética empresarial y la responsabilidad social corporativa.

A medida que el RGPD entra en su sexto año, es probable que veamos más desarrollos y cambios en la legislación de protección de datos en todo el mundo. Las empresas deben estar atentas a estos cambios y asegurarse de que sus prácticas de protección de datos estén en línea con las normativas más recientes y relevantes.

Sin embargo, a pesar de los desafíos que presenta el cumplimiento con el RGPD, la normativa ofrece una oportunidad para que las empresas demuestren su compromiso con la protección de los datos personales de sus clientes, mejorando así su reputación y fortaleciendo su posición en el mercado.

¿Cómo cumplir con el RGPD?

Cumplir con el Reglamento General de Protección de Datos (RGPD) es un desafío significativo, especialmente para las organizaciones que manejan grandes cantidades de datos personales. El RGPD impone una serie de requisitos estrictos a las empresas en términos de cómo recopilan, almacenan y usan los datos personales. Aquí hay una guía más detallada para el cumplimiento del RGPD.

1. Conciencia y educación:

El primer paso crucial en el camino hacia el cumplimiento del RGPD es la conciencia y la educación. Todos los miembros de su organización que manejan datos personales deben entender completamente las implicaciones del RGPD y las responsabilidades que conlleva. Esto no sólo incluye a los gerentes y ejecutivos, sino también a los empleados que tienen acceso regular a los datos personales. Puede ser útil organizar seminarios o sesiones de formación en profundidad para asegurarse de que todos comprenden la importancia del cumplimiento del RGPD y los riesgos de no cumplir con las normas.

2. Auditoría de datos:

Una vez que todo el mundo en su organización entiende el significado del RGPD, el siguiente paso es llevar a cabo una auditoría completa de los datos personales que maneja su empresa. Deberá conocer exactamente qué tipos de datos está recogiendo, por qué los está recogiendo, cómo los está utilizando, quién tiene acceso a ellos y dónde se almacenan. Una auditoría

de datos no sólo le dará una visión completa de cómo se manejan los datos en su empresa, sino que también es un requisito clave del RGPD para demostrar la responsabilidad.

3. Políticas y procedimientos:

El RGPD exige que las organizaciones establezcan políticas y procedimientos claros para el manejo de los datos personales. Estas políticas deben abarcar todo, desde el consentimiento del usuario hasta la seguridad de los datos y la respuesta a las violaciones de datos. También deben ser accesibles y comprensibles para todos los miembros de su organización.

4. Derechos de los interesados:

Una parte esencial del RGPD es que otorga a los individuos ciertos derechos sobre sus datos personales. Estos derechos incluyen el derecho a ser informado, el derecho de acceso, el derecho a la rectificación, el derecho al olvido, el derecho a restringir el procesamiento, el derecho a la portabilidad de los datos, el derecho a objetar y el derecho a no ser objeto de decisiones automatizadas, incluida la elaboración de perfiles. Es crucial que su organización tenga sistemas en vigor para permitir que los individuos ejerzan estos derechos.

5. Designación de un Delegado de Protección de Datos (DPD):

Algunas organizaciones estarán obligadas a nombrar a un Delegado de Protección de Datos (DPD) según el RGPD. El DPD actúa como el enlace entre la organización y cualquier Autoridad de Control que supervisa su cumplimiento del RGPD, además de ser el punto de contacto para los interesados que

quieran ejercer sus derechos en virtud del RGPD. La designación de un DPD es una medida clave para demostrar el cumplimiento del RGPD.

6. Evaluación de Impacto de Protección de Datos (EIPD):

Una Evaluación de Impacto de Protección de Datos (EIPD) es otro requisito para ciertas organizaciones bajo el RGPD. La EIPD es un proceso para ayudar a identificar y minimizar los riesgos de protección de datos de un proyecto. Se necesita realizar una EIPD cuando se planea procesar datos personales que podrían resultar en un alto riesgo para los derechos y libertades de los individuos.

7. Seguridad de los datos:

El RGPD impone estrictas obligaciones en términos de seguridad de los datos. Las organizaciones deben garantizar que tienen las medidas de seguridad adecuadas para proteger los datos personales que manejan. Esto puede incluir encriptación, anonimización y garantizar la confidencialidad, integridad, disponibilidad y resistencia de los sistemas de procesamiento.

8. Notificación de violaciones de datos:

Bajo el RGPD, las organizaciones están obligadas a informar a la Autoridad de Control de cualquier violación de datos que pueda resultar en un riesgo para los derechos y libertades de los individuos. Esta notificación debe realizarse dentro de las 72 horas posteriores a tener conocimiento de la violación. Los individuos afectados también deben ser notificados si la violación es probable que resulte en un alto riesgo para sus derechos y libertades.

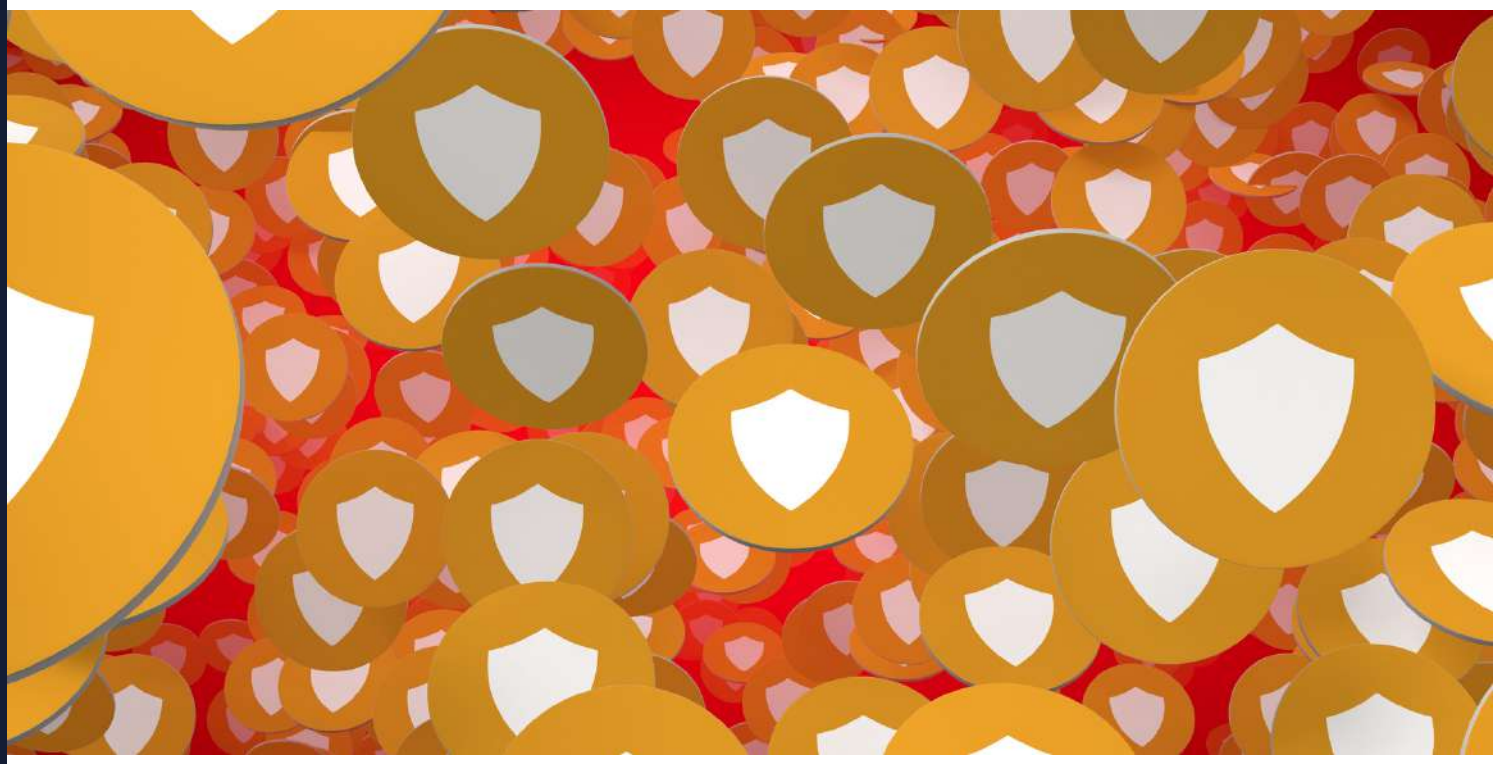
9. Transferencias internacionales de datos:

El RGPD también establece restricciones sobre la transferencia de datos personales fuera de la Unión Europea. Las organizaciones deben garantizar que las transferencias de datos a países fuera de la UE cumplan con los requisitos del RGPD. Esto puede implicar la utilización de cláusulas contractuales estándar u otros mecanismos de transferencia de datos aprobados por la UE.

10. Continua revisión y actualización:

El cumplimiento del RGPD no es un hecho único. Las organizaciones deben revisar y actualizar regularmente sus políticas y procedimientos de protección de datos para garantizar su cumplimiento continuo. También es importante mantenerse al tanto de cualquier cambio o actualización en la legislación de protección de datos.

La implementación de estos pasos puede parecer una tarea desalentadora, pero el incumplimiento de las regulaciones del RGPD puede resultar en sanciones severas. Así que es mejor abordar estos requisitos con un plan bien pensado y detallado.



Casos y sanciones ejemplares por el RGPD

A lo largo de los años, el RGPD ha tenido un impacto significativo en cómo las organizaciones manejan los datos personales de los individuos. Sin embargo, no todas las organizaciones han logrado cumplir con sus obligaciones. Algunas infracciones han sido tan graves que los reguladores han impuesto multas significativas. Veamos algunos de los casos más relevantes.

1. Google LLC - Francia (50 millones de euros):

Google fue multada por la CNIL, la autoridad de protección de datos de Francia, por no proporcionar a los usuarios una información transparente y comprensible sobre el uso de sus datos. Además, Google no obtuvo un consentimiento válido para la personalización de sus anuncios.

2. TIM - Italia (27,8 millones de euros):

La autoridad italiana de protección de datos multó a TIM por realizar actividades de marketing y publicidad sin el consentimiento de los usuarios. También señalaron que la empresa no implementó medidas adecuadas para garantizar la protección de los datos.

3. British Airways - Reino Unido (22 millones de euros):

British Airways fue multada por la ICO, la autoridad británica de protección de datos, después de que los datos de reserva de más de 400,000 clientes fueran robados por ciberatacantes debido a la falta de medidas de seguridad adecuadas.

4. Marriott International - Reino Unido (20,45 millones de euros):

Marriott International fue multada por la ICO después de un ciberataque que expuso los datos de 339 millones de huéspedes. La ICO determinó que Marriott no había realizado la debida diligencia cuando adquirió Starwood Hotels y no había protegido adecuadamente los datos de sus clientes.

5. Wind Tre SpA - Italia (16,7 millones de euros):

Wind Tre fue multada por la autoridad italiana de protección de datos por violar varios artículos del RGPD, incluyendo la falta de consentimiento y la violación de las medidas de seguridad de los datos.

6. Deutsche Wohnen SE - Alemania (14,5 millones de euros):

Deutsche Wohnen fue multada por la autoridad alemana de protección de datos por retener datos personales sin tener una razón legítima para hacerlo y por no tener medidas de seguridad adecuadas.

7. 1&1 Telecom GmbH - Alemania (9,55 millones de euros):

1&1 Telecom fue multada por la autoridad alemana de protección de datos por no tener suficientes medidas técnicas y organizativas para prevenir el acceso no autorizado a los datos personales de los clientes. Este caso es particularmente interesante porque ilustra la importancia de las medidas de seguridad en todos los niveles de las operaciones de una empresa. En este caso, la falta de seguridad

en la identificación de los clientes durante las llamadas de servicio al cliente resultó en la violación de la protección de datos. De acuerdo con el RGPD, es esencial garantizar que sólo las personas autorizadas tengan acceso a los datos personales y que este acceso esté debidamente registrado y controlado. Por lo tanto, este caso subraya la importancia de las medidas de seguridad adecuadas y proporciona un buen ejemplo de cómo se pueden aplicar las sanciones del RGPD.

8. Österreichische Post AG - Austria (18 millones de euros):

La autoridad austriaca de protección de datos multó a Österreichische Post, la empresa de correos de Austria, por procesar datos personales más allá de lo necesario para la ejecución de sus contratos postales. La empresa había creado perfiles de más de tres millones de austríacos, incluyendo su afinidad política.

9. H&M Hennes & Mauritz Online Shop A.B. & Co. KG - Alemania (35,2 millones de euros):

H&M fue multada por el supervisor de protección de datos de Hamburgo por mantener un extenso registro de datos personales de los empleados de su servicio al cliente. Los datos incluían información sobre la vida privada de los empleados, lo que constituía una grave infracción del RGPD.

10. Google - Francia (100 millones de euros) y Amazon - Francia (35 millones de euros):

En diciembre de 2020, la CNIL impuso dos multas significativas a Google y Amazon por incumplir las normas del RGPD en relación

con el uso de cookies. A Google se le impuso una multa de 100 millones de euros y a Amazon una multa de 35 millones de euros por colocar cookies en los ordenadores de los usuarios sin obtener su consentimiento previo y por no proporcionar suficiente información a los usuarios sobre el uso de cookies.

Estos casos destacan la importancia del cumplimiento del RGPD y muestran el enfoque proactivo de los reguladores en la protección de los derechos de los individuos. Cada uno de ellos nos enseña lecciones valiosas sobre los diferentes aspectos del RGPD, desde la obtención del consentimiento hasta la implementación de medidas de seguridad adecuadas. Y quizás lo más importante es que demuestran la disposición de las autoridades de protección de datos para hacer uso de sus poderes de sanción para asegurar el cumplimiento de las reglas del RGPD.

Por último, pero no menos importante, estas sanciones ejemplares deberían ser un recordatorio para todas las organizaciones de la importancia de invertir en un cumplimiento adecuado de la protección de datos. Los riesgos de no hacerlo, como se puede ver, pueden ser muy costosos.

Conclusiones

Al reflexionar sobre los últimos cinco años desde la entrada en vigor del RGPD, es evidente que la normativa ha tenido un impacto significativo en la forma en que las organizaciones manejan los datos personales. No solo ha transformado las prácticas de tratamiento de datos dentro de la UE, sino que ha establecido un nuevo estándar global para la privacidad y la protección de datos.

El alcance extraterritorial del RGPD ha permitido que la normativa influya en la formación de legislaciones de protección de datos en todo el mundo. Las empresas en todas las jurisdicciones deben estar atentas a los requisitos del RGPD, especialmente si tratan con datos personales de individuos en la UE.

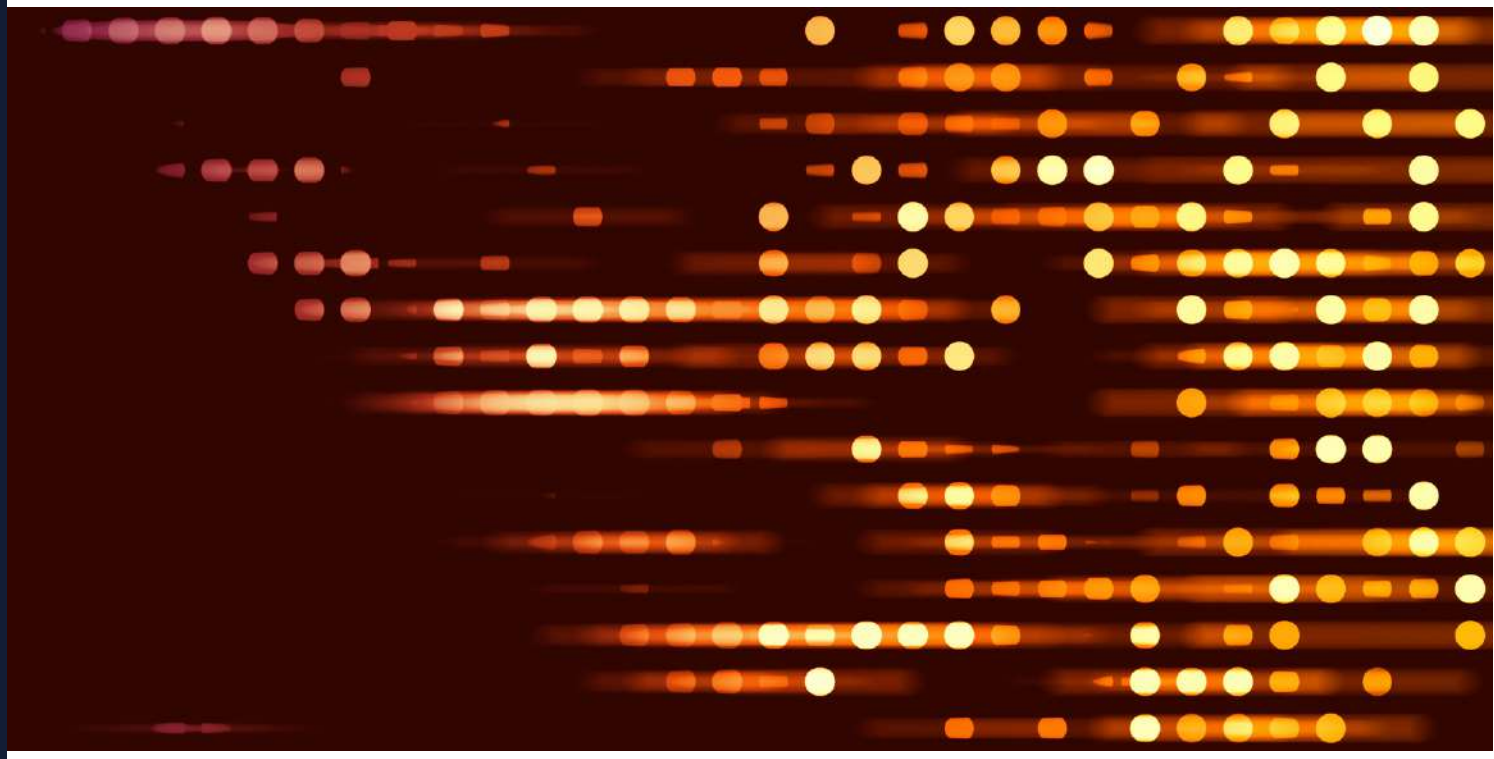
El régimen de sanciones del RGPD ha demostrado ser una herramienta efectiva para garantizar el cumplimiento de la normativa. Sin embargo, el cumplimiento del RGPD no debe verse simplemente como un medio para evitar sanciones. Cumplir con el RGPD ofrece a las empresas la oportunidad de demostrar su compromiso con la protección de los datos personales, lo que puede fortalecer la confianza de los clientes y mejorar la reputación de la empresa.

Aunque ha habido avances significativos en la conciencia y el cumplimiento del RGPD en los últimos cinco años, todavía hay desafíos por superar. La interpretación y aplicación de las complejas disposiciones del RGPD puede ser difícil, y muchas empresas todavía tienen dificultades para cumplir plenamente con la normativa.

A medida que el RGPD entra en su sexto año, es probable que veamos más cambios y desarrollos en la legislación de protección de datos en todo el mundo. Las empresas deben estar preparadas para adaptarse a estos cambios y asegurarse de que sus prácticas de protección de datos están en línea con las normativas más recientes y relevantes.

Referencias

- El Español. (2023). El Reglamento General de Protección de Datos: una energía para socavarlo o cumplirlo. Recuperado de https://www.elespanol.com/invertia/disruptores-innovadores/politica-digital/europa/20230524/reglamento-general-proteccion-datos-energia-socavarlo-cumplirlo/766173378_0.html
- Cinco Días. (2023). Cinco años de GDPR: más de 1.000 millones de euros en multas y aún queda mucho por hacer. Recuperado de https://cincodias.elpais.com/cincodias/2023/05/24/legal/1684951388_163332.html
- Business Insider España. (2023). Los desafíos del RGPD, 5 años después de su entrada en vigor. Recuperado de https://www.businessinsider.es/desafios-rgpd-5-anos-despues-entrada-vigor-1248034
- PowerData. (2023). GDPR - Protección de Datos. Recuperado de https://www.powerdata.es/gdpr-proteccion-datos
- Web Cvent. (2023). 5 Years of GDPR: The Lessons Learned and The Road Ahead. Recuperado de https://web.cvent.com/event/6aecfda0-8303-458b-8b8e-1af11989a535/summary



- CNIL. (2019). Decision SAN-2019-001. Retrieved from https://www.cnil.fr/fr/la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-google-llc
- Italian Data Protection Authority. (2019). Decision No. 9418. Retrieved from https://www.garanteprivacy.it/home/diritti/diritto-di-accesso-a-propri-dati-personali
- ICO. (2020). Decision of 16 October. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/
- ICO. (2020). Decision of 30 October. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/marriott-international-inc-fined-18-4million-for-failing-to-keep-customers-personal-data-secure/
- Italian Data Protection Authority. (2019). Decision No. 159. Retrieved from https://www.garanteprivacy.it/home/diritti/diritto-di-accesso-a-propri-dati-personali
- Berlin Commissioner for Data Protection and Freedom of Information. (2019). Decision of 30 October. Retrieved from https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2019-BlnBDI-Hinweise_zur_DS-GVO_fuer_Wahlvorstaende.pdf
- Federal Commissioner for Data Protection and Freedom of Information. (2019). Decision of 9 December. Retrieved from https://www.bfdi.bund.de/SharedDocs/Publikationen/Entscheidungssammlung/DSB_Sachsen_Zweckbindung_Telekommunikation.html

- Austrian Data Protection Authority. (2018). Decision DSB-D123.270/0005-DSB. Retrieved from https://www.data-protection-authority.gv.at/
- Hamburg Commissioner for Data Protection and Freedom of Information. (2020). Decision 3/2019. Retrieved from https://datenschutz-hamburg.de/news/detail/id/12020/name/Datenschutzpanne+bei+H%26M+%96+Bu%C3%9Fgeld+in+H%C3%B6he+von+35%2C258%2C708%2C95+Euro
- CNIL. (2020). Decision SAN-2020-012 and SAN-2020-013. Retrieved from https://www.cnil.fr/fr/la-cnil-prononce-deux-sanctions-de-3-millions-et-600-000-euros-lencontre-de-carrefour-banque