GUÍA PRÁCTICA ADAPTACIÓN REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

iab.spain

iab spain

1. Concienciación
2. Revisión y documentación de la ruta de cumplimiento
3. Legitimación para tratar datos personales
4. Consentimiento
5. Seudonimización
6. Políticas de Privacidad
7. Elaboración de perfiles
8. Derechos de los individuos
9. Responsables y encargados del tratamiento
10. Brechas de seguridad
11. Privacidad desde el diseño y evaluación de impacto sobre la privacidad
12. Delegado de Protección de Datos
13. Autoridad competente
14. Transferencias Internacionales

Sobre IAB Spain

IAB es la asociación que representa al sector de la publicidad en medios digitales en España y engloba a los diferentes actores del panorama publicitario online: agencias de medios, agencias creativas, anunciantes, soportes, redes, empresas de mobile marketing, de vídeo, de e-mail marketing, digital signage, buscadores, consultoras, observadores, medios de comunicación y proveedores tecnológicos.

El fin de IAB Spain, que en la actualidad cuenta con más de 200 empresas asociadas, se centra en impulsar el desarrollo de la publicidad, el marketing y la comunicación digital en España.

Contacto

- **Paula Ortiz**- Directora Jurídica y de Relaciones Institucionales IAB Spain (paula@iabspain.es)

- **María Torres**- Responsable de comunicación IAB Spain (comunicacion@iabspain.es)

- www.iabspain.es

- http://iabspain.es/policy-legal/

Introducción

El 25 de mayo de 2018 comenzará a ser de aplicación el Reglamento General de Protección de Datos (en adelante, RGPD) a todas las empresas, establecidas o no en la Unión Europea, que tratan datos personales de personas residentes en Europa en la Unión Europea, sustituyendo la Ley Orgánica de Protección de Datos del año 1999. Desde IAB Spain hemos ido publicando documentos para ayudar a comprender a nuestros asociados lo que la nueva norma significa para sus negocios. Sin embargo, asesorar a las empresas sobre los procesos concretos que han de implantar para cumplir con el RGPD ha sido una tarea mucho más difícil.

El RGPD es un texto ambiguo y está lleno de áreas grises que podrían tener consecuencias de gran alcance para nuestra industria. Si bien muchos de los conceptos y principios del RGPD son parecidos a la norma actual (y por tanto, si estás cumpliendo ahora, es un muy buen punto de partida) el RGPD introduce nuevos elementos, que suponen nuevas obligaciones.obligaciones y nuevos retos. La fecha de aplicación del RGPD se aproxima, y todavía hay muchas cuestiones en el aire. No obstante cada día van apareciendo nuevas orientaciones de las autoridades de control que facilitarán la labor de acometer las modificaciones necesarias en aras al cumplimiento de la nueva norma.

Con esta guía pretendemos ayudar en la ruta de cumplimiento a la industria de la publicidad digital. Es un documento dinámico, y se irá actualizando con las nuevas orientaciones. Para estar al tanto de las futuras versiones, puedes inscribirte en nuestro newsletter legal, escribiendo a comunicacion@iabspain.es

Además, la Agencia Española de Protección de Datos tiene una sección con documentos, orientaciones y directrices que pueden ser de tu interés para adaptarte y entender mejor las novedades y consecuencias del RGPD. Puedes consultarla aquí.

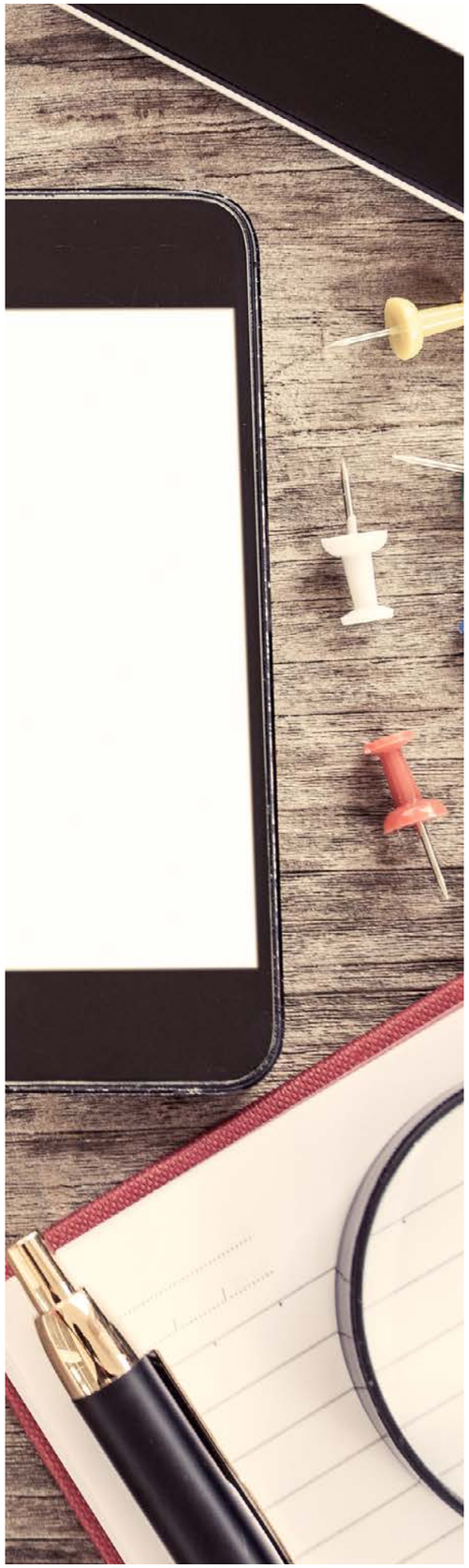
1. Concienciación

El RGPD introduce importantes multas de hasta un 4% de la facturación global anual o 20 millones de euros-. Pero esta no es la única razón por la que los responsables de las organizaciones deben estar al tanto de la nueva norma. Algunos procesos - y quizás incluso productos- tendrán que cambiar como resultado de la aplicación del RGPD. Para muchos negocios de publicidad digital, por vez primera será necesario cumplir con las normas de protección de datos.

Desde IAB Spain recomendamos que reúnas a diferentes departamentos para informarles y concienciarles sobre el Reglamento y que elabores un plan de cumplimiento que incluya a miembros de todos los departamentos pertinentes. También hay que tener en cuenta que el RGPD se aplicará a todas las empresas que hacen negocios en la Unión Europea, así que asegúrate de que tus colegas en el extranjero – en particular los ubicados en EE.UU. – cumplen con la normativa.

2. Revisión y documentación de la ruta de cumplimiento

Uno de los pilares sobre los que se basa el RGPD es el “principio de responsabilidad proactiva”[1], siendo el hilo conductor de todo el RGPD. La clave para satisfacer este principio es documentar los tratamientos de datos personales que llevas a cabo e identificar las áreas de riesgo.
Este sería el primer paso por el que deberíamos empezar e implica hacer un inventario de todas las actividades de tratamiento que llevas a cabo en tu compañía. Qué datos tienes, de dónde vienen, con quién los compartes. Esto es importante no sólo para conocer con precisión qué datos estás tratando, sino también cómo los estás tratando. Además, el proceso de revisión puede revelar que algún tratamiento requiere precauciones adicionales (por ejemplo, si es de aplicación la disposición sobre elaboración de perfiles). Una buena manera de abordar esta tarea es formar un grupo de trabajo dentro de la empresa, con representación de los distintos departamentos. No recomendamos que esta labor sea realizada únicamente por el equipo legal, el delegado de protección de datos o el equipo de IT. Comprender todos los procesos es clave. Para ello, mantener entrevistas con empleados de todos los departamentos - y potencialmente con proveedores y socios - te permitirá identificar qué tipo de tratamientos de datos se llevan a cabo en la empresa.



[1] Responsable de cumplir con los principios del Reglamento y capaz de demostrarlo

Elementos a documentar en tus tratamientos de datos

Todas las actividades de tratamientos de datos deben ser revisadas y documentadas identificando “cuando, por qué y quién” realizando un análisis de riesgo en cada tratamiento. También incluye los datos de empleados. A modo de ejemplo, algunas de las preguntas que tenemos que hacernos son las siguientes:

- ¿Qué información doy en la recogida de datos?
- ¿Dónde, cuándo y por qué trato los datos?
- ¿Tengo un fundamento jurídico para tratarlos?,
- ¿Estoy aplicando los principios del tratamiento de datos?
- ¿Qué datos se anonimizan, qué datos se seudonimizan?
- ¿Por cuánto tiempo almaceno estos datos?
- ¿Con quién comparto estos datos?
- ¿Cuál es el nivel de riesgo por tratamiento?
- ¿En qué casos soy el responsable del tratamiento, el encargado o comparto la responsabilidad?
- ¿Estoy tratando los datos por razones de seguridad?
- ¿Estoy transfiriendo datos fuera de la UE?
- ¿Pido el consentimiento solo para mi empresa o para terceros?
- ¿He revisado y documentado los procesos de seguridad? Según el RGPD, las violaciones de seguridad de los datos deben ser notificadas a la Autoridad de Protección de Datos dentro de las 72 horas siguientes a la infracción. Si todavía no tienes un plan para esto, es necesario crearlo. Considera la posibilidad de crear una plantilla para enviar esta información.

Recuerda que la definición de datos personales incluidos en el RGPD incluye también el “número de identificación, datos de localización, un identificador en línea”. Esto es importante porque algunos elementos que se utilizan en la práctica en publicidad digital y a los que actualmente no se aplicaba la legislación de protección de datos, ahora entrarán dentro del ámbito de aplicación de la normativa. Los identificadores únicos (por ejemplo, ID de cookie o ID de publicidad) pasan a ser datos de carácter personal..

Como tal, quizás sea más fácil para los miembros de IAB Spain tratar todos los identificadores en línea como datos personales, así que asegúrate que conoces las fuentes de esos datos y delimita con quién las compartes. Considera llevar a cabo una auditoría para ayudar con este ejercicio y conocer y metodizar tus tratamientos de datos personales.

3. Legitimación para tratar datos personales

El tratamiento de datos sólo es lícito si se cuenta con una base legal adecuada. El RGPD ofrece seis alternativas:

- Consentimiento
- Contratos
- Cumplimiento de obligación legal
- Proteger los intereses vitales de una persona
- Interés público
- Interés legítimo

Las dos bases jurídicas más utilizadas en la publicidad digital son el consentimiento y el interés legítimo. Como tal, piensa en las diversas formas en que tratas los datos e identifica cuál es la base jurídica que mejor se adapta a los tipos de tratamientos que llevas a cabo. En algunos casos, puede resultarte útil utilizar una combinación de consentimiento e interés legítimo, dependiendo del tipo de tratamiento que desees realizar o si deseas tratar los datos para fines distintos a los inicialmente previstos.

Es importante recordar que bajo la actual Directiva ePrivacy, transpuesta a la LSSI, es necesario solicitar el consentimiento para acceder y/o almacenar información en el dispositivo de un usuario. La Unión Europea está redactando actualmente un Reglamento que viene a sustituir la Directiva sobre ePrivacy, que puede dar lugar a algunos cambios en esos requisitos. Visita la página de Policy de IAB Spain para estar al tanto de las últimas actualizaciones sobre este tema.

4. Consentimiento

El consentimiento desempeña un papel fundamental en el RGPD. Sin embargo, el consentimiento es, como hemos visto, sólo una de las seis bases jurídicas de las que disponen las empresas para tratar los datos personales en algunos casos no es el fundamento jurídico más adecuado.

El RGPD refuerza las condiciones de consentimiento en comparación con la LOPD. El consentimiento tiene que ser libre, específico, informado e inequívoco. Y el consentimiento debe de consistir en una declaración o una clara acción afirmativa, no admitiéndose por tanto el consentimiento tácito. Este es un cambio importante que introduce el RGPD. En algunos casos, el consentimiento habrá de ser explícito, como sucede si el responsable trata los datos para para elaborar perfiles, si trata datos sensibles o si realiza transferencias internacionales de datos. El RGPD establece que el interesado tendrá derecho a retirar su consentimiento en cualquier momento. Para obtener el consentimiento se pueden usar casillas, pero el RGPD establece que las casillas premarcadas o la simple inacción no constituyen una forma válida de prestar el consentimiento. Además, cuando se vayan a utilizar los datos para varias finalidades, se tendrá que recabar el consentimiento para todas ellas.

Si usas el consentimiento como base legal es fundamental poder demostrar que lo has obtenido de forma legal y especialmente si otra organización obtiene el consentimiento en tu nombre.

5. Seudonimización

El RGPD recoge un concepto nuevo, el de seudonimización. La seudonimización es un proceso al que sometemos los datos, por ejemplo, encriptación o hashing, para garantizar que estos ya no están directamente vinculados a un individuo. Los datos personales que no tengan detalles de identificación directa también podrían ser seudónimos en origen. Por ejemplo, un ID de cookie aleatorio que permite que un usuario sea reconocido, pero no identificado directamente.

En cualquier caso, es fundamental tener en cuenta que el RGPD establece que los datos seudonimizados siguen siendo datos personales, y, por tanto, será necesaria una legitimación para tratarlos. Dicho esto, existen beneficios en la seudonimización como medida de privacidad y seguridad, ya que las empresas que seudonimicen los datos, y esta identificación no se pueda revertir (es decir, no se puede reidentificar al interesado) no tienen que cumplir con algunas de las obligaciones del RGPD (por ejemplo, los derechos de los individuos). La seudonimización también puede ayudar a la hora de ponderar nuestro interés legítimo con los intereses y derechos de los afectados, si elegimos esta opción como base para el tratamiento de datos.
La AEPD tiene una guía sobre Orientaciones y garantías en los procedimientos de anonimización de datos personales.

6. Políticas de Privacidad

La transparencia es otro elemento fundamental del RGPD y requiere diferentes niveles de detalle dependiendo de si se obtienen los datos directamente del individuo o no . En todos los casos, el aviso deberá ser conciso, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. También tendrá que incluir la base de legitimación que habilita el tratamiento y explicar cuál es el interés legítimo en el que amparamos el tratamiento de datos personales, si optamos por utilizar esta base legal.

Desde IAB Spain recomendamos que revises ahora tus políticas de privacidad, analices los cambios que necesitas introducir y comiences a redactar esos cambios si aún no lo has hecho. Es clave que toda organización involucrada en la recogida y tratamiento de datos divulgue esta información.

La Agencia Española de Protección de Datos tiene una Guía para el cumplimiento del deber de informar, un documento de gran utilidad y que es un buen punto de partida

7. Elaboración de perfiles

El RGPD recoge el concepto de “elaboración de perfiles” y establece que sólo se podrá llevar a cabo bajo determinadas circunstancias. En ese sentido, establece el derecho de los individuos a “no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar”. El RGPD, como venimos diciendo, establece una serie de bases de legitimaciones para la elaboración de tales perfiles (si lo autoriza una ley, por ejemplo, para fines de prevención de fraude, si es necesario para la ejecución de un contrato entre el interesado y un responsable del tratamiento, o cuando el interesado haya dado su consentimiento, que debe ser explícito) y siempre se debe dar al usuario la posibilidad de oponerse. Respecto a la elaboración de perfiles, el RGPD establece además que se debe prestar atención en evitar posibles consecuencias discriminatorias que puedan surgir debido a criterios sensibles, como raza u origen étnico, opiniones políticas o creencias religiosas, estado de salud u orientación sexual. En cuanto a las obligaciones del responsable, es necesario informar sobre la elaboración de perfiles, la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. Además, en el caso de que lleves a cabo elaboración de perfiles, es necesario llevar a cabo una Evaluación de Impacto de Protección de datos (mira el punto 11).

8. Derechos

El RGPD otorga al titular de los datos una serie de derechos. Estos son:

- El derecho a ser informado (véase el punto 6)
- El derecho de acceso
- El derecho de rectificación
- El derecho a supresión (derecho al olvido)
- El derecho a la limitación del tratamiento
- El derecho a la portabilidad de datos
- El derecho de oposición (derecho a la exclusión voluntaria)
- El derecho a no someterse a la toma de decisiones automatizadas, incluyendo la elaboración de perfiles.

Es necesario que revises todos los procesos para asegurarte de que puedes responder adecuadamente a las solicitudes que puedas recibir. Y recuerda que si seudonimizas los datos, y esta re-identificación no es reversible, se reducirán las obligaciones de dar lugar los derechos de acceso, rectificación, cancelación, limitación del tratamiento y portabilidad, siempre y cuando el individuo no proporcione activamente información adicional para que se le pueda identificar.

9. Responsables y encargados del tratamiento

El RGPD mantiene las nociones de «responsable del tratamiento» y «encargado del tratamiento» que se encuentran en la legislación actual de protección de datos, para distinguir entre las diferentes funciones que desempeñan las organizaciones en el tratamiento de datos personales.

Como recordatorio, los responsables del tratamiento son las organizaciones que deciden - ya sea por sí mismas o conjuntamente con otros responsables - quién y por qué se tratan los datos personales, mientras que los "encargados" actúan en nombre del responsable y siguiendo sus instrucciones. Con las reglas actuales, la carga principal del cumplimiento de la normativa de protección de datos recae sobre el "responsable", no sobre el "encargado".

Pero es importante destacar que el RGPD extiende las obligaciones legales de los encargados. Esto significa que los encargados pueden estar sujetos a control por parte de las autoridades de protección de datos, y pueden recibir cualquier posible multa a partir de mayo de 2018. En virtud del RGPD, las obligaciones para los encargados incluyen:

- Acuerdos - los encargados deben tener un contrato escrito (u otro acto legal) con los responsables. Debe precisarse la duración, la naturaleza y el objeto del tratamiento, el tipo y las categorías de datos personales, así como las obligaciones y los derechos del responsable del tratamiento.

- Seguridad de los datos: los encargados deben adoptar las medidas de seguridad adecuadas e informar a los responsables sin demora injustificada en caso de una violación de datos.
- Sub-encargados: los encargados sólo pueden recurrir a otro encargado con la previa autorización por escrito del responsable. Los proveedores también tendrán que dar al responsable la oportunidad de oponerse ante cualquier cambio en el uso de sub-encargados.

- Instrucciones del responsable: los encargados sólo pueden tratar datos personales de acuerdo con las instrucciones del responsable.

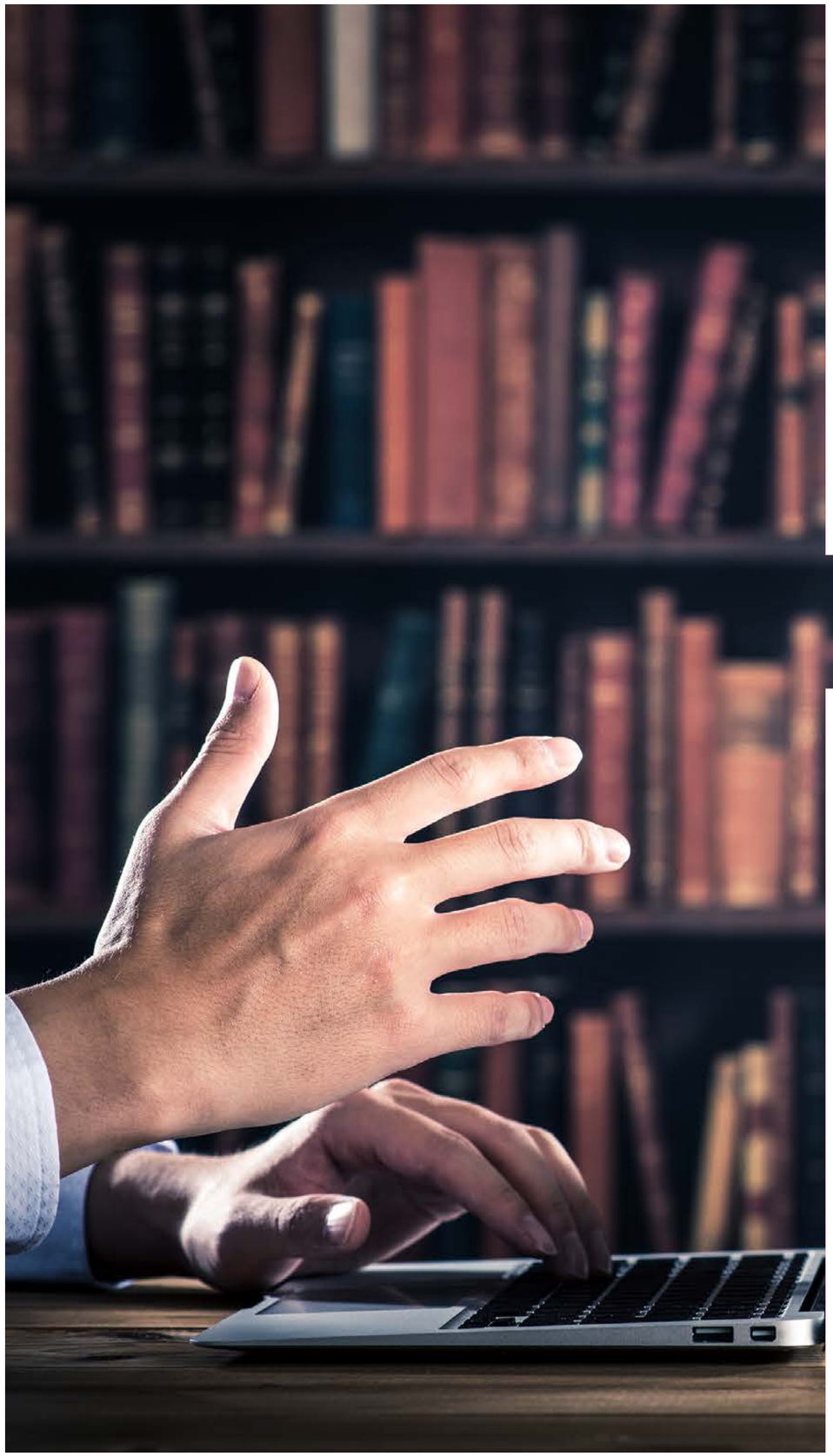
- Rendición de cuentas: los encargados deben, en determinadas circunstancias, mantener registros de las actividades de tratamiento de datos y ponerlos a disposición de la Autoridad correspondiente, cuando así se les requiera.

- Delegados de Protección de Datos: Los responsables y los encargados deben, en determinadas circunstancias, designar a un delegado de protección de datos

- Transferencias internacionales: los encargados deben cumplir las restricciones relativas a las transferencias transfronterizas.

Dado que tanto los responsables como los encargados tendrán obligaciones en virtud del RGPD, es importante que las empresas aclaren sus funciones, que incluso pueden cambiar durante el desarrollo de una campaña publicitaria.

Al respecto de lo anterior, te recomendamos las Directrices para la elaboración de contratos entre responsables y encargados del tratamiento de la Agencia Española de Protección de Datos para ayudar en ese ejercicio y, por ejemplo, conocer qué rol tiene tu empresa en cada determinada acción. En cualquier caso, es más que recomendable empezar a trabajar en los contratos con tus socios y revisar los que ya tienes para asegurarte que están en línea con los requisitos del RGPD.



10. Violaciones de datos

Las brechas de seguridad pueden tener importantes consecuencias, tanto en términos reputacionales como económicos. Por lo tanto, **debemos asegurarnos de poner en marcha todos los procedimientos que permitan detectar, informar e investigar una brecha de seguridad**. El RGPD exige a los responsables del tratamiento que hayan sufrido una iinfracción en la que el individuo sufra algún tipo de daño, como por robo de identidad o violación de la seguridad de los datos personales, notifiquen a su Autoridad de Protección de Datos en un plazo máximo de 72 horas (en caso contrario deberá ir acompañada de indicación de los motivos de la dilación). Los encargados están obligados a notificar al responsable sin demora indebida cualquier incumplimiento en el que hayan incurrido. Es conveniente identificar aquellas categorías de datos cuya afectación puede activar el requisito de notificación. Una auditoría puede ser de gran ayuda.

11. Privacidad desde el diseño y evaluación de impacto sobre la protección de datos

Las Evaluaciones de Impacto de la Protección de datos (PIA) juegan un papel importante en la nueva normativa. El requisito de llevar a cabo una PIA se exige en situaciones de alto riesgo, por ejemplo, cuando una nueva tecnología se está desplegando o cuando se van a elaborar perfiles que afecten significativamente a los interesados. Actualmente no está claro si este requisito se aplicará al tratamiento de datos seudónimos.

El RGPD también se refiere a nuevos principios como privacidad desde el diseño y por defecto. En ambos casos, llevar a cabo un PIA puede ayudarte a evaluar cómo incorporar estos dos principios en cualquier nuevo producto o servicio que se pretenda introducir en el mercado. La Agencia Española de Protección de Datos ha elaborado una Guía para la Evaluación de Impacto en la Protección de Datos personales, que, una vez más, ofrece un gran punto de partida para este ejercicio.

12. Delegado de Protección de Datos

El RGPD estipula que uno de los criterios para decidir si es necesario designar un delegado de protección de datos es cuando "*las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala*".

Si esto se aplica a tu empresa, tienes que nombrar a alguien con la responsabilidad de su cumplimiento RGPD. También tendrás que pensar en qué parte de la estructura empresarial se ajusta este perfil. Para ayudar en este tema, las autoridades europeas de protección de datos han aprobado un documento con Directrices sobre el rol del Delegado de Protección de Datos.

El delegado de protección de datos puede ser desempeñada por un empleado o por una persona externa. Además, el RGPD establece que un grupo de empresas pueden designar un DPD siempre que sea fácilmente accesible desde cada empresa. El DPD tiene una protección especial respecto a su empleador, y la organización no puede instruirle sobre cómo llevar a cabo su trabajo.

13. Autoridad competente

Uno de los beneficios potenciales que el RGPD puede proporcionar a las empresas es el concepto de ventanilla única. Las organizaciones con múltiples establecimientos en toda la UE, como es el caso de muchas de las organizaciones de la industria publicitaria digital, pueden beneficiarse de este nuevo principio, que permite la designación de una "autoridad de supervisión principal". Por lo tanto, las organizaciones que operan en varios estados miembros tendrán que evaluar cuidadosamente sus opciones en relación con el establecimiento de la autoridad principal.

En el marco del RGPD, la Autoridad de protección de datos del país de la UE en el que la organización tenga su "establecimiento principal" será su autoridad principal, que tiene competencia sobre los tratamientos transfronterizos que esa organización realice en todos los Estados miembros. El establecimiento principal suele ser la sede europea de la empresa, pero podría ser diferente en ciertas situaciones.

El Grupo de Trabajo del Artículo 29 ha adoptado unas Directrices para identificar la autoridad principal que pueden resultar de utilidad para ayudar en el ejercicio de la determinación de la autoridad líder.

14. Transferencias internacionales

Tienes que pensar en las opciones para transferir datos a países fuera de la UE sobre todo en caso de que esta obligación sea nueva para ti, dado que es posible que, hasta ahora, la información que tratabas no se considerase dato personal. Si transfieres datos fuera de la Unión Europea, es necesario que la fundamentes en alguna de las bases de legitimación que recoge el RGPD . La transferencia a países que la Comisión Europea considera que proporcionan una norma de protección de datos “adecuada” es de gran utilidad. La lista de países que actualmente gozan de este estatus está disponible aquí e incluye el Escudo de Privacidad (Privacy Shield) UE - EE.UU. Existen otras opciones, como las transferencias mediante “garantías adecuadas”, que incluyen una serie de supuestos que facilitan este trámite, como las cláusulas contractuales tipo elaboradas por la Comisión o por la autoridad de control, o los códigos de conducta bajo determinadas circunstancias.

Independientemente de la etapa de adaptación en la que se encuentre tu empresa, desde el departamento jurídico de IAB podemos asesorarte en la implementación.


iab
spain