Acronis

PREGUNTAS FRECUENTES SOBRE EL RGPD

PREGUNTAS FRECUENTES

P: ¿Qué es el RGPD?

R: El Reglamento general de protección de datos (RGPD) de la Unión Europea es una nueva ley de la UE que garantiza la protección de los datos privados que pertenecen a los residentes en la Unión Europea. Se trata de un único conjunto de normas que reemplaza a las distintas normativas de privacidad de los datos nacionales que existían anteriormente, y que se aplica directamente a todos los estados miembros de la UE.

P: ¿Cuándo entra en vigor el RGPD?

R: El 25 de mayo de 2018.

P: ¿Se aplica el RGPD solamente a las empresas con sede en la Unión Europea?

R: La respuesta a esta confusión habitual es "No." Toda empresa con clientes en la Unión Europea y que adquiera o gestione de cualquier otra forma datos personales de dichos clientes está sometida al cumplimiento del RGPD.

P: ¿Qué significa "datos personales" según el RGPD?

R: "Datos personales" se refiere a toda información que pueda servir para identificar a una persona. Es un concepto que va mucho más allá de la definición tradicional de información de identificación personal, ya que incluye el nombre, dirección de correo electrónico, publicaciones en medios sociales, información física, fisiológica o genética, datos médicos, ubicación, detalles bancarios, dirección IP, cookies e identidad cultural de la persona en cuestión.

P: ¿Qué regula exactamente el RGPD?

R: El RGPD regula la obtención, almacenamiento, transferencia y/o uso de todos los datos personales –lo que se denomina de forma colectiva "tratamiento"– que pertenecen a los residentes de la Unión Europea. Toda organización que trate datos personales de residentes de la UE, incluido el seguimiento de su localización o actividades; por ejemplo, mediante las cookies de un navegador, está sometida al cumplimiento de la ley, aunque dicha organización no resida físicamente en la Unión Europea.

El reglamento distingue entre "responsables" y "encargados" del tratamiento de los datos personales. El responsable es quien determina qué hacer con los datos personales y por qué motivo. Un tercero contratado por el responsable para realizar cualquier operación con los datos personales, como un proveedor de servicios en la nube, es un encargado.

P: ¿Qué efecto tiene el RGPD sobre los derechos a la privacidad?

R: El RGPD amplía considerablemente los derechos a la privacidad de los ciudadanos de la Unión Europea e impone obligaciones importantes relativas a la protección de dichos derechos a las empresas, instituciones o individuos que gestionen datos personales de estos ciudadanos. Los nuevos requisitos que deben satisfacer los encargados de los datos personales son:

- **Derechos de los interesados:** los residentes de la Unión Europea tienen un mayor control de sus datos personales. Esto incluye el derecho a solicitar a los encargados que les entreguen una copia, corrijan posibles errores y eliminen completamente los datos si así se les solicita.
- **Prueba del cumplimiento:** los encargados deben implementar las políticas y procedimientos adecuados de seguridad de los datos y mantener un registro detallado de sus actividades de tratamiento de datos.
- **Notificación de violación de la seguridad:** los encargados deberán comunicar las violaciones de datos a las autoridades de control del RGPD y, en el caso de violaciones graves, al interesado.
- **Multas por incumplimiento:** los organismos reguladores del RGPD pueden imponer multas cuantiosas a las organizaciones acusadas de incumplimiento, dependiendo de la gravedad de la violación y los daños derivados.

P: ¿Requiere el RGPD que los datos personales permanezcan en la UE?

R: No exactamente, pero trasladar los datos fuera de la UE (lo que se conoce como "transferencias de datos transfronterizas") sin incumplir el reglamento puede resultar complicado. Se deben tener en cuenta varias reglas. En principio se autorizan transferencias de datos normalmente a todo país que esté en la lista de la Unión Europea de destinos con seguridad "adecuada", que son los que cuentan con medidas de protección de la privacidad de los datos que se ajustan a los estándares de la UE. En algunos casos, es posible que aunque el país íntegro no se considere adecuado, sí lo sean determinados territorios o zonas. A principios de 2018, la lista aprobada incluía a todos los países de la UE, tres países no comunitarios que forman parte del Espacio Económico Europeo (Islandia, Liechtenstein y Noruega), y algunos otros países y territorios (Andorra, Argentina, Canadá, Islas Faroe, Guernsey, Isla de Man, Israel, Jersey, Nueva Zelanda, Suiza y Uruguay).

También se permiten transferencias de datos a destinos que cumplen las "normas corporativas vinculantes" de la UE. Estas normas permiten a determinadas entidades legales de una corporación y, en algunos casos, a grupos de empresas independientes que participan en alguna actividad económica conjunta, transferir datos personales. Para obtener la autorización, las normas corporativas vinculantes deben ser aprobadas por una autoridad de control adecuada y cumplir los estándares de coherencia de la Unión Europea.

Se permiten además otros destinos de los datos siempre que se ajusten a determinados "códigos de conducta" y "mecanismos de certificación", normalmente elaborados por una asociación sectorial o alguno de sus órganos representantes, y solamente si cuentan con la aprobación de los organismos reguladores del RGPD.

Otras transferencias de datos son legítimas si se pueden englobar dentro del epígrafe "derogaciones", es decir, excepciones a las normas estándar. Entre los ejemplos se incluyen las transferencias de datos personales:

- Que el interesado haya consentido de manera explícita tras conocer los riesgos asociados.
- Para las que el encargado deba cumplir una obligación contractual o satisfacer una demanda legal.
- Que se consideran de interés público o de vital interés para el interesado.
- Que sean en "interés legítimo" del responsable del tratamiento de los datos, siempre que dicho interés no entre en conflicto con el del propio interesado. El responsable del tratamiento debe evaluar las circunstancias de la transferencia y tomar las medidas razonables para proteger los datos personales

En definitiva, generalmente es más sencillo, más seguro y más barato para la mayoría de las empresas no trasladar datos personales fuera de la UE y su breve lista de países aprobados. Prepárese para asumir gastos y esfuerzo adicionales para trasladar los datos personales a otro lugar y para demostrar ante las autoridades de control del RGPD todo lo que ha hecho para su protección. Debe contar con un buen asesor legal si decide hacer uso de normas corporativas vinculantes, códigos de conducta, mecanismos de certificación y/o derogaciones específicas para justificar otros tipos de transferencias de datos a otros países.

P: ¿Cómo afecta el RGPD a nuestras respuestas a las violaciones de la seguridad?

R: El RGPD exige que tanto los responsables como los encargados del tratamiento implementen sistemas para proteger, supervisar y comunicar posibles violaciones de la seguridad, así como que apliquen y documenten tecnología, políticas y procedimientos para la prevención, detección, comunicación y notificación de violaciones. Se aplican nuevos requisitos de divulgación más estrictos a cualquier incidente que provoque el acceso, transferencia, alteración o destrucción de los datos personales por partes no autorizadas, tanto si es de manera accidental como intencionada.

Los incidentes de protección de la privacidad pueden ser provocados por fallos tecnológicos (por ejemplo, un fallo de un disco duro), errores humanos (por ejemplo, un miembro del equipo de TI elimina o daña de forma accidental archivos del usuario) o una violación intencionada con fines maliciosos (por ejemplo, un ataque de ransomware llevado a cabo por ciberdelincuentes que cifran datos personales y exigen el pago de un rescate para obtener la clave que los desbloquea).

En definitiva, los responsables y los encargados del tratamiento deben esforzarse más en identificar los incidentes de seguridad que afectan a los datos personales, comunicarlos a las autoridades de control en un plazo de 72 horas desde la detección y, en casos de daños graves a datos personales, robo o pérdida, notificar rápidamente a los interesados afectados también.

P: ¿Qué nuevos derechos del usuario deben respetar los responsables del tratamiento?

R: El RGPD proporciona a los interesados mucho más control y visibilidad sobre el uso que hacen los responsables de sus datos personales. Si así lo solicitan los usuarios (y sin ningún coste para estos), los responsables del tratamiento están obligados a informarles de qué partes de sus datos personales han adquirido y a proporcionárselos en un formato fácilmente accesible, así como a corregir los errores que hayan identificado los usuarios y eliminar determinados datos personales si así se lo piden (lo que se denomina el "derecho al olvido").

P: ¿Qué es el delegado de protección de datos? ¿Necesitan uno los responsables y encargados del tratamiento?

R: El delegado de protección de datos es un empleado o un consultor que deberán designar muchos responsables y encargados del tratamiento como principal responsable de supervisar el cumplimiento del RGPD. En el caso de las instituciones públicas, la exigencia es mayor: casi todas están obligadas a elegir a un delegado de protección de datos. Las empresas privadas deben nombrar a un delegado de protección de datos solo si tratan una gran cantidad de datos personales del interesado que revelan su raza u origen étnico, opiniones políticas, creencias religiosas o filosóficas, datos genéticos o biométricos, y/o infracciones penales.

El delegado debe ser un profesional del cumplimiento de normativas con la formación necesaria y con experiencia en las leyes y mejores prácticas de protección de datos. Su trabajo es comunicar a los responsables y encargados del tratamiento, así como a los empleados de la empresa sus obligaciones conforme al RGPD, supervisar el cumplimiento del reglamento y servir como conexión con la autoridad de control.

P: ¿Qué ocurre si un responsable o encargado del tratamiento, o ambos, incumplen las normas del RGPD?

R: Las multas por incumplimiento del RGPD no son nada desdeñables. Su autoridad de control local puede valorar la multa en 10 millones de euros o el 2 % de sus ingresos anuales, según la cifra que sea superior, para las infracciones de primer nivel, como no mantener registros por escrito o implementar las medidas técnicas u organizativas necesarias para satisfacer los requisitos de cumplimiento. Las multas pueden llegar a 20 millones de euros o el 4 % de sus ingresos anuales globales, según la cifra que sea superior, para infracciones más graves, como violaciones de datos importantes o la desprotección de los datos frente a robos, alteraciones o eliminaciones.

Tenga en cuenta que se pueden aplicar multas tanto a responsables como a encargados del tratamiento. Las autoridades de control pueden asignar la multa proporcionalmente al responsable y a los encargados, valorando su parte de responsabilidad en la violación, en función de los pasos que hayan dado cada uno de ellos para garantizar el cumplimiento del RGPD.

Además de estas temidas penalizaciones financieras, las empresas que de manera deliberada ignoren o menosprecien sus obligaciones en relación al cumplimento del RGPD se enfrentan a daños de su reputación posiblemente duraderos, así como a demandas judiciales de particulares por daños "materiales o no materiales" si se produce la violación de sus datos personales. Estas mismas sanciones y multas se aplican también a terceros que actúan como encargados del tratamiento si gestionan datos personales en nombre de otra empresa. Pensemos en cómo han crecido exponencialmente las violaciones de datos en los últimos años

Por ejemplo, si considera cómo han aumentado los ataques de ransomware, que han pasado de ser un negocio ilícito de 800 000 dólares/año en 2015 a 8000 - 1000 millones de dólares previstos para 2018, el potencial de incumplimiento solo en cuanto a comunicación de la violación es enorme.

P: La tarea de conseguir el cumplimiento del RGPD parece enorme. ¿Por dónde empezamos?

R: Como proveedor de soluciones de protección de datos, Acronis cree que un buen primer paso para el cumplimiento del RGPD es centrarse en actualizar su infraestructura de almacenamiento y copia de seguridad de los datos. Saber exactamente donde se almacenan sus datos, para evitar ataques como los de ransomware, y proteger los datos con un cifrado fuerte, tanto en tránsito como en reposo, son medidas fundamentales que tienen un impacto concreto y positivo en su estado de cumplimiento del RGPD.

Sin embargo, no debe depender de nosotros para decidir cómo abordar el reto del RGPD. Asegúrese también de contar con asesores legales y profesionales cualificados.

Estas preguntas frecuentes se proporcionan exclusivamente con fines informativos. No deben utilizarse ni interpretarse como asesoramiento legal. No debe actuar ni abstenerse de actuar basándose en el contenido de estas preguntas frecuentes sin solicitar asesoramiento legal o profesional de otra índole.

Acronis

Para obtener más información, visite **https://www.acronis.com/es-es/gdpr/**