SANS SECURITY AWARENESS

Boletín mensual de seguridad para todos

Reglamento General de Protección de Datos

Resumen

Puede ser que hayas escuchado sobre una nueva ley llamada GDPR (General Data Protection Regulation) o RGPD por sus siglas en español (Reglamento General de Protección de Datos). Esta ley fue desarrollada por la Unión Europea y entra en vigor el 25 de mayo de 2018. Es aplicable a cualquier organización que maneja la información personal de cualquier residente dentro de la Unión Europea, sin importar en qué parte del mundo se encuentra la organización. RGPD requiere que las organizaciones mantengan la privacidad y la seguridad de la información personal de cualquier residente de la Unión Europea. Para asegurar que se cumpla con la ley, se necesita comprender e implementar ciertos principios clave.

La gente tiene el derecho a la privacidad. Las organizaciones necesitan respetar la privacidad al restringir la información personal que recolectan y procesan acerca de los usuarios protegiendo esa información. Las obligaciones de privacidad son aplicables a cualquier información, ya sea por sí misma o cuando es usada con otras piezas de información, que podrían identificar a un individuo que vive en la Unión Europea. Esta información podrían ser elementos como el domicilio, números de pasaportes, números de licencia para conducir, detalles financieros, biométricos, membresías de sindicatos, historiales médicos, ubicación o información que se relaciona con la orientación sexual, religiosa o política. La regulación es aplicable a una "persona natural", es decir, a una persona viva. Aquí hay algunos de los principios fundamentales del RGPD que deberían ser respetados.

La información personal de los individuos debe ser procesada conforme a la ley, de manera justa y transparente.

Se debe notificar a la gente sobre qué información se recolecta y con qué propósito.

La información personal debe ser recolectada para propósitos específicos, explícitos y legítimos. No debe ser usada para cualquier otra razón que esté en conflicto con estos propósitos.

La información personal debe ser resguardada y procesada solamente por cuanto tiempo sea requerido para los propósitos y no más de eso.

La información personal debe estar actualizada y ser correcta.

La gente tiene el derecho de recibir una copia de su información o puede requerir que su información no sea usada, o en algunos casos, que sea eliminada.

Las organizaciones deben implementar medidas apropiadas de seguridad para proteger la información personal contra destrucción accidental o en contra de la ley, así como pérdida, alteración o revelación.

Adicionalmente, las organizaciones necesitan asegurar que todo el equipo que maneja información personal está entrenado apropiadamente para asegurar y proteger esos datos.

Las medidas de protección que aseguran la información personal deben garantizar un nivel de protección apropiado para la naturaleza sensible de la información. Dado que el riesgo asociado con la información se vuelve más grande, lo mismo debería suceder con el esfuerzo y la extensión de las medidas para proteger la información. Estas medidas deben ser revisadas y actualizadas regularmente. Es útil llevar registros bien documentados acerca de las decisiones de privacidad y seguridad, además de las medidas que ayudan a evidenciar el cumplimiento de estos requerimientos. Adicionalmente, las organizaciones están legalmente vinculadas a emplear estas medidas, como contratos y revisiones de diligencia debida para proteger la información personal cuando se transfiere a partes terciarias externas o particularmente aquellas instancias que se encuentran fuera de la Unión Europea. Finalmente, en el caso de un incidente de filtración de información personal, las organizaciones deben reportarlo en 72 horas después de que se den cuenta de ello. Si la organización falla en cumplir con el RGPD, puede sufrir multas de hasta el 4% de sus ganancias globales, lo que hace a esta ley una de las más costosas en el mundo.

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Editor Invitado

Brian Honan *es director general de BH Consulting, una firma de consultoría independiente de ciberseguridad y protección de la información en Dublín, Irlanda. Brian ha fungido como asesor especial del Centro de Cibercrimen de Europol (EC3), es fundador del primer CERT de Irlanda, y es miembro asesor de diversas compañías de seguridad innovadoras. Puedes encontrarlo en* www.linkedin.com/in/brianhonan *o en Twitter* @BrianHonan.

Recursos

¿Qué es la regulación GDPR?:	http://gdprandyou.ie
Reglamento General de Protección de Datos:	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
Boletín OUCH!:	https://www.sans.org/u/D88