MAYO 2023

Boletín de Protección de Datos Personales
y Seguridad de la Información

ESTUDIO OLAECHEA

GDPR: Diferencias y semejanzas con la Ley Peruana

A cinco años de la entrada en vigencia del GDRP.

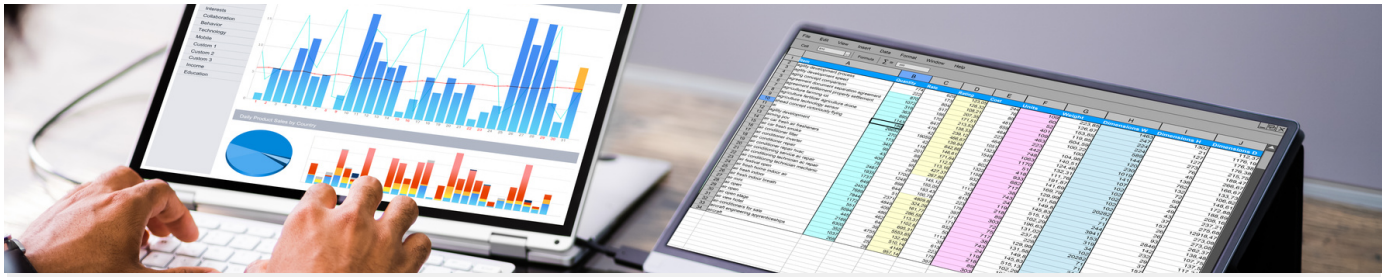
¿Qué es el GDRP?

El General Data Protection Regulation (GDPR) o Reglamento General de Protección de Datos (RGPD) es el reglamento creado por la Unión Europea con la finalidad de establecer lineamientos de obligatoria observancia a todos los países miembros de la Unión Europea en lo relativo a la protección de datos personales, con la finalidad de reforzar y unificar la legislación de protección de datos personales en todos los países miembros.

Acerca del GDRP

¿Es aplicable en Perú?

En 2018 la Autoridad Nacional de Protección de Datos Personales (ANPD) emitió la opinión consultiva 046-2018-JUS/DGTAIPD-DPDP, señala que el GDPR solo es aplicable cuando el tratamiento de datos personales de residentes de la Unión Europea se realice en dicho territorio; por lo tanto, no es aplicable al marco de tratamiento de datos personales realizados en el Perú respecto de residentes de la Unión Europa.
Entonces, teniendo en cuenta la soberanía del Estado Peruano, dentro del territorio nacional se aplicará la Ley de Protección de Datos (en Adelante, la LPDP) y su Reglamento.



¿Ha habido algún impacto en Perú desde la entrada en vigencia del GDPR?

Sí. La ANPD ha introducido, a través de jurisprudencia, uno de los principios más relevantes del GDPR: el principio de responsabilidad proactiva y demostrada.
Este principio señala que el Responsable del tratamiento debe ser capaz de demostrar el cumplimiento de los principios, por ejemplo, mediante la documentación de las medidas adoptadas.

¿Cuáles son las semejanzas y diferencias entre el GPDR y la normativa peruana de protección de datos personales?

	Ley peruana	GPDR
Base de legitimación del consentimiento	Ley autoritativa, consentimiento o excepciones al consentimiento.	Interés legítimo y consentimiento
Principios rectores	Consentimiento, legalidad, finalidad, confidencialidad, proporcionalidad, calidad, seguridad, disposición de recurso y nivel de protección adecuado.	Licitud, lealtad, transparencia, finalidad, minimización de datos, exactitud, confidencialidad, integridad y responsabilidad proactiva.
Extraterritorialidad	Si	Si

	Ley peruana	GPDR
Derechos del titular de los datos personales	Información, acceso, rectificación, cancelación u oposición.	Información, acceso, rectificación, supresión, limitación al tratamiento, portabilidad, oposición (incluye el tratamiento de decisiones individualizadas automatizadas).
Plazos de atención de los derechos de los titulares	Información: 8 días hábiles. Acceso: 20 días hábiles. Rectificación, cancelación y oposición: 10 días hábiles Plazos prorrogables por el mismo término	Un mes prorrogable por dos meses más.
Responsabilidad proactiva y demostrada	No regulado expresamente, pero aplicable por disposición jurisprudencial.	Sí, obligatorio
Protección de datos desde el diseño y por defecto	No regulado expresamente, pero aplica los principios establecidos en la Red Iberoamericana de Protección de Datos.	Sí, obligatorio
Designación de Oficial de Datos Personales	Obligatorio sólo para instituciones públicas.	Sí

	Ley peruana	GPDR
Evaluaciones de impacto en protección de datos.	No	Sí. Obligatorio en los casos valuación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, tratamientos a gran escala y observación sistemática a gran escala en zonas de acceso público.
Inscripciones de bancos de datos	Sí, obligatorio	No. Se exige un registro de actividades de tratamiento de datos.
Transferencias internacionales de datos	Legítimas siempre que cumpla con el principio de finalidad y consentimiento, el país de destino cumpla con el principio de nivel adecuado de tratamiento. Se aplican las cláusulas contractuales tipo de la Red Iberoamericana de Protección de Datos.	Legítimas si el tratamiento se realiza a un país calificado como de alto nivel de protección en datos personales, y a través de las cláusulas contractuales tipo de la UE.

Notificación de incidentes de seguridad a la autoridad	48 horas para las empresas del sector público, según el Reglamento de la Ley de Confianza Digital	72 horas después que se haya tenido constancia de la misma, menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.
Multas económicas	• Infracciones leves, cuyas multas rondan entre las 0,5 UIT (625.75 Euros aprox) y 5 UIT (6,257 Euros aprox). • Infracciones graves, por las cuales pueden imponerse multas de entre 5 UIT (6,257 Eurso aprox) y 50 UITs (62,570 Euros aprox). • Infracciones muy graves, con multas que oscilan entre las 50 UIT (62,570 Eurso aprox). y 100 UIT (125,403 Euros aprox).	• Para infracciones graves: multa de hasta 10 millones de euros (o el 2% de la facturación anual, aplicando la cuantía que resulte más alta). • Para infracciones muy graves: multa de hasta 20 millones de euros (o el 4% de la facturación anual, aplicando la cuantía que resulte más alta). La multa más alta impuesta asciende a 1,200 millones de euros.

Para más información, puede contactar al área de Protección de Datos Personales y Seguridad de la Información:

Carol Quiroz
Socia
carolquiroz@esola.com.pe