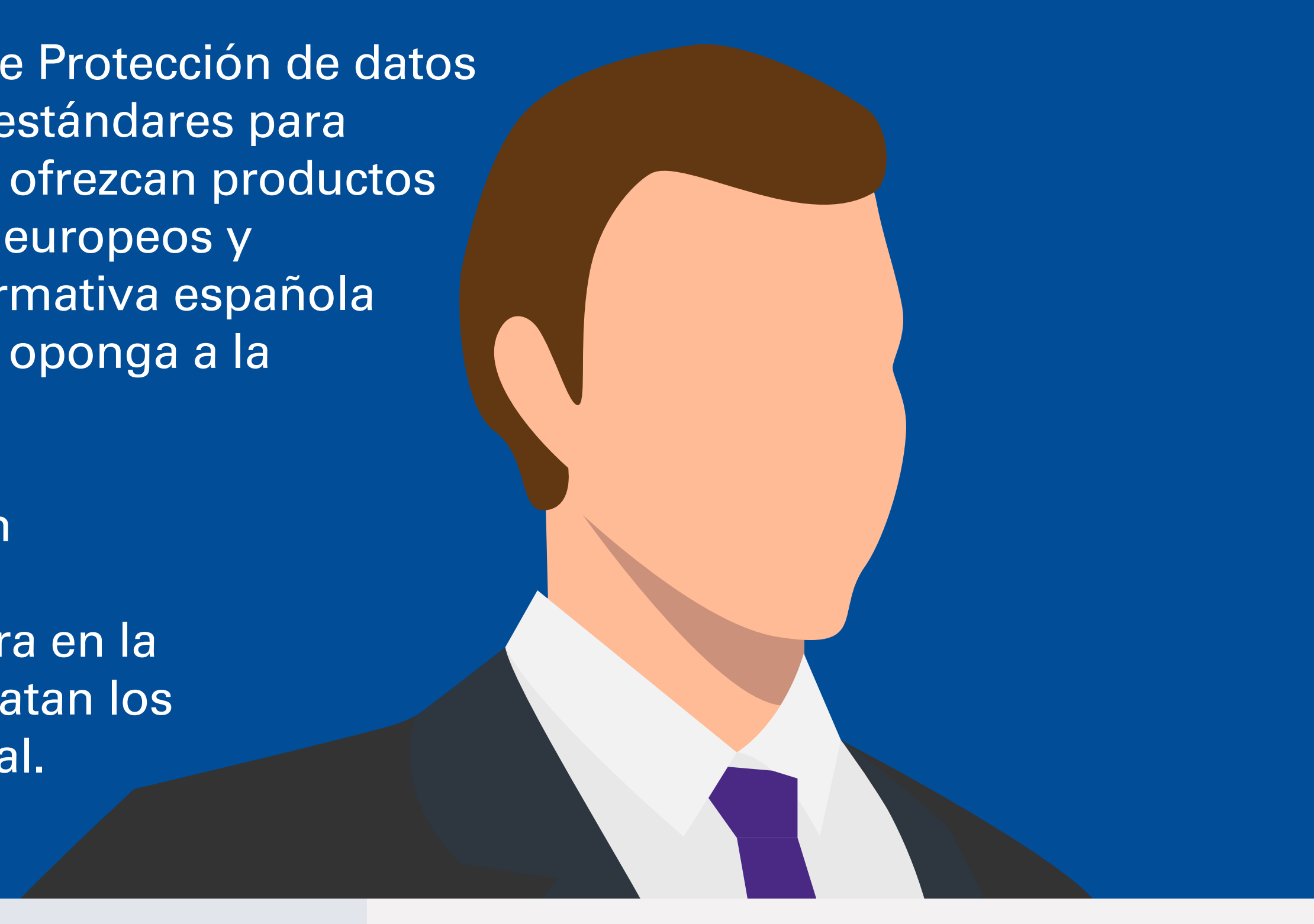
KPMG

# Novedades del RGDP

## ¿Cuáles son las principales novedades introducidas por el RGDP?

El Reglamento General de Protección de datos (RGPD) marcará nuevos estándares para todas las compañías que ofrezcan productos o servicios a ciudadanos europeos y desplazará a la actual normativa española (LOPD) en todo lo que se oponga a la regulación europea.

Estos cambios requerirán adaptaciones y mejoras significativas en la manera en la que las organizaciones tratan los datos de carácter personal.



Reglamento LOPD

VS

Nuevo RGPD

### Multas

Las multas en España varían, en función de la gravedad, entre 601,01€ y 601.012,10 €

Estructura escalonada de multas dependiendo del incumplimiento. El nivel 1 es el 2% de la facturación global o 10M € (lo que sea más alto). El nivel 2 es el 4% de la facturación global o 20M € (lo que sea más alto)

### Data Protection Officer (DPO)

Si bien no es obligatorio que exista esta figura, sí lo es nombrar a un responsable de Seguridad

Se requerirá para los cuerpos normativos y para las organizaciones que realicen vigilancia masiva o procesamiento masivo de datos de categorías especiales

### Autoridades de supervisión

La Agencia Española de Protección de Datos es una de las autoridades europeas con mayores funciones

Se proporcionará a las autoridades locales un rango de poder todavía mayor

### Inventario

Si bien no se utiliza este término, en España es obligatorio registrar los ficheros de tratamiento de datos de carácter personal

Generalmente las organizaciones necesitarán un inventario de datos de carácter personal (es probable que en España se mantenga la obligación de declarar los ficheros)

### Notificación

Generalmente no hay obligación de notificar los incumplimientos

Obligación de comunicar las brechas de seguridad de privacidad al regulador dentro de las 72 horas posteriores al evento

### Seguridad

Requerimientos establecidos en función del nivel del fichero

Requerimientos explícitos acerca de monitorización, encriptado y anonimización. Controles de seguridad en función del riesgo e impacto

### Privacy Impact Assessments (PIAs)

No hay requerimiento obligatorio de realizar PIAs

Las compañías deberían realizar PIAs si su actividad se considera de 'Alto Riesgo'

### Derechos de los interesados

Distintos derechos, incluyendo el derecho de acceso

Los derechos se amplían incluyendo portabilidad de datos y el derecho al olvido

### Datos personales sensibles

Incluyen creencias religiosas, datos sanitarios y origen étnico, entre otros

Similar, pero extendido a datos biométricos y genéticos

### Consentimiento

Consentimiento tácito permitido actualmente en España

Requerimiento de obtener consentimiento explícito y auditable

Fuentes:
- Elaboración propia